STMicroelectronics

ST33F1M/1M0/896/768/640/512F, SC33F1M0/896/768/640/512/384F, SM33F1M/1M0/896/768/640/512F, SE33F1M/1M0/896/768/640/512F, SL33F1M/1M0/896/768/640/512F, SP33F1MF, with dedicated software revision D or E, optional cryptographic library NESLIB 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 Security Target - Public Version

Common Criteria for IT security evaluation

SMD_SM33Fxxx_ST_12_001 Rev 02.01

December 2012

BLANK

SM33Fxxx
Security Target - Public Version

Common Criteria for IT security evaluation

1 Introduction

1.1 Security Target reference

1 Document identification: ST33F1M/1M0/896/768/640/512F, SC33F1M0/896/768/640/512/384F, SM33F1M/1M0/896/768/640/512F, SE33F1M/1M0/896/768/640/512F, SL33F1M/1M0/896/768/640/512F, SP33F1MF, with dedicated software revision D or E, optional cryptographic library Neslib 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 SECURITY TARGET - PUBLIC VERSION.

2 Version number: Rev 02.01, issued December 2012.

3 Registration: registered at ST Microelectronics under number SMD_SM33Fxxx_ST_12_001.

1.2 Purpose

4 This document presents **the Security Target - Public version (ST)** of the **ST33F1M/1M0/896/768/640/512F, SC33F1M0/896/768/640/512/384F, SM33F1M/1M0/896/768/640/512F, SE33F1M/1M0/896/768/640/512F, SL33F1M/1M0/896/768/640/512F, SP33F1MF** Security Integrated Circuits (IC), designed on the **ST33 platform of STMicroelectronics**, with Dedicated Software (DSW) rev D or E, optional cryptographic library **Neslib 3.0 or 3.2,** and optional technology **MIFARE DESFire™ EV1**.

5 The precise reference of the Target of Evaluation (TOE) and the security IC features are given in *Section 3: TOE description*.

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

Contents

List of tables

List of figures

2 Context

7 The Target of Evaluation (TOE) referred to in *Section 3: TOE description*, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Secure Microcontrollers Division of STMicroelectronics (ST).

8 The Target of Evaluation (TOE) is the ST33F1M with 30 commercial derivatives: ST33F1M0, ST33F896, ST33F768, ST33F640, ST33F512, SC33F1M0, SC33F896, SC33F768, SC33F640, SC33F512, SC33F384, SM33F1M, SM33F1M0, SM33F896, SM33F768, SM33F640, SM33F512, SE33F1M, SE33F1M0, SE33F896, SE33F768, SE33F640, SE33F512, SL33F1M, SL33F1M0, SL33F896, SL33F768, SL33F640, SL33F512, and SP33F1M rev F, with dedicated software rev D or E, with or without the cryptographic library Neslib 3.0 or 3.2, with or without the MIFARE DESFire™ EV1 technology.

9 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

10 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.

11 This ST claims to be an instantiation of the "*Security IC Platform Protection Profile*" (PP) registered and certified under the reference *BSI-PP-0035* 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.

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

13 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-PP-0035*, ***AUG1*** for Addition #1 of *AUG* and ***AUG4*** for Addition #4 of *AUG*.

3 TOE description

3.1 TOE identification

14 The Target of Evaluation (TOE) comprises the ST33F1M and 30 commercial derivatives: ST33F1M0, ST33F896, ST33F768, ST33F640, ST33F512, SC33F1M0, SC33F896, SC33F768, SC33F640, SC33F512, SC33F384, SM33F1M, SM33F1M0, SM33F896, SM33F768, SM33F640, SM33F512, SE33F1M, SE33F1M0, SE33F896, SE33F768, SE33F640, SE33F512, SL33F1M, SL33F1M0, SL33F896, SL33F768, SL33F640, SL33F512, and SP33F1M rev F, with dedicated software rev D or E. All of them may include the optional cryptographic library Neslib 3.0 or 3.2, and/or may include the optional library MIFARE DESFire™ EV1.

15 The master product is the ST33F1M. All based on the same hardware, the different derivatives 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 personalisation process.

16 All products of the TOE share the same hardware design, and the same maskset, thus mainly share the same characteristics:

Table 1. Master product and derivatives common characteristics

Maskset	Commercial revision	Product revision	Master identification number [(1)]	System ROM revision (1)	OST revision (1)	Optional crypto library name & revision[(2)]	Optional MIFARE DESFire EV1 Id[(3)]	Optional MIFARE DESFire EV1 revision[(4)]
K8C0A	F	J	0000h	000Dh or 000Eh	0023h	Neslib 3.0 or 3.2 1300h / 1320h	0x02, 0x06 or 0x07	1.1.0

1. Part of the product information.
2. See the Neslib User Manual referenced in *Section 9* .
3. See the ST33F1M and derivatives Flash loader installation guide referenced in *Section 9* .
4. See the MIFARE DESFire EV1 User Manual referenced in *Section 9* .

17 The commercial revision (aka external revision) is updated when hardware or OST modification has a visible impact for the customer.

18 The product revision (aka internal revision) is updated when hardware or OST is modified. This letter completely identifies the product.

19 The different derivatives differ from the master product, only on the available NVM and RAM memories size, on the availability of the SWP interface, and on the presence of the MIFARE technology (libraries).

20 In order to clearly distinguish between them, they have a specific identification number, as detailed here below:

Table 2. Master product and derivatives specific characteristics

Commercial name	Product Id [1]	NVM size	RAM size	SWP	MIFARE technology [2]
ST33F1M	0000h	1.2 MBytes	30 Kbytes	Yes	No
SP33F1M	0000h	1.2 MBytes	30 Kbytes	Yes	Yes
SM33F1M	002Bh	1.2 MBytes	30 Kbytes	Yes	Yes
SE33F1M	002Bh	1.2 MBytes	30 Kbytes	Yes	Yes
SL33F1M	002Bh	1.2 MBytes	30 Kbytes	Yes	Yes
ST33F1M0	0034h	1 MBytes	30 Kbytes	Yes	No
SC33F1M0	0038h	1 MBytes	30 Kbytes	No	No
SM33F1M0	0035h	1 MBytes	30 Kbytes	Yes	Yes
SE33F1M0	0035h	1 MBytes	30 Kbytes	Yes	Yes
SL33F1M0	0035h	1 MBytes	30 Kbytes	Yes	Yes
ST33F896	0036h	896 Kbytes	30 Kbytes	Yes	No
SC33F896	0039h	896 Kbytes	30 Kbytes	No	No
SM33F896	0037h	896 Kbytes	30 Kbytes	Yes	Yes
SE33F896	0037h	896 Kbytes	30 Kbytes	Yes	Yes
SL33F896	0037h	896 Kbytes	30 Kbytes	Yes	Yes
ST33F768	0026h	768 Kbytes	24 Kbytes	Yes	No
SC33F768	0027h	768 Kbytes	24 Kbytes	No	No
SM33F768	002Ch	768 Kbytes	24 Kbytes	Yes	Yes
SE33F768	002Ch	768 Kbytes	24 Kbytes	Yes	Yes
SL33F768	002Ch	768 Kbytes	24 Kbytes	Yes	Yes
ST33F640	001Ah	640 Kbytes	24 Kbytes	Yes	No
SC33F640	0025h	640 Kbytes	24 Kbytes	No	No
SM33F640	002Dh	640 Kbytes	24 Kbytes	Yes	Yes
SE33F640	002Dh	640 Kbytes	24 Kbytes	Yes	Yes
SL33F640	002Dh	640 Kbytes	24 Kbytes	Yes	Yes
ST33F512	0028h	512 Kbytes	24 Kbytes	Yes	No
SC33F512	0029h	512 Kbytes	24 Kbytes	No	No
SM33F512	002Eh	512 Kbytes	24 Kbytes	Yes	Yes
SE33F512	002Eh	512 Kbytes	24 Kbytes	Yes	Yes
SL33F512	002Eh	512 Kbytes	24 Kbytes	Yes	Yes
SC33F384	002Ah	384 Kbytes	24 Kbytes	No	No

1. Part of the product information.
The derivatives prefixed by “SM”, “SE” and “SL” which share the same suffix, have the same Product Id, because they have exactly the same product configuration. The “SM”, “SE” and “SL” prefix only reflects different contract conditions.
The derivative prefixed by “SP” has the same Product Id as the Master Product because it is only a transitory commercial name, changed during profiling.

2. Amongst the MIFARE libraries, only MIFARE DESFire EV1 is in the scope of the evaluation.

21 All along the product life, specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: Master product and derivatives common characteristics* and *Table 2: Master product and derivatives specific characteristics*.

22 In this Security Target, the terms:

- "TOE" or "SM33Fxxx" mean all products listed in *Table 2: Master product and derivatives specific characteristics*,
- "DESFire" means MIFARE DESFire™ EV1.

23 The rest of this document applies to all products, with or without Neslib and/or DESFire, except when a restriction is mentioned. For easier reading, the restrictions are typeset as indicated here.

3.2 TOE overview

24 The TOE is a serial access Secure Microcontroller 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.

25 The TOE offers a high-density User Flash memory, an internally generated clock, an MPU, an internal true random number generator (TRNG) and accelerators dedicated to cryptographic algorithms.

26 Operations can be synchronized with an external clock or with an internally generated clock issued by the Clock Generator module. The internal speed of the device is fully software programmable. High performance can be reached by using high speed internal clock frequency (up to 22.5 MHz). The CPU interfaces with the on-chip RAM, ROM and Flash memories via a 32-bit internal bus.

27 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 E-DES (Enhanced DES) module supports efficiently the Data Encryption Standard (DES *[2]*) with built-in coutermeasures against side channel attacks. Additionally, an extra feature allows fast implementation of CBC and CBC-MAC modes *[10] [9]*.

29 The NExt Step CRYPTography accelerator (NESCRYPT) enables efficient computation for both GF(p) and GF(2^n) with a very high level of performance. NESCRYPT also includes dedicated instructions to accelerate hash function SHA-1 and SHA-2 families. NESCRYPT allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance (*[4]*, *[8]*, *[12]*, *[18]*,*[19]*, *[20]*, *[21]*).

