

**ST31 - K330A**  
**version H (dual or contactless mode only),**  
**with optional cryptographic library NESLIB 3.2,**  
**and optional technology MIFARE® DESFire®**  
**EV1 2.2**  
**and optional technology MIFARE® Plus® 1.3**  
**Security Target - Public Version**

Common Criteria for IT security evaluation

SMD\_MR31Zxxx\_ST\_13\_002 Rev 02.02

December 2014



BLANK



# ST31 - K330A Security Target - Public Version

## Common Criteria for IT security evaluation

### 1 Introduction

#### 1.1 Security Target reference

- 1 Document identification: ST31 - K330A version H (dual or contactless mode only), with optional cryptographic library Neslib 3.2, and optional technology MIFARE® DESFire® EV1 2.2, and optional technology MIFARE® Plus® S 1.3 SECURITY TARGET - PUBLIC VERSION.
- 2 Version number: Rev 02.02, issued December 2014.
- 3 Registration: registered at ST Microelectronics under number SMD\_MR31Zxxx\_ST\_13\_002.

#### 1.2 Purpose

- 4 This document presents **the Security Target - Public version (ST)** of the **ST31 - K330A Security Integrated Circuits (IC)**, designed on the **ST31 platform of STMicroelectronics**, with Dedicated Software (DSW), optional cryptographic library **Neslib 3.2**, and optional technology **MIFARE® DESFire® EV1 2.2**, and optional technology **MIFARE® Plus® S 1.3**.
- 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

- 1 Introduction ..... 3**
  - 1.1 Security Target reference ..... 3
  - 1.2 Purpose ..... 3
  
- 2 Context ..... 11**
  
- 3 TOE description ..... 12**
  - 3.1 TOE identification ..... 12
  - 3.2 TOE overview ..... 13
  - 3.3 TOE life cycle ..... 16
  - 3.4 TOE environment ..... 17
    - 3.4.1 TOE Development Environment ..... 17
    - 3.4.2 TOE production environment ..... 18
    - 3.4.3 TOE operational environment ..... 18
  
- 4 Conformance claims ..... 20**
  - 4.1 Common Criteria conformance claims ..... 20
  - 4.2 PP Claims ..... 20
    - 4.2.1 PP Reference ..... 20
    - 4.2.2 PP Additions ..... 20
    - 4.2.3 PP Claims rationale ..... 20
  
- 5 Security problem definition ..... 22**
  - 5.1 Description of assets ..... 22
  - 5.2 Threats ..... 24
  - 5.3 Organisational security policies ..... 27
  - 5.4 Assumptions ..... 29
  
- 6 Security objectives ..... 31**
  - 6.1 Security objectives for the TOE ..... 33
  - 6.2 Security objectives for the environment ..... 37
  - 6.3 Security objectives rationale ..... 38
    - 6.3.1 Assumption "Usage of secure values for MFPlus" ..... 41

6.3.2	Assumption "Terminal support to ensure integrity for MFPlus" . . . . .	41
6.3.3	Assumption "Usage of secure values for DESFire" . . . . .	41
6.3.4	Assumption "Terminal support to ensure integrity and confidentiality for DESFire" . . . . .	42
6.3.5	TOE threat "Memory Access Violation" . . . . .	42
6.3.6	TOE threat "Unauthorised data modification for MFPlus" . . . . .	42
6.3.7	TOE threat "Impersonating authorised users during authentication for MFPlus" . . . . .	42
6.3.8	TOE threat "Cloning for MFPlus" . . . . .	43
6.3.9	TOE threat "MFPlus resource unavailability" . . . . .	43
6.3.10	TOE threat "MFPlus code confidentiality" . . . . .	43
6.3.11	TOE threat "MFPlus data confidentiality" . . . . .	43
6.3.12	TOE threat "MFPlus code integrity" . . . . .	44
6.3.13	TOE threat "MFPlus data integrity" . . . . .	44
6.3.14	TOE threat "Unauthorised data modification for DESFire" . . . . .	44
6.3.15	TOE threat "Impersonating authorised users during authentication for DESFire" . . . . .	44
6.3.16	TOE threat "Cloning for DESFire" . . . . .	45
6.3.17	TOE threat "DESFire resource unavailability" . . . . .	45
6.3.18	TOE threat "DESFire code confidentiality" . . . . .	45
6.3.19	TOE threat "DESFire data confidentiality" . . . . .	45
6.3.20	TOE threat "DESFire code integrity" . . . . .	45
6.3.21	TOE threat "DESFire data integrity" . . . . .	46
6.3.22	Organisational security policy "Additional Specific Security Functionality" . . . . .	46
6.3.23	Organisational security policy "Integrity during communication for MFPlus" . . . . .	46
6.3.24	Organisational security policy "Un-traceability of end-users for MFPlus" . . . . .	47
6.3.25	Organisational security policy "Confidentiality during communication for DESFire" . . . . .	47
6.3.26	Organisational security policy "Transaction mechanism for DESFire" . . . . .	47
6.3.27	Organisational security policy "Un-traceability of end-users for DESFire" . . . . .	48
6.3.28	Organisational security policy "Usage of hardware platform" . . . . .	48
6.3.29	Organisational security policy "Treatment of user data" . . . . .	48
<b>7</b>	<b>Security requirements . . . . .</b>	<b>49</b>
7.1	Security functional requirements for the TOE . . . . .	49