30 As randomness is a key stone in many applications, the SM33Fxxx features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 *[1]* and directly accessible through dedicated registers.

31 The TOE offers 2 or 3 communication channels to the external world: a serial communication interface fully compatible with the ISO/IEC 7816-3 standard, an optional 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. See the list of products including or not the SWP in *Table 2: Master product and derivatives specific characteristics*.

32 In a few words, the SM33Fxxx 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,
- Hardware Security Enhanced DES accelerator,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- NExt Step CRYPTography accelerator (NESCRYPT),
- optional cryptographic library,
- optional secure MIFARE DESFire EV1 library.

33 The TOE includes in the OST ROM 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.

34 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.

35 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.

36 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.

37 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 DESFire, when they are embedded.

38 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 developper in his applicative code.

Neslib provides the most useful operations in public key algorithms 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 *[20]*),
- 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) *[18]*,
- an asymmetric key cryptographic support module that provides secure hash functions (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 *[4]*),
- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES *[7]*),
- prime number generation *[6]*.

39 The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is a MIFARE technology library (see the list of products including or not the MIFARE technology in *Table 2: Master product and derivatives specific characteristics*).
This library may be a secure library called MIFARE DESFire™ EV1, which is **in the scope of this evaluation**. DESFire features a mutual three pass authentication, a data encryption on RF channel, and a flexible self-securing file system.
This library may alternatively be MIFARE Classic™, which is **not in the scope of this evaluation**.
Note that Mifare Classic may also co-exist on the TOE with MIFARE DESFire™ EV1.

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

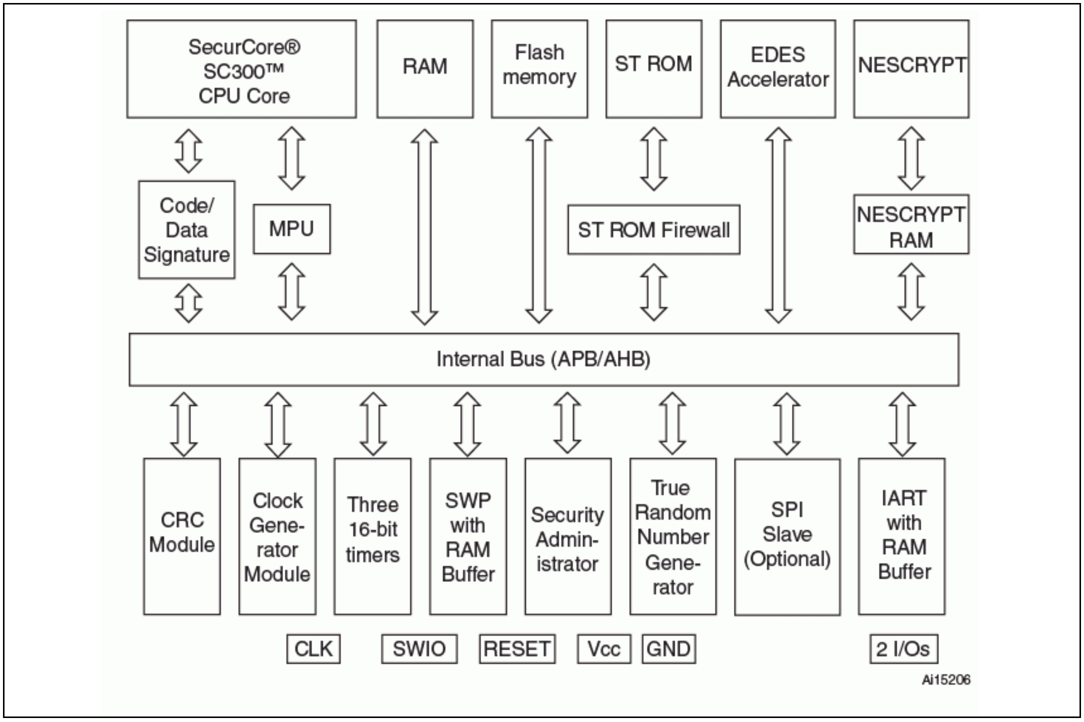
- the product Data Sheet and die description,
- the product family Security Guidance,
- the AIS31 user manuals,
- the Cortex M3 SC300 Technical Reference Manuals,
- the System ROM user manual,
- the Flash loader installation guide,
- optionally the Neslib user manual,
- optionally the MIFARE DESFire EV1 user manual,
- optionally the MIFARE Classic user manual.

41 The complete list of guidance documents is detailed in *Section 9*.

42 The TOE includes neither the Operating System (OS) nor the application layer.
In the following, the term "OS" means the Operating System built on top of the TOE.
In the following, the term "applications" means all software components built on top of the TOE, except the OS. The OS and applications may or may not be evaluated under the Common Criteria, by the OS or application developers. In case DESFire is embedded, the OS evaluation is mandatory.

43 *Figure 1* provides an overview of the SM33Fxxx.

Figure 1. SM33Fxxx block diagram



3.3 TOE life cycle

44 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 *Security IC Platform Protection Profile* (*BSI-PP-0035*), section 1.2.3.

45 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.

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

47 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.

48 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.

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

50 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.

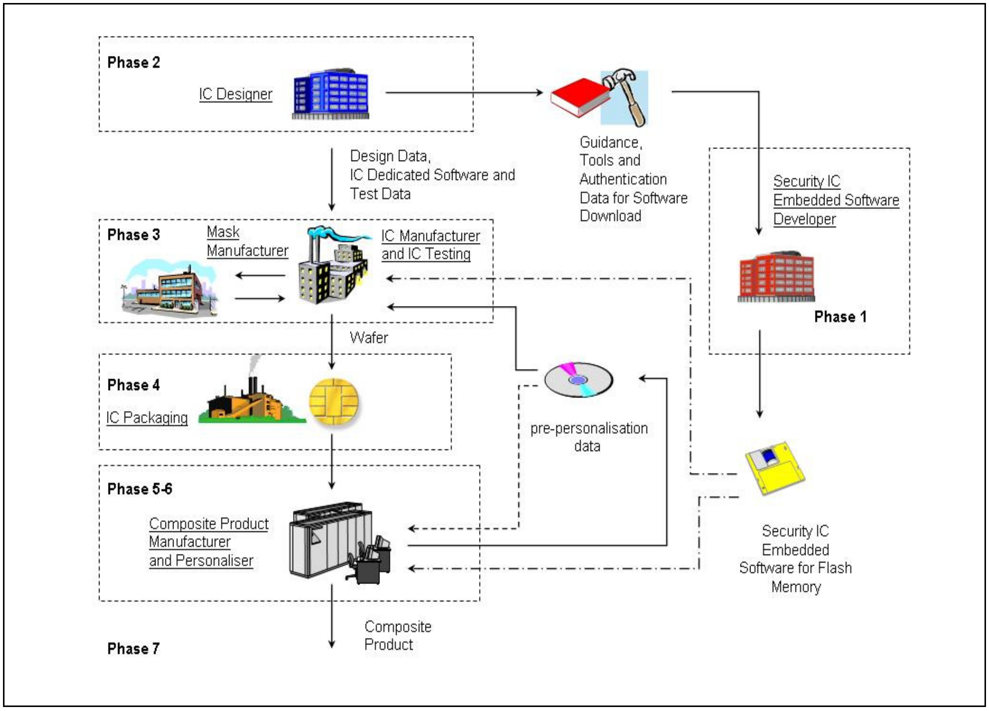
51 The TOE is delivered in ISSUER or USER configuration.

Table 3. Composite product life cycle phases

Phase	Name	Description	Responsible party
1	IC embedded software development	security IC embedded software development specification of IC pre-personalization requirements	IC embedded software developer
2	IC development	IC design IC dedicated software development	IC developer: **ST**
3	IC manufacturing	integration and photomask fabrication IC production IC testing pre-personalisation	IC manufacturer: **ST** or **TSMC**
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary	IC packaging manufacturer: **ST** or **NEDCARD** or **SMARTFLEX** or **STATSCHIP PAK** or **AMKOR**
5	Composite product integration	composite product finishing process composite product testing	Composite product integrator
6	Personalisation	composite product personalisation composite product testing	Personaliser
7	Operational usage	composite product usage by its issuers and consumers	End-consumer

52 The following figure shows the possible organization of the life cycle, adapted to the TOE which comprises programmable NVM. Thus, the Security IC Embedded Software may be loaded onto the TOE in phase 3, 4, 5 or 6, depending on customer’s choice.

Figure 2. Security IC life cycle


Phase 2
IC Designer
Guidance, Tools and Authentication Data for Software Download
Design Data, IC Dedicated Software and Test Data
Security IC Embedded Software Developer
Phase 1
Phase 3
Mask Manufacturer
IC Manufacturer and IC Testing
Wafer
Phase 4
IC Packaging
pre-personalisation data
Phase 5-6
Composite Product Manufacturer and Personaliser
Security IC Embedded Software for Flash Memory
Composite Product
Phase 7

3.4 TOE environment

53 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.

3.4.1 TOE Development Environment

54 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.

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

56 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).

57 The development centres involved in the development of the TOE are the following: **ST Rousset (France)** and **ST Ang Mo Kio (Singapore)**, for the design activities, **ST Rousset**

(FRANCE), for the engineering activities, **ST ROUSSET (FRANCE)** and **ST ZAVENTEM (BELGIUM)** for the software development activities.

58 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 with accountability and traceability of all (good and bad) products. 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).

59 The authorized sub-contractors involved in the TOE mask manufacturing can be **DNP (JAPAN)** and **DPE (ITALY)**.

3.4.2 TOE production environment

60 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.

61 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.

62 The authorized front-end plant involved in the manufacturing of the TOE can be **ST ROUSSET (FRANCE)** or **TSMC (TAIWAN)**. **ST CROLLES (FRANCE)** can be involved for the mask inspection.

63 The authorized EWS plant involved in the testing of the TOE can be **ST ROUSSET (FRANCE)** or **ST TOA PAYOH (SINGAPORE)**.

64 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.

65 When the product is delivered after phase 4, the authorized back-end plant involved in the packaging of the TOE can be **ST BOUSKOURA (MOROCCO)** or **ST CALAMBA (THE PHILIPPINES)** or **ST MUAR (MALAYSIA)** or **NEDCARD (THE NETHERLANDS)** or **SMARTFLEX (SINGAPORE)** or **STATSCHIP PAK (SINGAPORE)** or **AMKOR (THE PHILIPPINES)**. **ST SHENZHEN (CHINA)** or **DISCO (GERMANY)** can be involved for the wafers backlap and sawing.

66 **ST LOYANG (SINGAPORE)** can also be involved for the logistics.

3.4.3 TOE operational environment

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

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

69 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.

4 Conformance claims

4.1 Common Criteria conformance claims

70 The SM33Fxxx Security Target claims to be conformant to the Common Criteria version 3.1.

71 Furthermore it claims to be CC Part 2 (*CCMB-2012-09-002*) extended and CC Part 3 (*CCMB-2012-09-003*) conformant. The extended Security Functional Requirements are those defined in the *Security IC Platform Protection Profile* (*BSI-PP-0035*).

72 The assurance level for the SM33Fxxx Security Target is ***EAL 5*** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

73 The SM33Fxxx Security Target claims strict conformance to the *Security IC Platform Protection Profile* (*BSI-PP-0035*), as required by this Protection Profile.

4.2.2 PP Refinements

74 The main refinements operated on the *BSI-PP-0035* are:

- Addition #1: “Support of Cipher Schemes” from *AUG*,
- Addition #4: “Area based Memory Access Control” from *AUG*,
- Specific additions for the Secure Flash Loader
- Specific additions for DESFire,
- Refinement of assurance requirements.

75 All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-PP-0035* being typeset as indicated here. Text originating in *AUG* is typeset as indicated here.

4.2.3 PP Additions

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

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

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

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

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

4.2.4 PP Claims rationale

81 The differences between this Security Target security objectives and requirements and those of *BSI-PP-0035*, to which conformance is claimed, have been identified and justified in *Section 6* and in *Section 7*. They have been recalled in the previous section.

82 In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the *BSI-PP-0035*.

83 The security problem definition presented in *Section 5*, clearly shows the additions to the security problem statement of the PP.

84 The security objectives rationale presented in *Section 6.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-PP-0035*.

85 Similarly, the security requirements rationale presented in *Section 7.4* has been updated with respect to the protection profile.

86 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.

5 Security problem definition

87 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.

88 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 *Security IC Platform Protection Profile* (*BSI-PP-0035*), section 3. Only those originating in *AUG*, and the one introduced in this Security Target, are detailed in the following sections.

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

5.1 Description of assets

90 Since this Security Target claims strict conformance to the *Security IC Platform Protection Profile* (*BSI-PP-0035*), the assets defined in section 3.1 of the Protection Profile are applied and the assets regarding threats are clarified in this Security Target.

91 The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software,
- 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,
- the EDES accelerator, the NESCRYPT crypto processor, the random number generator,
- when DESFire is embedded, the special functions for the communication with an external interface device,
- when DESFire or Neslib is embedded, the cryptographic function for AES,
- the User Data comprising, especially when 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.

92 This Security Target includes optionally Security IC Embedded Software and therefore does contain more assets compared to *BSI-PP-0035*. These assets are described above.

93 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.

Table 4. Summary of security environment

	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	Unauthorised data modification
	T.Impersonate	Impersonating authorised users during authentication
	T.Cloning	Cloning
	T.Integ-Applic-Code	DESFire code integrity
	T.Resource	DESFire resource unavailability
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	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	Confidentiality during communication
	P.Transaction	Transaction mechanism
	P.No-Trace	Un-traceability of end-users
	P.Plat-Appl	Usage of hardware platform
	P.Resp-Appl	Treatment of user data
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Plat-Appl	Usage of Hardware Platform
	BSI.A.Resp-Appl	Treatment of User Data
	A.Secure-Values	Usage of secure values
	A.Terminal-Support	Terminal support to ensure integrity and confidentiality
	A.Confid-Applic-Code	DESFire code confidentiality
	A.Confid-Applic-Data	DESFire data confidentiality
	A.Integ-Applic-Data	DESFire data integrity

5.2 Threats

94 The threats are described in the BSI-PP-0035, section 3.2. Only those originating in AUG and those related to 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.

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

Unauthorised data modification:

T.Data-Modification 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.

Impersonating authorised users during authentication:

T.Impersonate 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.

Cloning:

T.Cloning 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.Integ-Applic-Code DESFire code integrity:

MIFARE DESFire EV1 Licensed product code must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to memory area where the MIFARE DESFire EV1 licensed product executable code is stored.
The attacker executes an application that tries to alter (part of) the DESFire EV1 code.

T.Resource DESFire resource unavailability:

The availability of resources for the MIFARE DESFire EV1 Licensed product shall be controlled to prevent denial of service or malfunction.
An attacker prevents correct execution of DESFire EV1 through consumption of some resources of the card: e.g. RAM or non volatile RAM.

5.3 Organisational security policies

96 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.

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

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

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

100 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.

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

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

BSI.P.Process-TOE Protection 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.

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

The TOE shall provide the following specific security functionality to the Security IC Embedded Software:

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Advanced Encryption Standard (AES), if Neslib is embedded only***,***
- ***Elliptic Curves Cryptography on GF(p),*** if Neslib is embedded only***,***
- ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if Neslib is embedded only***,***
- Rivest-Shamir-Adleman (RSA)***,*** if Neslib is embedded only,
- ***Prime Number Generation,*** if Neslib is embedded only***.***

Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

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 Confidentiality during communication:

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

P.Transaction Transaction mechanism:

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 Un-traceability of end-users:

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.Plat-Appl Usage of hardware platform:

The Security IC Embedded Software, part of the TOE, uses the TOE hardware platform according to the assumption A.Plat-Appl defined in *BSI-PP-0035*.

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-PP-0035*.

5.4 Assumptions

103 The assumptions are described in the *BSI-PP-0035*, section 3.4.

BSI.A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

BSI.A.Plat-Appl Usage of Hardware Platform

BSI.A.Resp-Appl Treatment of User Data

104 The following assumptions are defined for DESFire only.
Thus, they do not contradict with the security problem definition of the *BSI-PP-0035*, as they are only related to assets which are out of the scope of this PP.

105 In consequence, the addition of these asumptions does not contradict with the strict conformance claim on the *BSI-PP-0035*.

106 These assumptions are valid in case DESFire is embedded in the TOE.

A.Secure-Values Usage of secure values:

Only confidential and secure keys shall be used to set up the authentication and access rights in DESFire. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal-Support Terminal support to ensure integrity and confidentiality:

The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication.

A.Confid-Applic-Code DESFire code confidentiality:

The Security IC Embedded Software is designed so that DESFire code is protected against unauthorized disclosure.
The memory areas where the DESFire executable code is stored are kept protected from disclosure.

A.Confid-Applic-Data DESFire data confidentiality:

The Security IC Embedded Software is designed so that DESFire data is protected against unauthorized disclosure.
The read access to the DESFire data by another application is prevented.

A.Integ-Applic-Data DESFire data integrity:

The Security IC Embedded Software is designed so that DESFire data is protected against unauthorized modification.
The write access to the DESFire data by another application is prevented.

6 Security objectives

107 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.

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

109 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 protection profile. Only those originating in *AUG*, and the one 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
	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	Access Control for DESFire
	O.Authentication	Authentication for DESFire
	O.Confidentiality	DESFire Confidential Communication
	O.Type-Consistency	DESFire Data type consistency
	O.Transaction	DESFire Transaction mechanism
	O.No-Trace	Preventing Traceability for DESFire
	O.Plat-Appl	Usage of hardware platform
	O.Resp-Appl	Treatment of user data
	O.Resource	Resource availability for DESFire
	O.Verification	DESFire code integrity check

Table 5. Summary of security objectives (continued)

	Label	Title
Environments	BSI.OE.Plat-Appl	Usage of Hardware Platform
	BSI.OE.Resp-Appl	Treatment of User Data
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing
	OE.Firewall	DESFire firewall
	OE.Shr-Res	DESFire data cleaning for resource sharing
	OE.Secure-Values	Generation of secure values
	OE.Terminal-Support	Terminal support to ensure integrity and confidentiality

6.1 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

AUG1.O.Add-Functions

Additional Specific Security Functionality:

The TOE must provide the following specific security functionality to the ***Security IC*** Embedded Software:

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Advanced Encryption Standard (AES), if Neslib is embedded only*,*
- ***Elliptic Curves Cryptography on GF(p),*** if Neslib is embedded only*,*
- ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if Neslib is embedded only*,*
- Rivest-Shamir-Adleman (RSA)*,* if Neslib is embedded only,
- ***Prime Number Generation,*** if Neslib is embedded only***.***

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.

110 The following objectives are only valid in case DESFire is embedded:

O.Access-Control

Access Control for 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

Authentication for 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

DESFire Confidential Communication:

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

O.Type-Consistency

DESFire Data type consistency:

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

O.Transaction

DESFire 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

Preventing Traceability for 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.Plat-Appl	Usage of hardware platform: To ensure that the TOE is used in a secure manner the Security IC Embedded Software, part of the TOE, shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC dedicated software of the TOE, (iii) TOE application notes, other guidance documents, and (iii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software.
O.Resp-Appl	Treatment of user data: Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.
O.Resource	Resource availability for DESFire: The TOE shall control the availability of resources for MIFARE DESFire EV1 Licensed product.
O.Verification	DESFire code integrity check: The TOE shall ensure that MIFARE DESFire EV1 code is verified prior being executed.

6.2 Security objectives for the environment

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

BSI.OE.Plat-Appl	Usage of Hardware Platform
BSI.OE.Resp-Appl	Treatment of User Data

112 This section details the security objectives for the operational environment, related to DESFire, and enforced by the Security IC Embedded Software.