- 7.1.1 Security Functional Requirements from the Protection Profile ..... 53
- 7.1.2 Additional Security Functional Requirements for the cryptographic services ..... 55
- 7.1.3 Additional Security Functional Requirements for the memories protection ..... 57
- 7.1.4 Additional Security Functional Requirements related to MFPlus ..... 58
- 7.1.5 Additional Security Functional Requirements related to DESFire ..... 63
- 7.1.6 Additional Security Functional Requirements common to DESFire and MFPlus ..... 69
- 7.2 TOE security assurance requirements ..... 70
- 7.3 Refinement of the security assurance requirements ..... 71
  - 7.3.1 Refinement regarding functional specification (ADV\_FSP) ..... 72
  - 7.3.2 Refinement regarding test coverage (ATE\_COV) ..... 73
- 7.4 Security Requirements rationale ..... 73
  - 7.4.1 Rationale for the Security Functional Requirements ..... 73
  - 7.4.2 Additional security objectives are suitably addressed ..... 74
  - 7.4.3 Additional security requirements are consistent ..... 80
  - 7.4.4 Dependencies of Security Functional Requirements ..... 83
  - 7.4.5 Rationale for the Assurance Requirements ..... 88
- 8 TOE summary specification ..... 89**
  - 8.1 Limited fault tolerance (FRU\_FLT.2) ..... 89
  - 8.2 Failure with preservation of secure state (FPT\_FLS.1) ..... 89
  - 8.3 Limited capabilities (FMT\_LIM.1) ..... 89
  - 8.4 Limited availability (FMT\_LIM.2) ..... 89
  - 8.5 Audit storage (FAU\_SAS.1) ..... 90
  - 8.6 Resistance to physical attack (FPT\_PHP.3) ..... 90
  - 8.7 Basic internal transfer protection (FDP\_ITT.1), Basic internal TSF data transfer protection (FPT\_ITT.1) & Subset information flow control (FDP\_IFC.1) ..... 90
  - 8.8 Random number generation (FCS\_RNG.1) ..... 90
  - 8.9 Cryptographic operation: DES / 3DES operation (FCS\_COP.1 [EDES]) . 90
  - 8.10 Cryptographic operation: AES operation (FCS\_COP.1 [AES]) ..... 91
  - 8.11 Cryptographic operation: RSA operation (FCS\_COP.1 [RSA]) if Neslib only ..... 91
  - 8.12 Cryptographic operation: Elliptic Curves Cryptography operation (FCS\_COP.1 [ECC]) if Neslib only ..... 91