113 These security objectives for the operational environment are only valid if DESFire is embedded in the TOE:

OE.Firewall	DESFire firewall: In order to ensure that the code and data of DESFire are protected against unauthorised disclosure and unauthorised modification, the Security IC Embedded Software shall be designed to ensure isolation of data and code between DESFire and the other applications. An application shall not read, write, compare piece of data or code belonging to DESFire.

OE.Shr-Res DESFire data cleaning for resource sharing:

The Security IC Embedded Software shall be designed to ensure that any hardware resource that is shared by DESFire and other applications or by any application which has access to such hardware resource, is always cleaned whenever 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 DESFire is interrupted by another application.

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

BSI.OE.Process-Sec-IC Protection during composite product manufacturing

115 This section details the security objectives for the operational environment, related to DESFire, and to be enforced after TOE delivery up to phase 6.

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

OE.Secure-Values Generation of secure values:

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 Terminal support to ensure integrity and confidentiality:

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.

6.3 Security objectives rationale

117 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-PP-0035* protection profile, together with those in *AUG*, and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 5* are addressed by the security objectives stated in this chapter.

118 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).

119 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*)".

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

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

121 As required by CC Part 1 (*CCMB-2012-09-001*), no assumption nor objective for the environment has been added to those of the *BSI-PP-0035* Protection Profile to which strict conformance is claimed.

122 The justification of the additional policies and the additional threat provided in the next subsections shows that they do not contradict to the rationale already given in the protection profile *BSI-PP-0035* for the assumptions, policy and threats defined there.

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Plat-Appl	*BSI.OE.Plat-Appl*	Phase 1
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
A.Confid-Applic-Code	*OE.Firewall*	Phase 1
A.Confid-Applic-Data	*OE.Firewall*	Phase 1
A.Integ-Applic-Data	*OE.Firewall* *OE.Shr-Res*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 4-6
P.Controlled-ES-Loading	*O.Controlled-ES-Loading*	Phase 4-6
A.Secure-Values	*OE.Secure-Values*	Phases 5-7
A.Terminal-Support	*OE.Terminal-Support*	Phase 7
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
P.Confidentiality	*O.Confidentiality* *OE.Terminal-Support*	

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
P.Transaction	*O.Transaction*	
P.No-Trace	*O.No-Trace* *O.Access-Control* *O.Authentication*	
P.Plat-Appl	*O.Plat-Appl*	
P.Resp-Appl	*O.Resp-Appl*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
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	*O.Access-Control* *O.Type-Consistency* *OE.Terminal-Support*	
T.Impersonate	*O.Authentication*	
T.Cloning	*O.Access-Control* *O.Authentication*	
T.Integ-Applic-Code	*O.Verification* *OE.Firewall*	
T.Resource	*O.Resource*	

6.3.1 Assumption "Usage of secure values"

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

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

125 *A.Secure-Values* and *OE.Secure-Values* do not contradict with the security problem definition of the *BSI-PP-0035*, because they are only related to DESFire, which is out of the scope of this protection profile.

6.3.2 Assumption "Terminal support to ensure integrity and confidentiality"

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

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

128 *A.Terminal-Support* and *OE.Terminal-Support* do not contradict with the security problem definition of the *BSI-PP-0035*, because they are only related to DESFire, which is out of the scope of this protection profile.

6.3.3 Assumption "DESFire code confidentiality"

129 The justification related to the assumption “DESFire code confidentiality, (*A.Confid-Applic-Code*)” is as follows:

130 Since *OE.Firewall* requires that the Security IC Embedded Software is designed to ensure isolation of code between DESFire and the other applications, the code of DESFire is protected against unauthorised disclosure, therefore *A.Confid-Applic-Code* is covered by *OE.Firewall*.

131 *A.Confid-Applic-Code* and *OE.Firewall* do not contradict with the security problem definition of the *BSI-PP-0035*, because they are only related to DESFire, which is out of the scope of this protection profile.

6.3.4 Assumption "DESFire data confidentiality"

132 The justification related to the assumption “DESFire data confidentiality, (*A.Confid-Applic-Data*)” is as follows:

133 Since *OE.Firewall* requires that the Security IC Embedded Software is designed to ensure isolation of data between DESFire and the other applications, the data of DESFire is protected against unauthorised disclosure, therefore *A.Confid-Applic-Data* is covered by *OE.Firewall*.

134 *A.Confid-Applic-Data* and *OE.Firewall* do not contradict with the security problem definition of the *BSI-PP-0035*, because they are only related to DESFire, which is out of the scope of this protection profile.

6.3.5 Assumption "DESFire data integrity"

135 The justification related to the assumption “DESFire data integrity, (*A.Integ-Applic-Data*)” is as follows:

136 Since *OE.Firewall* and *OE.Shr-Res* require that the Security IC Embedded Software is designed to ensure isolation of data between DESFire and the other applications, the data of DESFire is protected against unauthorised modification, therefore *A.Integ-Applic-Data* is covered by *OE.Firewall* together with *OE.Shr-Res*.

137 *A.Integ-Applic-Data*, *OE.Firewall* and *OE.Shr-Res* do not contradict with the security problem definition of the *BSI-PP-0035*, because they are only related to DESFire, which is out of the scope of this protection profile.

6.3.6 TOE threat "Memory Access Violation"

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

139 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.

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

6.3.7 TOE threat "Unauthorised data modification"

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

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

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

6.3.8 TOE threat "Impersonating authorised users during authentication"

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

145 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* is that an authentication mechanism is implemented in the TOE that prevents these attacks. Therefore the threat is covered by *O.Authentication*.

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

6.3.9 TOE threat "Cloning"

147 The justification related to the threat “Cloning, (*T.Cloning*)” is as follows:

148 The concern of *T.Cloning* is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objective *O.Authentication* together with *O.Access-Control* 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* states that no keys used for authentication shall ever be output. Therefore the two objectives cover *T.Cloning*.

6.3.10 TOE threat "DESFire resource unavailability"

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

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

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

6.3.11 TOE threat "DESFire code integrity"

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

153 The threat is related to the alteration of DESFire code by an attacker. *O.Verification* requires that the TOE verifies the code integrity before its execution. Complementary, *OE.Firewall* requires that the Security IC Embedded Software is designed to ensure isolation of code between DESFire and the other applications, thus protecting the code of DESFire against unauthorised modification. Therefore the threat is covered by *O.Verification* together with *OE.Firewall*.

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

6.3.12 Organisational security policy "Additional Specific Security Functionality"

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

156 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.

157 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*.

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

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

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

160 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.

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

6.3.14 Organisational security policy "Confidentiality during communication"

162 The justification related to the organisational security policy "Confidentiality during communication, (*P.Confidentiality*)" is as follows:

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

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

6.3.15 Organisational security policy "Transaction mechanism"

165 The justification related to the organisational security policy "Transaction mechanism, (*P.Transaction*)" is as follows:

166 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*, therefore the policy *P.Transaction* is covered by *O.Transaction*.

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

6.3.16 Organisational security policy "Un-traceability of end-users"

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

169 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* 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* and *O.Access-Control* provide means to authorise subjects and to implement access control to data elements in a way that unauthorised subjects can not read any element usable for tracing. Therefore the policy is covered by these three objectives.

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

6.3.17 Organisational security policy "Usage of hardware platform"

171 The justification related to the organisational security policy "Usage of hardware platform, (*P.Plat-Appl*)" is as follows:

172 The policy states that the Security IC Embedded Software included in the TOE, uses the TOE hardware according to the respective PP assumption *BSI.A.Plat-Appl*. *O.Plat-Appl* has

the same objective as *BSI.OE.Plat-Appl* defined in the PP. Thus, the objective *O.Plat-Appl* covers the policy *P.Plat-Appl*.

173 The added objective for the TOE *O.Plat-Appl* does not introduce any contradiction in the security objectives.

6.3.18 Organisational security policy "Treatment of user data"

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

175 In analogy to *P.Plat-Appl*, the policy *P.Resp-Appl* is covered in the same way by the objective *O.Resp-Appl*.

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

7 Security requirements

177 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 7.1*), a section on security assurance requirements (SARs) for the TOE (*Section 7.2*), a section on the refinements of these SARs (*Section 7.3*) as required by the "*BSI-PP-0035*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 7.4*).

7.1 Security functional requirements for the TOE

178 Security Functional Requirements (SFRs) from the "*BSI-PP-0035*" Protection Profile (PP) are drawn from *CCMB-2012-09-002*, except the following SFRs, that are **extensions** to *CCMB-2012-09-002*:

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

The reader can find their certified definitions in the text of the "*BSI-PP-0035*" Protection Profile.

179 All extensions to the SFRs of the "*BSI-PP-0035*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2012-09-002*.

180 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2012-09-001*. They are easily identified in the following text as they appear ***as indicated here***. Note that in order to improve readability, iterations are sometimes expressed within tables.

181 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.

182 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-PP-0035*	*CCMB-2012-09-002*
FPT_FLS.1	Failure with preservation of secure state			

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

Label	Title	Addressing	Origin	Type
FMT_LIM.1 [Test]	Limited capabilities	Abuse of TEST functionality	*BSI-PP-0035*	Extended
FMT_LIM.2 [Test]	Limited availability			
FMT_LIM.1 [Issuer]	Limited capabilities	Abuse of ISSUER functionality	Security Target Operated	
FMT_LIM.2 [Issuer]	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-PP-0035* Operated	
FPT_PHP.3	Resistance to physical attack	Physical manipulation & probing	*BSI-PP-0035*	*CCMB-2012-09-002*
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-PP-0035* Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	*CCMB-2012-09-002*
FCS_CKM.1 (if Neslib)	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-2012-09-002
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_SMF.1 [Loader]	Specification of management functions	Abuse of ISSUER functionality		
FMT_SMR.1 [MIFARE]	Security roles	DESFire access control (if DESFire is embedded only)	Security Target Operated	
FDP_ACC.1 [MIFARE]	Subset access control			
FDP_ACF.1 [MIFARE]	Security attribute based access control			
FMT_MSA.3 [MIFARE]	Static attribute initialisation			
FMT_MSA.1 [MIFARE]	Management of security attribute			
FMT_SMF.1 [MIFARE]	Specification of management functions			
FDP_ITC.2 [MIFARE]	Import of user data with security attributes			
FPT_TDC.1 [MIFARE]	Inter-TSF basic TSF data consistency			

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

Label	Title	Addressing	Origin	Type
FCS_COP.1 [AES/MIFARE]	Cryptographic operation	DESFire confidentiality and authentication (if DESFire is embedded only)		CCMB-2012-09-002
FIA_UID.2 [MIFARE]	User identification before any action			
FIA_UAU.2 [MIFARE]	User authentication before any action			
FIA_UAU.5 [MIFARE]	Multiple authentication mechanisms			
FMT_MTD.1 [MIFARE]	Management of TSF data			
FPT_TRP.1 [MIFARE]	Trusted path			
FCS_CKM.4 [MIFARE]	Cryptographic key destruction			
FDP_ROL.1 [MIFARE]	Basic rollback	DESFire robustness (if DESFire is embedded only)		
FPT_RPL.1 [MIFARE]	Replay detection			
FPR_UNL.1 [MIFARE]	Unlinkability			
FPT_TST.1 [MIFARE]	TSF testing	DESFire correct operation (if DESFire is embedded only)		
FRU_RSA.2 [MIFARE]	Minimum and maximum quotas			

7.1.1 Limited fault tolerance (FRU_FLT.2)

183 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).***

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

184 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.***

185 Refinement:

The term “failure” above also covers “circumstances”. The TOE prevents failures for the “circumstances” defined above.

Regarding application note 15 of *BSI-PP-0035*, 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.

7.1.3 Limited capabilities (FMT_LIM.1) [Test]

186 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].

7.1.4 Limited availability (FMT_LIM.2) [Test]

187 The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Limited capability and availability Policy [Test].

188 SFP_1: Limited capability and availability Policy [Test]

Deploying Test Features after TOE Delivery does not allow User Data 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.

7.1.5 Audit storage (FAU_SAS.1)

189 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***.

7.1.6 Resistance to physical attack (FPT_PHP.3)

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

191 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.

7.1.7 Basic internal transfer protection (FDP_ITT.1)

192 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.

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

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

194 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.

7.1.9 Subset information flow control (FDP_IFC.1)

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

196 SFP_2: Data Processing Policy

User Data 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.

7.1.10 Random number generation (FCS_RNG.1)

197 The TSF shall provide a ***physical*** random number generator that implements a ***total failure test of the random source.***

198 The TSF shall provide random numbers that meet ***PTG.2 class of*** *BSI-AIS20/AIS31*.

7.1.11 Cryptographic operation (FCS_COP.1)

199 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]
Even without Neslib	EDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode * MAC computation in CBC-MAC	Data Encryption Standard (DES)	56 bits	*FIPS PUB 46-3* *ISO/IEC 9797-1* *ISO/IEC 10116*
			Triple Data Encryption Standard (3DES)	168 bits	
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	Rivest, Shamir & Adleman's	up to 4096 bits	*PKCS #1 V2.1*
If Neslib	AES	* encryption (cipher) * decryption (inverse cipher) * key expansion * randomize	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS PUB 197*

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	* 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)	up to 640 bits	*IEEE 1363-2000, chapter 7* *IEEE 1363a-2004*
If Neslib	SHA	* SHA-1 * SHA-224 * SHA-256 * SHA-384 * SHA-512 * Protected SHA-1	Secure Hash Algorithm	assignment pointless because algorithm has no key	*FIPS PUB 180-1* *FIPS PUB 180-2* *ISO/IEC 10118-3:1998*

7.1.12 Cryptographic key generation (FCS_CKM.1)

200 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	up to 2048 bits	*FIPS PUB 140-2* *FIPS PUB 186*
Protected prime generation	prime generation and RSA prime generation algorithm, protected against side channel attacks	up to 2048 bits	*FIPS PUB 140-2* *FIPS PUB 186*
RSA key generation	RSA key pair generation algorithm	up to 4096 bits	*FIPS PUB 140-2* *ISO/IEC 9796-2* *PKCS #1 V2.1*
Protected RSA key generation	RSA key pair generation algorithm, protected against side channel attacks	up to 4096 bits	*FIPS PUB 140-2* *ISO/IEC 9796-2* *PKCS #1 V2.1*

7.1.13 Static attribute initialisation (FMT_MSA.3) [Memories]

201 The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to provide ***minimally protective***[a] 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.

7.1.14 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.***

7.1.15 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.

7.1.16 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 Issuer 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.***

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.*

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

211 *SFP_3: Dynamic Memory Access Control Policy*

[a] See the Datasheet referenced in *Section 9* for actual values.

212 *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.*

7.1.17 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.***

7.1.18 Limited capabilities (FMT_LIM.1) [Issuer]

214 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 [Issuer]***.

7.1.19 Limited availability (FMT_LIM.2) [Issuer]

215 The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: ***Limited capability and availability Policy [Issuer]***.

216 *SFP_4: Limited capability and availability Policy [Issuer]*

217 *Deploying Loading or Final Test Artifacts after TOE Delivery to final user (phase 7 / USER configuration) does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, stored software to be reconstructed or altered, and no substantial information about construction of TSF to be gathered which may enable other attacks.*

7.1.20 Import of user data without security attributes (FDP_ITC.1) [Loader]

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

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

220 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.***

7.1.21 Static attribute initialisation (FMT_MSA.3) [Loader]

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

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

7.1.22 Management of security attributes (FMT_MSA.1) [Loader]

223 The TSF shall enforce the ***Loading Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***password*** to ***the Standard Loader.***

7.1.23 Subset access control (FDP_ACC.1) [Loader]

224 The TSF shall enforce the ***Loading Access Control Policy*** on ***the execution of the Standard Loader instructions and/or the Advanced Loader instructions***.

7.1.24 Security attribute based access control (FDP_ACF.1) [Loader]

225 The TSF shall enforce the ***Loading Access Control Policy*** to objects based on the following: ***an external process may execute the Standard Loader instructions and/or the Advanced Loader instructions, depending on the presentation of valid passwords.***

226 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the Standard Loader instructions and/or Advanced Loader instructions can be executed only if valid passwords have been presented.***

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

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

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

230 SFP_5: Loading Access Control Policy

231 According to a password control, the TSF grants execution of the instructions of the Standard Loader, Advanced Loader or Profiler.

7.1.25 Specification of management functions (FMT_SMF.1) [Loader]

232 The TSF will be able to perform the following management functions: ***modification of the Standard Loader behaviour, by the Advanced Loader, under the Loading Access Control Policy.***

233 The following SFRs are extensions to "*BSI-PP-0035*" Protection Profile (PP), related to the capabilities and protections of DESFire.

234 They are only valid in case DESFire is embedded.

235 **Note**: MIFARE DESFire EV1 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.

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

7.1.26 Security roles (FMT_SMR.1) [MIFARE]

237 The TSF shall maintain the roles ***Administrator, Application Manager, Application User and Everybody***.

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

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

7.1.27 Subset access control (FDP_ACC.1) [MIFARE]

240 The TSF shall enforce the ***MIFARE Access Control Policy*** on ***all subjects, objects, operations and attributes defined by the MIFARE Access Control Policy.***

7.1.28 Security attribute based access control (FDP_ACF.1) [MIFARE]

241 The TSF shall enforce the ***MIFARE Access Control Policy*** to objects based on the following: ***all subjects, objects and attributes***.

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

- ***The Administrator 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.***

243 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.***

244 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.***

245 The following SFP ***MIFARE Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) [MIFARE]":

246 SFP_6: MIFARE Access Control Policy

247 The Security Function Policy (SFP) MIFARE Access Control Policy uses the following definitions:

248 The subjects are:

- *The 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.*

249 *The objects are:*

- *The Card itself.*
- *The 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.*

250 *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.*

251 *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 an application, a value or a data file,*
- *delete an application, a value or a data file and*
- *modify attribute of the 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.

252 *The security attributes are:*

- *Attributes of the card, applications, values and data files.*
  There is a set of attributes for the card, a set of attributes for every application and a set of attributes for every single file within an application.
  The term "card attributes" will be used for the set of attributes related to the 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. These keys are considered as authentication data and not as security attributes. The 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.*

254 *Implications of the MIFARE Access Control Policy:*

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

7.1.29 Static attribute initialisation (FMT_MSA.3) [MIFARE]

256 The TSF shall enforce the ***MIFARE Access Control Policy*** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

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

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

7.1.30 Management of security attributes (FMT_MSA.1) [MIFARE]

259 The TSF shall enforce the ***MIFARE Access Control Policy*** to restrict the ability to ***modify or freeze*** the security attributes ***card attributes, application attributes and file attributes*** to the ***Administrator, Application Manager and Application User, respectively***.

260 Refinement:

The detailed management abilities are:

- The 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.

7.1.31 Specification of Management Functions (FMT_SMF.1) [MIFARE]

261 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 card, Changing a key, Occurrence of any error during the execution of a command, Reset,***
- ***Changing a security attribute,***
- ***Creating or deleting an application, a value or a data file.***

7.1.32 Import of user data with security attributes (FDP_ITC.2) [MIFARE]

262 The TSF shall enforce the ***MIFARE Access Control Policy*** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

265 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.

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

7.1.33 Inter-TSF basic TSF data consistency (FPT_TDC.1) [MIFARE]

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

268 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.

7.1.34 Cryptographic operation (FCS_COP.1[AES/MIFARE])

269 The TSF shall perform ***encryption and decryption*** in accordance with a specified cryptographic algorithm ***Advanced Encryption Standard (AES) algorithm*** and cryptographic key sizes of ***128 bits*** that meet the following ***standard***: FIPS PUB 197.

7.1.35 Cryptographic key destruction (FCS_CKM.4) [MIFARE]

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

7.1.36 User identification before any action (FIA_UID.2) [MIFARE]

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

Application note:
Identification of a user 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’.