8.13	Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only .....	91
8.14	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 ..	92
8.15	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	92
8.16	Static attribute initialisation (FMT_MSA.3) [Memories] .....	92
8.17	Management of security attributes (FMT_MSA.1) [Memories] & Specification of management functions (FMT_SMF.1) [Memories] .....	92
8.18	Complete access control (FDP_ACC.2) [Memories] & Security attribute based access control (FDP_ACF.1) [Memories] .....	92
8.19	Security roles (FMT_SMR.1) [MFPlus] .....	92
8.20	Subset access control (FDP_ACC.1) [MFPlus] .....	93
8.21	Security attribute based access control (FDP_ACF.1) [MFPlus] .....	93
8.22	Static attribute initialisation (FMT_MSA.3) [MFPlus] .....	93
8.23	Management of security attributes (FMT_MSA.1) [MFPlus] .....	93
8.24	Specification of Management Functions (FMT_SMF.1) [MFPlus] .....	94
8.25	Import of user data with security attributes (FDP_ITC.2) [MFPlus] .....	94
8.26	Inter-TSF basic TSF data consistency (FPT_TDC.1) [MFPlus] .....	94
8.27	Cryptographic key destruction (FCS_CKM.4) [MFPlus] .....	94
8.28	User identification before any action (FIA_UID.2) [MFPlus] .....	94
8.29	User authentication before any action (FIA_UAU.2) [MFPlus] .....	94
8.30	Multiple authentication mechanisms (FIA_UAU.5) [MFPlus] .....	94
8.31	Management of TSF data (FMT_MTD.1) [MFPlus] .....	94
8.32	Trusted path (FTP_TRP.1) [MFPlus] .....	95
8.33	Replay detection (FPT_RPL.1) [MFPlus] .....	95
8.34	Unlinkability (FPR_UNL.1) [MFPlus] .....	95
8.35	Minimum and maximum quotas (FRU_RSA.2) [MFPlus] .....	95
8.36	Subset residual information protection (FDP_RIP.1) [MFPlus] .....	95
8.37	Security roles (FMT_SMR.1) [DESFire] .....	95
8.38	Subset access control (FDP_ACC.1) [DESFire] .....	95
8.39	Security attribute based access control (FDP_ACF.1) [DESFire] .....	95
8.40	Static attribute initialisation (FMT_MSA.3) [DESFire] .....	96

8.41	Management of security attributes (FMT_MSA.1) [DESFire]	96
8.42	Specification of Management Functions (FMT_SMF.1) [DESFire]	96
8.43	Import of user data with security attributes (FDP_ITC.2) [DESFire]	96
8.44	Inter-TSF basic TSF data consistency (FPT_TDC.1) [DESFire]	96
8.45	Cryptographic key destruction (FCS_CKM.4) [DESFire]	96
8.46	User identification before any action (FIA_UID.2) [DESFire]	96
8.47	User authentication before any action (FIA_UAU.2) [DESFire]	96
8.48	Multiple authentication mechanisms (FIA_UAU.5) [DESFire]	97
8.49	Management of TSF data (FMT_MTD.1) [DESFire]	97
8.50	Trusted path (FTP_TRP.1) [DESFire]	97
8.51	Basic rollback (FDP_ROL.1) [DESFire]	97
8.52	Replay detection (FPT_RPL.1) [DESFire]	97
8.53	Unlinkability (FPR_UNL.1) [DESFire]	97
8.54	TSF testing (FPT_TST.1) [DESFire]	97
8.55	Minimum and maximum quotas (FRU_RSA.2) [DESFire]	97
8.56	Subset residual information protection (FDP_RIP.1) [DESFire]	98
8.57	Subset access control (FDP_ACC.1) [MIFARE_FWL] & Security attribute based access control (FDP_ACF.1) [MIFARE_FWL]	98
8.58	Static attribute initialisation (FMT_MSA.3) [MIFARE_FWL]	98
<b>9</b>	<b>References</b>	<b>99</b>
<b>Appendix A</b>	<b>Glossary</b>	<b>102</b>
A.1	Terms	102
A.2	Abbreviations	104
<b>10</b>	<b>Revision history</b>	<b>106</b>



## List of tables

Table 1.	TOE identification	12
Table 2.	Derivative devices configuration possibilities	12
Table 3.	Composite product life cycle phases	17
Table 4.	Summary of security environment	23
Table 5.	Summary of security objectives	32
Table 6.	Security Objectives versus Assumptions, Threats or Policies	39
Table 7.	Summary of functional security requirements for the TOE	49
Table 8.	FCS_COP.1 iterations (cryptographic operations)	55
Table 9.	FCS_CKM.1 iterations (cryptographic key generation)	57
Table 10.	TOE security assurance requirements	70
Table 11.	Impact of EAL5 selection on <a href="#">BSI-PP-0035</a> refinements	72
Table 12.	Dependencies of security functional requirements	83
Table 13.	List of abbreviations	104
Table 14.	Document revision history	106