7.1.37 User authentication before any action (FIA_UAU.2) [MIFARE]

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

7.1.38 Multiple authentication mechanisms (FIA_UAU.5) [MIFARE]

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

274 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 Administrator, Application Manager and Application User.***

7.1.39 Management of TSF data (FMT_MTD.1) [MIFARE]

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

276 Refinement:

The detailed management abilities are:

- The Administrator can modify the card master key. The 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 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.

7.1.40 Trusted path (FTP_TRP.1) [MIFARE]

277 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***.

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

279 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***.

7.1.41 Basic rollback (FDP_ROL.1) [MIFARE]

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

281 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***.

7.1.42 Replay detection (FPT_RPL.1) [MIFARE]

282 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***.

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

7.1.43 Unlinkability (FPR_UNL.1) [MIFARE]

284 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***.

7.1.44 TSF testing (FPT_TST.1) [MIFARE]

285 The TSF shall run a suite of self tests ***during initial start-up and periodically during normal operation*** to demonstrate the correct operation of ***DESFire***.

286 The TSF shall provide authorised users with the capability to verify the integrity of ***the DESFire code***.

287 The TSF shall provide authorised users with the capability to verify the integrity of ***DESFire***.

Application note:
DESFire itself is the authorised user that verifies the integrity of its own code and execution.

7.1.45 Minimum and maximum quotas (FRU_RSA.2) [MIFARE]

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

289 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 DESFire, and all other applications running on the TOE. The goal is to ensure that DESFire always have enough NVM and RAM for its own usage.

7.2 TOE security assurance requirements

290 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.

291 Regarding application note 21 of *BSI-PP-0035*, the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

292 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-PP-0035*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-PP-0035*
ADV_INT.2	Well-stuctured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/*BSI-PP-0035*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-PP-0035*
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/*BSI-PP-0035*
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-PP-0035*
ALC_DVS.2	Sufficiency of security measures	*BSI-PP-0035*
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-PP-0035*
ALC_TAT.2	Compliance with implementation standards	EAL5
ATE_COV.2	Analysis of coverage	EAL5/*BSI-PP-0035*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-PP-0035*

Table 10. TOE security assurance requirements (continued)

Label	Title	Origin
ATE_IND.2	Independent testing - sample	EAL5/*BSI-PP-0035*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-PP-0035*

7.3 Refinement of the security assurance requirements

293 As *BSI-PP-0035* defines refinements for selected SARs, these refinements are also claimed in this Security Target.

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

295 Regarding application note 22 of *BSI-PP-0035*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

296 The text of the impacted refinements of *BSI-PP-0035* is reproduced in the next sections.

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

Table 11. Impact of EAL5 selection on *BSI-PP-0035* refinements

Assurance Family	*BSI-PP-0035* 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

7.3.1 Refinement regarding functional specification (ADV_FSP)

298 ~~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.***

299 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.

300 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.

301 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.

302 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.

303 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-PP-0035* refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

7.3.2 Refinement regarding test coverage (ATE_COV)

304 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).

305 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).

306 ~~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.***

7.4 Security Requirements rationale

7.4.1 Rationale for the Security Functional Requirements

307 Just as for the security objectives rationale of *Section 6.3*, the main line of this rationale is that the inclusion of all the security requirements of the *BSI-PP-0035* protection profile, together with those in *AUG*, and with those introduced in this Security Target, guarantees that all the security objectives identified in *Section 6* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

308 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 10*, it can be verified that the justifications provided by the *BSI-PP-0035* protection profile and *AUG* can just be carried forward to their union.

309 From *Table 5*, it is straightforward to identify two additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem-Access*) tracing back to *AUG*, and eleven additional objectives (*O.Controlled-ES-Loading, O.Access-Control, O.Authentication, O.Confidentiality, O.Type-Consistency, O.Transaction, O.No-Trace, O.Plat-Appl, O.Resp-Appl, O.Resource,* and *O.Verification*) introduced in this Security Target. This rationale must show that security requirements suitably address these three.

310 Furthermore, a more careful observation of the requirements listed in *Table 7* and *Table 10* shows that:

- there are security requirements introduced from *AUG* (*FCS_COP.1*, *FDP_ACC.2 [Memories]*, *FDP_ACF.1 [Memories]*, *FMT_MSA.3 [Memories]* and *FMT_MSA.1 [Memories]*),
- there are additional security requirements introduced by this Security Target (*FCS_CKM.1*, *FMT_LIM.1 [Issuer]*, *FMT_LIM.2 [Issuer]*, *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_SMF.1 [Memories]*, *FMT_SMR.1 [MIFARE], FDP_ACC.1 [MIFARE], FDP_ACF.1 [MIFARE], FMT_MSA.3 [MIFARE], FMT_MSA.1 [MIFARE], FMT_SMF.1 [MIFARE], FDP_ITC.2 [MIFARE], FPT_TDC.1 [MIFARE], FCS_COP.1 [AES/MIFARE], FIA_UID.2 [MIFARE], FIA_UAU.2 [MIFARE], FIA_UAU.5 [MIFARE], FMT_MTD.1 [MIFARE], FMT_MTD.1 [MIFARE], FPT_TRP.1 [MIFARE], FCS_CKM.4 [MIFARE], FDP_ROL.1 [MIFARE], FPT_RPL.1 [MIFARE], FPR_UNL.1 [MIFARE], FPT_TST.1 [MIFARE],* and *FRU_RSA.2 [MIFARE],* and various assurance requirements of EAL5).

311 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-PP-0035* protection profile, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

312 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-PP-0035*, they form an internally consistent whole, is provided in the next subsections.

7.4.2 Additional security objectives are suitably addressed

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

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

314 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.

315 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*)”

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

317 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*)”

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

319 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.

320 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 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 DESFire (*O.Access-Control*)”

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

322 The security functional requirement "*Security roles (FMT_SMR.1) [MIFARE]*" defines the roles of the MIFARE Access Control Policy.
The security functional requirements "*Subset access control (FDP_ACC.1) [MIFARE]*" and "*Security attribute based access control (FDP_ACF.1) [MIFARE]*" define the rules and "*Static attribute initialisation (FMT_MSA.3) [MIFARE]*" and "*Management of security attributes (FMT_MSA.1) [MIFARE]*" the attributes that the access control is based on.
The security functional requirement "*Management of TSF data (FMT_MTD.1) [MIFARE]*" provides the rules for the management of the authentication data.
The management functions are defined by "*Specification of Management Functions (FMT_SMF.1) [MIFARE]*".
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) [MIFARE]*".
Since cryptographic keys are used for authentication (refer to *O.Authentication*), 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) [MIFARE]*".
These nine SFRs together provide an access control mechanism as required by the objective *O.Access-Control*.

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

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

324 The two security functional requirements "*Cryptographic operation (FCS_COP.1)*[DES]" and "*Cryptographic operation (FCS_COP.1[AES/MIFARE])*" 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) [MIFARE]*", "*User authentication before any action (FIA_UAU.2) [MIFARE]*" and "*Multiple authentication mechanisms (FIA_UAU.5) [MIFARE]*" together define that users must be identified and authenticated before any action. The ‘none’ authentication of "*Multiple authentication mechanisms (FIA_UAU.5) [MIFARE]*" 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) [MIFARE]*" 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) [MIFARE]*" which requires a replay detection for these authentication requests, the seven security functional requirements fulfil the objective *O.Authentication*.

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

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

326 The security functional requirement "*Cryptographic operation (FCS_COP.1[AES/MIFARE])*" 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) [MIFARE]*" 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) [MIFARE]*" which requires a replay detection for these data transfers, the three security functional requirements fulfil the objective *O.Confidentiality*.

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

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

328 The security functional requirement "*Inter-TSF basic TSF data consistency (FPT_TDC.1) [MIFARE]*" 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*.

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

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

330 The security functional requirement "*Basic rollback (FDP_ROL.1) [MIFARE]*" 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*.

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

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

332 The security functional requirement "*Unlinkability (FPR_UNL.1) [MIFARE]*" 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*.

Security objective “Usage of hardware platform (*O.Plat-Appl*)”

333 The justification related to the security objective “Usage of hardware platform (*O.Plat-Appl*)” is as follows:

334 The objective was translated from an environment objective in the PP into a TOE objective in this ST. Its goal is to ensure that the hardware platform is used in a secure manner, which is based on the insight that hardware and software have to supplement each other in order to build a secure whole. The ST claims conformance to the PP and the PP SFRs do cover the PP TOE objectives. The PP uses the environment objective OE.Plat-Appl to ensure appropriate software support for its SFRs, but since the TOE does now consist of hardware and software, the PP SFRs do also apply to the Security IC Embedded Software included in the TOE, and thereby all PP SFRs fulfil the objective O.Plat-Appl. In other words: the software support required by the hardware-focused PP is now included in this combined hardware-software TOE and both hardware and software fulfil the PP SFRs.

Security objective “Treatment of user data (*O.Resp-Appl*)”

335 The justification related to the security objective “Treatment of user data (*O.Resp-Appl*)” is as follows:

336 The objective was translated from an environment objective in the PP into a TOE objective in this ST. The objective is that “Security relevant User Data (especially cryptographic keys)

are treated by the Security IC Embedded Software as required by the security needs of the specific application context." The application context is defined by the security environment described in this ST. The additional SFRs defined in this ST do address the additional TOE objectives of the ST based on the ST security environment, therefore *O.Resp-Appl* is fulfilled by the additional ST SFRs.

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

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

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

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

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

340 The security functional requirement "*TSF testing (FPT_TST.1) [MIFARE]*" requires that the TSF runs a suite of self tests to demonstrate the correct operation of DESFire. This meets the objective *O.Verification*.