## List of figures

Figure 1. ST31 - K330A block diagram ..... 16

## 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 assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented by ASE\_TSS.2, ALC\_DVS.2 and AVA\_VAN.5.
- 9 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE security ICs, and to summarise their chosen TSF services and assurance measures.
- 10 This ST claims to be an instantiation of the "[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.
- 11 Extensions introduced in this ST to the SFRs of the Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.
- 12 This ST makes various refinements to the above mentioned PP and [AUG](#). They are all properly identified in the text typeset as **indicated here**. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: **BSI** for [BSI-PP-0035](#), **AUG1** for Addition #1 of [AUG](#) and **AUG4** for Addition #4 of [AUG](#).

### 3 TOE description

#### 3.1 TOE identification

13 The Target of Evaluation (TOE) is the ST31 - K330A version H (dual or contactless mode only), with the optional cryptographic library Neslib 3.2, and/or the optional library MIFARE® DESFire® EV1 2.2, and optional technology MIFARE® Plus® S 1.3, with guidance documentation.

**Table 1. TOE identification**

IC Maskset name	Maskset Major version	IC version	Master identification number <sup>(1)</sup>	OST name <sup>(1)</sup>	OST version <sup>(1)</sup>	Optional Neslib crypto library version <sup>(2)</sup>	Optional MIFARE DESFire EV1 version <sup>(3)</sup>	Optional MIFARE Plus S version <sup>(4)</sup>
K330	A	H	0033h	YGE	1.4	3.2	2.2	1.3

1. Part of the product information.
2. See the Neslib User Manual referenced in [Section 9](#).
3. See the MIFARE DESFire EV1 User Manual referenced in [Section 9](#).
4. See the MIFARE Plus S User Manual referenced in [Section 9](#).

- 14 The IC maskset name is the product hardware identification.  
The maskset major version is updated when the full maskset is changed (i.e. all layers of the maskset are changed at the same time).  
The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST software.  
The maskset name with major version and IC version (i.e. K330A version H) fully identify the IC (hardware and OST).
- 15 The K330A version H, is dedicated to Dual mode or contactless mode only. The 1.8V voltage range is deactivated.
- 16 Different derivative devices may be configured by ST during the manufacturing or packaging process, depending on the customer needs. They all share the same hardware design and the same maskset.
- 17 The configuration of the derivative devices can impact the I/O mode, the available NVM memory size, the availability of Nescrypt and the availability of MIFARE support features, as detailed here below:

**Table 2. Derivative devices configuration possibilities**

Features	Possible values
I/O mode	Dual mode, Contactless only
NVM size	52 Kbytes, 38 Kbytes, 22 Kbytes, 16 Kbytes
Nescrypt	Active, Inactive
MIFARE support	Active, Inactive

- 18 All combinations of different features values are possible and covered by this certification. All possible configurations can vary under a unique IC (i.e. K330A), and without impact on security.
- 19 The Master identification number is unique for all product configurations. Each derivative device has a specific Child product identification number, also part of the product information, and specified in the Data Sheet, referenced in [Section 9](#).
- 20 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in [Table 1: TOE identification](#), and the configuration elements as detailed in the Data Sheet, referenced in [Section 9](#).
- 21 In this Security Target, the term "DESFire" means MIFARE® DESFire® EV1 2.2.
- 22 In this Security Target, the term "MFPlus" means MIFARE® Plus® S 1.3.
- 23 The rest of this document applies to all possible configurations of the TOE, with or without Neslib, or MIFARE libraries, except when a restriction is mentioned. For easier reading, the restrictions are typeset as [indicated here](#).

## 3.2 TOE overview

- 24 Designed for secure ID and banking applications, the TOE is a serial access microcontroller that incorporates the most recent generation of ARM® processors for embedded secure systems. Its SecurCore® SC000™ 32-bit RISC core is built on the Cortex™ M0 core with additional security features to help to protect against advanced forms of attacks.
- 25 The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks. The AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. The 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (DES [\[2\]](#)), enabling Cipher Block Chaining (CBC) mode, fast DES and triple DES computation. If [Nescrypt is active](#), the NESCRYPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([\[4\]](#), [\[8\]](#), [\[12\]](#), [\[18\]](#),[\[19\]](#), [\[20\]](#), [\[21\]](#)).
- As randomness is a key stone in many applications, the ST31 - K330A features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS31 [\[1\]](#) and directly accessible thru dedicated registers.
- This device also includes the ARM® SecurCore® SC000™ memory protection unit (MPU), which enables the user to define its own region organization with specific protection and access permissions.
- 26 The TOE offers a contact serial communication interface fully compatible with the ISO/IEC 7816-3 standard, and a contactless interface including an RF Universal Asynchronous Receiver Transmitter (RF UART), enabling communication up to 848 Kbits/s compatible with the ISO/IEC 14443 Type A, B and B', and PayPass™ standards. These interfaces can be used simultaneously (dual mode), or the contact interface can be deactivated (see [Table 2: Derivative devices configuration possibilities](#)).

- 27 In a few words, the ST31 - K330A 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,
  - Hardware Security AES accelerator,
  - True Random Number Generator,
  - ISO 3309 CRC calculation block,
  - Memory Protection Unit,
  - optional NExt Step CRYPTography accelerator (NESCRYPT),
  - optional cryptographic library,
  - optional MIFARE support,
  - optional secure MIFARE® DESFire® EV1 library,
  - optional secure MIFARE® Plus® S library.
- 28 The TOE includes in the ST protected 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.
- 29 The Security IC Embedded Software (ES) is in User ROM.
- The ES is not part of the TOE and is out of scope of the evaluation, except Neslib MIFARE DESFire EV1, and MIFARE Plus S when they are embedded.**
- 30 The TOE optionally comprises a specific application in User ROM: this applicative Embedded Software is a cryptographic library called Neslib. Neslib is a cutting edge cryptographic library in terms of security and performance.
- Neslib is embedded by the ES developer in his applicative code.  
Note that Neslib can only be used if [Nescrypt is active](#).
- 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 [\[4\]](#)),
  - prime number generation [\[6\]](#).
- Note that the AES support module provided by Neslib is **not in the scope of this evaluation**.
- 31 The TOE optionally comprises a specific application in User ROM: this applicative Embedded Software is a MIFARE technology library.  
This library may be a secure library called MIFARE® DESFire® EV1. DESFire features a mutual three pass authentication, a data encryption on RF channel, and a flexible self-securing file system.

This library may be a secure library called MIFARE® Plus® S. MFPlus features AES authentication, data encryption on RF channel, potential for multiple instances of the file system consisting of 16byte blocks arranged into sectors with each sector having its own access control keys and conditions.