7.4.3 Additional security requirements are consistent

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

341 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]*)"

342 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]*)"

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

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

"Cryptographic operation (*FCS_COP.1 [AES/MIFARE]*),
User identification before any action (*FIA_UID.2 [MIFARE]*),
User authentication before any action (*FIA_UAU.2 [MIFARE]*),
Multiple authentication mechanisms (*FIA_UAU.5 [MIFARE]*)"

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

"Trusted path (*FPT_TRP.1 [MIFARE]*),
Replay detection (*FPT_RPL.1 [MIFARE]*)"

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

"Inter-TSF basic TSF data consistency (*FPT_TDC.1 [MIFARE]*)"

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

"Basic rollback (*FDP_ROL.1 [MIFARE]*)"

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

"Unlinkability (*FPR_UNL.1 [MIFARE]*)"

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

"Minimum and maximum quotas (*FRU_RSA.2 [MIFARE]*)"

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

"TSF testing (*FPT_TST.1 [MIFARE]*)"

351 This security requirement has already been argued in *Section : Security objective "DESFire code integrity check (O.Verification)"* above.

7.4.4 Dependencies of Security Functional Requirements

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

- those justified in the *BSI-PP-0035* protection profile security requirements rationale,
- those justifed in *AUG* security requirements rationale (except on FMT_MSA.2, see discussion below),
- the dependency of *FCS_COP.1* and *FCS_CKM.1* on FCS_CKM.4 (see discussion below).
- the dependency of *FMT_MSA.1 [Loader]* and *FMT_MSA.3 [Loader]* on FMT_SMR.1 (see discussion below).

353 Details are provided in *Table 12* below.

Table 12. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-PP-0035*
FPT_FLS.1	None	No dependency	Yes, *BSI-PP-0035*
FMT_LIM.1 [Test]	FMT_LIM.2 [Test]	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2 [Test]	FMT_LIM.1 [Test]	Yes	Yes, *BSI-PP-0035*
FMT_LIM.1 [Issuer]	FMT_LIM.2 [Issuer]	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2 [Issuer]	FMT_LIM.1 [Issuer]	Yes	Yes, *BSI-PP-0035*
FAU_SAS.1	None	No dependency	Yes, *BSI-PP-0035*
FPT_PHP.3	None	No dependency	Yes, *BSI-PP-0035*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, *BSI-PP-0035*
FPT_ITT.1	None	No dependency	Yes, *BSI-PP-0035*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-PP-0035*	Yes, *BSI-PP-0035*
FCS_RNG.1	None	No dependency	Yes, *BSI-PP-0035*
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-2012-09-002*

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FDP_ACF.1 [Memories]	FDP_ACC.1 [Memories]	Yes, by FDP_ACC.2 [Memories]	Yes, *AUG* ***#4***
	FMT_MSA.3 [Memories]	Yes	
FMT_MSA.3 [Memories]	FMT_MSA.1 [Memories]	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	
FMT_MSA.1 [Memories]	[FDP_ACC.1 [Memories] or FDP_IFC.1]	Yes, by FDP_ACC.2 [Memories] and FDP_IFC.1	Yes, *AUG* ***#4***
	FMT_SMF.1 [Memories]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	Yes, *AUG* ***#4***
FMT_SMF.1 [Memories]	None	No dependency	***No,*** *CCMB-2012-09-002*
FMT_ITC.1 [Loader]	[FDP_ACC.1 [Loader] or FDP_IFC.1]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_MSA.3 [Loader]	Yes	
FDP_ACC.1 [Loader]	FDP_ACF.1 [Loader]	Yes	***No,*** *CCMB-2012-09-002*
FDP_ACF.1 [Loader]	FDP_ACC.1 [Loader]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_MSA.3 [Loader]	Yes	
FMT_MSA.3 [Loader]	FMT_MSA.1 [Loader]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_SMR.1 [Loader]	No, see discussion below	
FMT_MSA.1 [Loader]	[FDP_ACC.1 [Loader] or FDP_IFC.1]	Yes	***No,*** *CCMB-2012-09-002*
	FDP_SMF.1 [Loader]	Yes	
	FDP_SMR.1 [Loader]	No, see discussion below	
FDP_SMF.1 [Loader]	None	No dependency	***No,*** *CCMB-2012-09-002*
FMT_SMR.1 [MIFARE]	FIA_UID.1 [MIFARE]	Yes, by FIA_UID.2 [MIFARE]	***No,*** *CCMB-2012-09-002*
FDP_ACC.1 [MIFARE]	FDP_ACF.1 [MIFARE]	Yes	***No,*** *CCMB-2012-09-002*

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FDP_ACF.1 [MIFARE]	FDP_ACC.1 [MIFARE]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_MSA.3 [MIFARE]	Yes	
FMT_MSA.3 [MIFARE]	FMT_MSA.1 [MIFARE]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_SMR.1 [MIFARE]	Yes	
FMT_MSA.1 [MIFARE]	[FDP_ACC.1 [MIFARE] or FDP_IFC.1]	Yes, by FDP_ACC.1 [MIFARE]	***No,*** *CCMB-2012-09-002*
	FMT_SMF.1 [MIFARE]	Yes	
	FMT_SMR.1 [MIFARE]	Yes	
FMT_SMF.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FDP_ITC.2 [MIFARE]	FDP_ACC.1 [MIFARE] or FDP_IFC.1	Yes, by FDP_ACC.1 [MIFARE]	***No,*** *CCMB-2012-09-002*
	FTP_ITC.1 or FPT_TRP.1 [MIFARE]	Yes, by FPT_TRP.1 [MIFARE]	
	FPT_TDC.1 [MIFARE]	Yes	
FPT_TDC.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FCS_COP.1 [AES/MIFARE]	[FDP_ITC.1 or FDP_ITC.2 [MIFARE] or FCS_CKM.1]	Yes, by FDP_ITC.2 [MIFARE]	***No,*** *CCMB-2012-09-002*
	FCS_CKM.4 [MIFARE]	Yes	
FIA_UID.2 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FIA_UAU.2 [MIFARE]	FIA_UID.1	Yes, by FIA_UID.2 [MIFARE]	***No,*** *CCMB-2012-09-002*
FIA_UAU.5 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FMT_MTD.1 [MIFARE]	FMT_SMR.1 [MIFARE]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_SMF.1 [MIFARE]	Yes	
FPT_TRP.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FCS_CKM.4 [MIFARE]	[FDP_ITC.1 or FDP_ITC.2 [MIFARE] or FCS_CKM.1]	Yes, by FDP_ITC.2 [MIFARE]	***No,*** *CCMB-2012-09-002*
FDP_ROL.1 [MIFARE]	FDP_ACC.1 [MIFARE] or FDP_IFC.1	Yes, by FDP_ACC.1 [MIFARE]	***No,*** *CCMB-2012-09-002*
FPT_RPL.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FPR_UNL.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FPT_TST.1 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*
FRU_RSA.2 [MIFARE]	None	No dependency	***No,*** *CCMB-2012-09-002*

354 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.

355 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.

356 Part 2 of the Common Criteria defines the dependency of "Management of security attributes (FMT_MSA.1) [Loader]" and "Static attribute initialisation (FMT_MSA.3) [Loader]" on "Security roles (FMT_SMR.1) [Loader]". This dependency is considered to be satisfied, because the access control defined for the loader is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a Security Functional Requirement "FMT_SMR.1".

7.4.5 Rationale for the Assurance Requirements

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

357 Regarding application note 21 of *BSI-PP-0035*, this Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

358 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.

359 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

360 Note that detailed and updated refinements for assurance requirements are given in *Section 7.3*.

Dependencies of assurance requirements

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

362 Augmentation to this package are identified in paragraph *290* and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

363 This section demonstrates how the TOE meets each Security Functional Requirement, which will be further detailed in the ADV_FSP documents.

364 The complete TOE summary specification has been presentad and evaluated in the ST33F1M/1M0/896/768/640/512F, SC33F1M0/896/768/640/512/384F, SM33F1M/1M0/896/768/640/512F, SE33F1M/1M0/896/768/640/512F, SL33F1M/1M0/896/768/640/512F, SP33F1MF, with dedicated software revision D or E, optional cryptographic library Neslib 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 - SECURITY TARGET.

365 For confidentiality reasons, the TOE summary specification is not fully reproduced here.

8.1 Limited fault tolerance (FRU_FLT.2)

366 The TSF provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to memory contents, CPU, random number generation and cryptographic operations, thus preventing risk of malfunction.

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

367 The TSF provides preservation of secure state by detecting and managing the following events, resulting in an immediate reset:

- Die integrity violation detection,
- Errors on memories,
- Glitches,
- High voltage supply,
- CPU errors,
- MPU errors,
- External clock incorrect frequency,
- etc..

368 The ES can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1) [Test]

369 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].

8.4 Limited capabilities (FMT_LIM.1) [Issuer]

370 The TSF ensures that the Secure Flash Loader and the final test capabilities are unavailable in USER configuration, in accordance with SFP_4: Limited capability and availability Policy [Issuer].

8.5 Limited availability (FMT_LIM.2) [Test] & [Issuer]

371 The TOE is either in TEST, ISSUER or USER configuration.

372 The only authorised TOE configuration modifications are:

- TEST to ISSUER configuration,
- TEST to USER configuration,
- ISSUER to USER configuration.

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

374 The TSF reduces the available features depending on the TOE configuration.

8.6 Audit storage (FAU_SAS.1)

375 In Issuer 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.

8.7 Resistance to physical attack (FPT_PHP.3)

376 The TSF ensures resistance to physical tampering, thanks to the following features:

- The TOE implements counter-measures that reduce the exploitability of physical probing.
- The TOE is physically protected by an active shield that commands an automatic reaction on die integrity violation detection.

8.8 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1)

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

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment,
- etc..

8.9 Random number generation (FCS_RNG.1)

378 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.

8.10 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES])

379 The TOE provides an EDES accelerator that has the capability to perform DES and Triple DES encryption and decryption conformant to FIPS PUB 46-3.

380 The EDES accelerator offers a Cipher Block Chaining (CBC) mode conformant to ISO/IEC 10116, and a Cipher Block Chaining Message Authentication Code (CBC-MAC) mode conformant to ISO/IEC 9797-1.

8.11 Cryptographic operation: RSA operation (FCS_COP.1 [RSA]) if Neslib only

381 The cryptographic library Neslib provides the RSA public key cryptographic operation for modulus sizes up to 4096 bits, conformant to PKCS #1 V2.1.