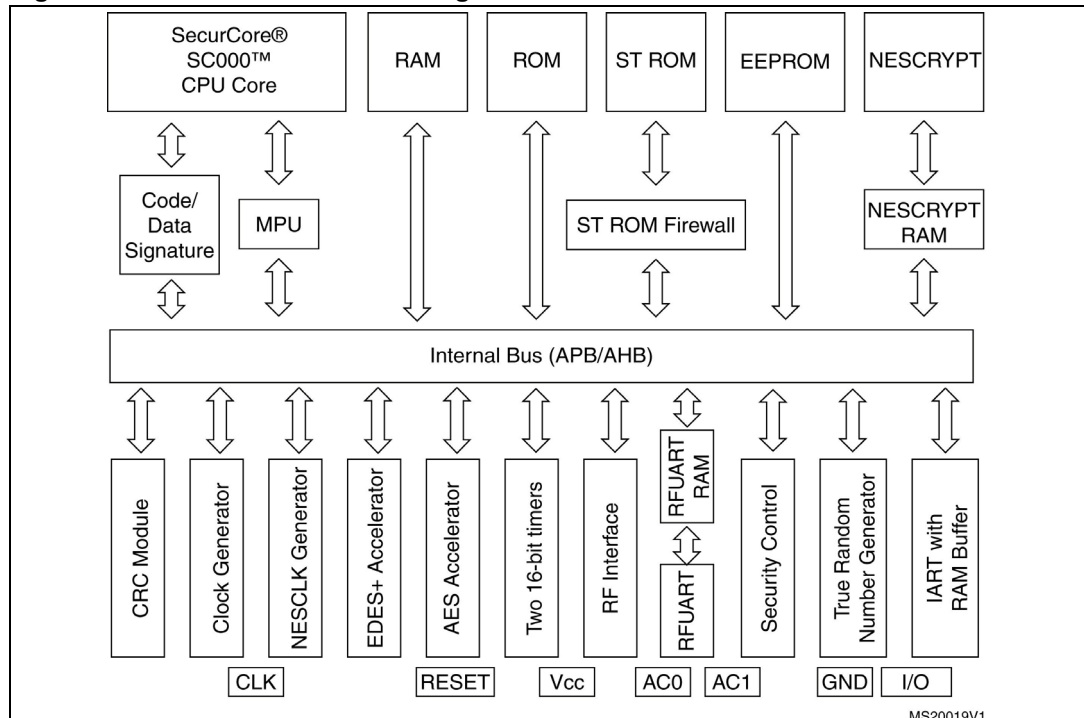
DESFire or MFPlus is embedded by the ES developer in his applicative code.

DESFire and MFPlus do not coexist on the TOE.

Note that DESFire and MFPlus can only be used if [Nescrypt and MIFARE support are active](#).

- 32 In MFPlus, the card is in one (of in total three) security levels. The main features of each security level are listed below:
- Security level 0: The card does not provide any functionality besides initialization. The card is initialized in plaintext, especially keys for the further levels can be brought in. A card in security level 0 is not usable for other purposes. After all mandatory keys and security attributes have been stored in the card, it can be switched to security level 1.
  - Security level 1: The card user can access the blocks in the card after an authentication procedure. The communication with the terminal is protected, however the authentication and the protected communication in the security level are not evaluated security services of the TOE. It can be switched to security level 3 if an authentication using the AES algorithm with the necessary key is performed.
  - Security level 3: The card user can access the data blocks in the card via an adequate card terminal after an authentication procedure based on the AES algorithm. The communication with the card terminal can be protected by using a message authentication code (MAC). The authentication and the MAC are security services of the TOE. The TOE cannot be switched to a different security level.
- 33 The Security levels 0 and 1 are outside the scope of this evaluation. Thus, MFPlus must be in Security level 3 on the field (Phase 7).  
In all security levels, the TOE does additionally support the so-called originality function which allows verifying the authenticity of the TOE.
- 34 The user guidance documentation, part of the TOE, consists of:
- the product Data Sheet and die description,
  - the product family Security Guidance,
  - the AIS31 user manuals,
  - the product family programming manual,
  - the ARM SC000 Technical Reference Manual,
  - optionally the Neslib user manual,
  - optionally the MIFARE DESFire EV1 user manual,
  - optionally the MIFARE Plus S user manual.
- 35 The complete list of guidance documents is detailed in [Section 9](#).
- 36 In addition, the ROM of the tested samples contains an operating system called "Card Manager" that allows the evaluators to use a set of commands with the I/O or in RF mode, and to load in EEPROM (or in RAM) test software. The card manager is not part of the TOE, and not in the scope of this evaluation. It will not be present on the field (Phase 7).
- 37 [Figure 1](#) provides an overview of the ST31 - K330A.

Figure 1. ST31 - K330A block diagram



### 3.3 TOE life cycle

38 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.

39 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.

40 The life cycle phases are summarized in [Table 3](#).

41 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.

42 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.

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

44 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.

45 The TOE is delivered in 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: <b>ST</b>
3	IC manufacturing	integration and photomask fabrication IC production IC testing pre-personalisation	IC manufacturer: <b>ST</b>
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary	IC packaging manufacturer: <b>ST</b> or <b>NEDCARD</b> or <b>SMARTFLEX</b> or <b>DISCO</b>
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

### 3.4 TOE environment

46 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

47 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.

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

49 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).

- 50 The development centres involved in the development of the TOE are the following: **ST ROUSSET (FRANCE)**, **ST ANG MO KIO (SINGAPORE)**, **ST SOPHIA (FRANCE)**, **ST GRENOBLE (FRANCE)**, **ST RENNES (FRANCE)**, **CMP GEORGES CHARPACK (FRANCE)** and **ST ZAVENTEM (BELGIUM)**.
- 51 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).
- 52 The authorized sub-contractors involved in the TOE mask manufacturing can be **DNP (JAPAN)** and **DPE (ITALY)**.

### 3.4.2 TOE production environment

- 53 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.
- 54 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.
- 55 The authorized front-end plant involved in the manufacturing of the TOE can be **ST ROUSSET (FRANCE)** or **ST CROLLES (FRANCE)**.
- 56 The authorized EWS plant involved in the testing of the TOE can be **ST ROUSSET (FRANCE)** or **ST TOA PAYOH (SINGAPORE)**.
- 57 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.
- 58 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)**, **ST CALAMBA (THE PHILIPPINES)**, **ST SHENZEN (CHINA)**, **ST ANG MO KIO (SINGAPORE)**, **NEDCARD (THE NETHERLANDS)**, **DISCO (GERMANY)** or **SMARTFLEX (SINGAPORE)**.
- 59 All ST back-end plants, **ST LOYANG (SINGAPORE)** and **ST ROUSSET (FRANCE)** can be involved for the logistics.

### 3.4.3 TOE operational environment

- 60 A TOE operational environment is the environment of phases 1, optionally 4, then 5 to 7.
- 61 At phases 1, 4, 5 and 6, the TOE operational environment is a controlled environment.
- 62 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

- 63 The ST31 - K330A Security Target claims to be conformant to the Common Criteria version 3.1 revision 4.
- 64 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 \(BSI-PP-0035\)](#).
- 65 The assurance level for the ST31 - K330A Security Target is **EAL 5** augmented by ASE\_TSS.2, ALC\_DVS.2 and AVA\_VAN.5.

### 4.2 PP Claims

#### 4.2.1 PP Reference

- 66 The ST31 - K330A Security Target claims strict conformance to the [Security IC Platform Protection Profile \(BSI-PP-0035\)](#), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

#### 4.2.2 PP Additions

- 67 The main additions operated on the [BSI-PP-0035](#) are:
- Addition #4: “Area based Memory Access Control” from [AUG](#),
  - Addition #1: “Support of Cipher Schemes” from [AUG](#),
  - Specific additions for DESFire and MFPlus,
  - Refinement of assurance requirements.
- 68 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](#).
- 69 The security environment additions relative to the PP are summarized in [Table 4](#).
- 70 The additional security objectives relative to the PP are summarized in [Table 5](#).
- 71 A simplified presentation of the TOE Security Policy (TSP) is added.
- 72 The additional SFRs for the TOE relative to the PP are summarized in [Table 7](#).
- 73 The additional SARs relative to the PP are summarized in [Table 10](#).

#### 4.2.3 PP Claims rationale

- 74 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.
- 75 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](#).

- 76 The security problem definition presented in [Section 5](#), clearly shows the additions to the security problem statement of the PP.
- 77 The security objectives rationale presented in [Section 6.3](#) clearly identifies modifications and additions made to the rationale presented in the [BSI-PP-0035](#).
- 78 Similarly, the security requirements rationale presented in [Section 7.4](#) has been updated with respect to the protection profile.
- 79 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

80 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.

81 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 ones introduced in this Security Target, are detailed in the following sections.

82 A summary of all these security aspects and their respective conditions is provided in [Table 4](#).

### 5.1 Description of assets

83 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.

84 The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks and product in any form,
- the TOE correct operation,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software,
- the cryptographic co-processors for Triple-DES and AES, the random number generator,
- when *DESFire* is embedded, the special functions for the communication with an external interface device,
- 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.

85 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.