382 The cryptographic library Neslib provides the RSA private key cryptographic operation with or without CRT for modulus sizes up to 4096 bits, conformant to PKCS #1 V2.1.

8.12 Cryptographic operation: AES operation (FCS_COP.1 [AES]) if Neslib only

383 The cryptographic library Neslib provides the standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to FIPS PUB 197 with intrinsic counter-measures against timing attacks (TA), fault attacks (FA), SPA, and DPA.

8.13 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1 [ECC]) if Neslib only

384 The cryptographic library Neslib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields, all conformant to IEEE 1363-2000 and IEEE 1363a-2004, including:

- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check.

8.14 Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only

385 The cryptographic library Neslib provides the SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to FIPS PUB 180-1, FIPS PUB 180-2, ISO/IEC 10118-3:1998.

386 The cryptographic library Neslib provides the SHA-1 secure hash function conformant to FIPS PUB 180-1, FIPS PUB 180-2, ISO/IEC 10118-3:1998, and offering resistance against side channel and fault attacks.

8.15 Cryptographic key generation: Prime generation (FCS_CKM.1 [Prime_generation]) & Cryptographic key generation: Protected prime generation (FCS_CKM.1 [Protected_prime_generation]) if Neslib only

387 The cryptographic library Neslib provides prime numbers generation for key sizes up to 2048 bits conformant to FIPS PUB 140-2 and FIPS PUB 186, and offering resistance against side channel and fault attacks.

8.16 Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_key_generation]) & Cryptographic key generation: Protected RSA key generation (FCS_CKM.1 [Protected_RSA_key_generation]) if Neslib only

388 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, and offering resistance against side channel and fault attacks.

8.17 Static attribute initialisation (FMT_MSA.3) [Memories]

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

8.18 Management of security attributes (FMT_MSA.1) [Memories] & Specification of management functions (FMT_SMF.1) [Memories]

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

8.19 Complete access control (FDP_ACC.2) [Memories] & Security attribute based access control (FDP_ACF.1) [Memories]

391 The TOE enforces the dynamic memory protection policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), programmed by the ES. Overriding the MPU set of access rights, the TOE enforces additional protections on specific parts of the memories.

8.20 Import of user data without security attributes (FDP_ITC.1) [Loader]

392 In Issuer configuration, the System Firmware provides the capability of securely loading user data into the NVM (Secure Flash Loader). The ciphered data is automatically

decrypted, before installation in the NVM.
The integrity of the loaded data is systematically checked, and the integrity of the NVM can also be checked by the ES.

8.21 Static attribute initialisation (FMT_MSA.3) [Loader]

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

8.22 Management of security attributes (FMT_MSA.1) [Loader] & Specification of management functions (FMT_SMF.1) [Loader]

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

8.23 Subset access control (FDP_ACC.1) [Loader] & Security attribute based access control (FDP_ACF.1) [Loader]

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

8.24 Security roles (FMT_SMR.1) [MIFARE]

396 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 Administrator, Application Manager, Application User, and Everybody.

8.25 Subset access control (FDP_ACC.1) [MIFARE]

397 For each DESFire command subject to access control, the DESFire library verifies if the DESFire access conditions are satisfied and returns an error when this is not the case.

8.26 Security attribute based access control (FDP_ACF.1) [MIFARE]

398 The DESFire library verifies the DESFire security attributes during the execution of DESFire commands to enforce the Access Control Policy defined by the DESFire interface specification.

8.27 Static attribute initialisation (FMT_MSA.3) [MIFARE]

399 The DESFire library initialises all the static attributes to the values defined by DESFire interface specifications before they can be used by the Embedded Software.

8.28 Management of security attributes (FMT_MSA.1) [MIFARE]

400 The DESFire library verifies the DESFire security attributes during the execution of DESFire commands to enforce the Access Control Policy on the security attributes.

8.29 Specification of Management Functions (FMT_SMF.1) [MIFARE]

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

8.30 Import of user data with security attributes (FDP_ITC.2) [MIFARE]

402 The DESFire library implements the DESFire interface specifications and enforces the Access Control Policy to associate the user data to the security attributes.

8.31 Inter-TSF basic TSF data consistency (FPT_TDC.1) [MIFARE]

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

8.32 Cryptographic operation (FCS_COP.1[AES/MIFARE])

404 The DESFire library uses AES or Triple DES as cryptographic operation, and implements the AES. Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

8.33 Cryptographic key destruction (FCS_CKM.4) [MIFARE]

405 The DESFire library erases key values from memory after their context becomes obsolete.

8.34 User identification before any action (FIA_UID.2) [MIFARE]

406 The DESFire library identifies the user through the key selected for authentication as specified by the DESFire Interface Specification.

8.35 User authentication before any action (FIA_UAU.2) [MIFARE]

407 During the authentication, the DESFire library verifies that the user knows the selected key.

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

8.36 Multiple authentication mechanisms (FIA_UAU.5) [MIFARE]

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

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

8.37 Management of TSF data (FMT_MTD.1) [MIFARE]

411 The DESFire library implements the DESFire Interface Specification, restricting key modifications in ways configurable through the security attributes to authenticated users, or disabling key modification capabilities.

8.38 Trusted path (FTP_TRP.1) [MIFARE]

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

8.39 Basic rollback (FDP_ROL.1) [MIFARE]

413 The DESFire library implements the 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.

8.40 Replay detection (FPT_RPL.1) [MIFARE]

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

8.41 Unlinkability (FPR_UNL.1) [MIFARE]

415 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 DESFire access control - when configured for this purpose - provides traceability protection.

8.42 TSF testing (FPT_TST.1) [MIFARE]

416 The DESFire library performs a code integrity test before starting execution of DESFire commands. This integrity check can also be performed on request of the Embedded Software.

8.43 Minimum and maximum quotas (FRU_RSA.2) [MIFARE]

417 The DESFire library ensures the memory required for its operation is available.

9 References

418 Protection Profile references

Component description	Reference	Revision
Security IC Platform Protection Profile	BSI-PP-0035	1.0

419 SM33Fxxx Security Target reference

Component description	Reference
ST33F1M/1M0/896/768/640/512F, SC33F1M0/896/768/640/512/384F, SM33F1M/1M0/896/768/640/512F, SE33F1M/1M0/896/768/640/512F, SL33F1M/1M0/896/768/640/512F, SP33F1MF, with dedicated software revision D or E, optional cryptographic library Neslib 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 - SECURITY TARGET	SMD_SM33Fxxx_ST_11_001

420 Guidance documentation references

Component description	Reference	Revision
ST33F1M Smartcard MCU and derivatives with ARM SecurCore SC300 CPU - Datasheet	DS_ST33F1M	2
ST33F1M: 90nm CMOS M10 Flash technology die description	DD_33F1M	5
ARM Cortex SC300 r0p0 Technical Reference Manual	ARM DDI 0337	F
ARM SC300 r0p0 SecurCore Technical Reference Manual Supplement 1A	ARM DDI 0337 Supp 1A	A
ARM Cortex M3 r2p0 Technical Reference Manual	ARM DDI 0337 F3c	F3c
ARM SecurCore SC300 technical limitations	ES_SC300	1
ST32/33 System ROM user manual	UM_32_33_SysROM	29
ST33F1M and derivatives Flash loader installation guide	UM_33F1M_FL	5
ST33 platform Security guidance	AN_SECU_33	3
ST33 - AIS31 Compliant Random Number user manual	UM_33_AIS31	1
ST33 - AIS31 Reference implementation - Startup, online and total failure tests - User manual	AN_33_AIS31	1
ST33 uniform timing application note	AN_33_UT	1
ST33 Secure MCU NesLib 3.0 cryptographic library user manual	UM_33_NESLIB_3.0	5

Component description	Reference	Revision
ST33 Secure microcontrollers NesLib 3.2 cryptographic library user manual	UM_33_NESLIB_3.2	2
User Manual MIFARE DESFire EV1 library 1.1	UM_MIFARE_DESFire_EV1	2
Resource sharing on ST33F1M devices - Application note	AN_MFDFEV1_F1M	2
User Manual MIFARE Classic Software library revision 1.4.0	UM_MIFARE_Classic	5
Application Note: How to identify certified HW devices using additional ST traceability information	AN_TRACE	2

421 Standards references

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]	FIPS PUB 46-3	FIPS PUB 46-3, Data encryption standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, 1999
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, U.S. Department of Commerce, 1999
[4]	FIPS PUB 180-1	FIPS PUB 180-1 Secure Hash Standard, National Institute of Standards and Technology, U.S. Department of Commerce,1995
[5]	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
[6]	FIPS PUB 186	FIPS PUB 186 Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S.A., 1994
[7]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[8]	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
[9]	ISO/IEC 9797-1	ISO/IEC 9797, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, ISO, 1999
[10]	ISO/IEC 10116	ISO/IEC 10116, Information technology - Security techniques - Modes of operation of an n-bit block cipher algorithm, ISO, 1997
[11]	ISO/IEC 10118-3:1998	ISO/IEC 10118-3:1998, Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions

Ref	Identifier	Description
[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]	CCMB-2012-09-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012, version 3.1 Revision 4
[14]	CCMB-2012-09-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012, version 3.1 Revision 4
[15]	CCMB-2012-09-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012, version 3.1 Revision 4
[16]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[17]	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
[18]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[19]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[20]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[21]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997

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 13. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI)
ALU	Arithmetical and Logical Unit.
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.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DES	Data Encryption Standard.
DIP	Dual-In-Line Package.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
ES	Security IC Embedded SoftWare.
FIPS	Federal Information Processing Standard.
I/O	Input / Output.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.

Table 13. List of abbreviations (continued)

Term	Meaning
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or Security Target.
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.

10 Revision history

Table 14. Document revision history

Date	Revision	Changes
28-Jun-2012	01.00	Initial release.
27-Aug-2012	01.01	Change of versions: MIFARE DESFire EV1, documents.
08-Oct-2012	02.00	Change of versions: Hardware, Dedicated software, documents. Change in references: CC V3.1 R4, BSI AIS20/AIS31.
29-Nov-2012	02.01	Addition of sites. Change in reference documents.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com