**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-MFPlus	Unauthorised data modification for MFPlus
	T.Impersonate-MFPlus	Impersonating authorised users during authentication for MFPlus
	T.Cloning-MFPlus	Cloning for MFPlus
	T.Confid-Applic-Code-MFPlus	MFPlus code confidentiality
	T.Confid-Applic-Data-MFPlus	MFPlus data confidentiality
	T.Integ-Applic-Code-MFPlus	MFPlus code integrity
	T.Integ-Applic-Data-MFPlus	MFPlus data integrity
	T.Application-Resource-MFPlus	MFPlus resource unavailability
	T.Data-Modification-DESFire	Unauthorised data modification for DESFire
	T.Impersonate-DESFire	Impersonating authorised users during authentication for DESFire
	T.Cloning-DESFire	Cloning for DESFire
	T.Confid-Applic-Code-DESFire	DESFire code confidentiality
	T.Confid-Applic-Data-DESFire	DESFire data confidentiality
	T.Integ-Applic-Code-DESFire	DESFire code integrity
	T.Integ-Applic-Data-DESFire	DESFire data integrity
	T.Resource-DESFire	DESFire resource unavailability

**Table 4. Summary of security environment**

	Label	Title
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
	P.MAC	Integrity during communication for MFPlus
	P.No-Trace-MFPlus	Un-traceability of end-users for MFPlus
	P.Confidentiality	Confidentiality during communication for DESFire
	P.Transaction	Transaction mechanism for DESFire
	P.No-Trace-DESFire	Un-traceability of end-users for DESFire
	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-MFPlus	Usage of secure values for MFPlus
	A.Terminal-Support-MFPlus	Terminal support to ensure integrity for MFPlus
	A.Secure-Values-DESFire	Usage of secure values for DESFire
	A.Terminal-Support-DESFire	Terminal support to ensure integrity and confidentiality for DESFire

## 5.2 Threats

86 The threats are described in the [BSI-PP-0035](#), section 3.2. Only those originating in [AUG](#) and those related to DESFire and MFPlus 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.

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

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

**T.Impersonate-MFPlus** Impersonating authorised users during authentication for MFPlus:  
 An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the middle or replay attack.

**T.Cloning-MFPlus** Cloning for MFPlus:  
 All data stored on the TOE (including keys) may be read out in order to create a duplicate.

**T.Confid-Applic-Code-MFPlus** MFPlus code confidentiality:  
 MIFARE Plus Licensed product code must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the MIFARE Plus licensed product executable code is stored.  
 The attacker executes an application to disclose code belonging to MIFARE Plus Licensed product.

T.Confid-Applic-Data-MFPlus	<p>MFPlus data confidentiality:</p> <p>MIFARE Plus Licensed product data must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the MIFARE Plus licensed product data by another application. For example, the attacker executes an application that tries to read data belonging to MIFARE Plus Licensed product.</p>
T.Integ-Applic-Code-MFPlus	<p>MFPlus code integrity:</p> <p>MIFARE Plus 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 Plus licensed product executable code is stored and executed. The attacker executes an application that tries to alter (part of) the MIFARE Plus Licensed product code.</p>
T.Integ-Applic-Data-MFPlus	<p>MFPlus data integrity:</p> <p>MIFARE Plus Licensed product data must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the MIFARE Plus Licensed product data by another application. The attacker executes an application that tries to alter (part of) the MIFARE Plus Licensed product data.</p>
T.Application-Resource-MFPlus	<p>MFPlus resource unavailability:</p> <p>The availability of resources for the MIFARE Plus Licensed product shall be controlled to prevent denial of service or malfunction. An attacker prevents correct execution of MIFARE Plus through consumption of some resources of the card: e.g. RAM or non volatile RAM.</p>
88	<p>The following additional threats are related to DESFire. They are valid in case <b>DESFire</b> is embedded in the TOE.</p>
T.Data-Modification-DESFire	<p>Unauthorised data modification for DESFire:</p> <p>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.</p>
T.Impersonate-DESFire	<p>Impersonating authorised users during authentication for DESFire:</p> <p>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.</p>
T.Cloning-DESFire	<p>Cloning for DESFire:</p> <p>User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.</p>

T.Confid-Applic-Code- DESFire	DESFire code confidentiality:  MIFARE DESFire EV1 Licensed product code must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the MIFARE DESFire EV1 licensed product executable code is stored. The attacker executes an application to disclose code belonging to MIFARE DESFire EV1 Licensed product.
T.Confid-Applic-Data- DESFire	DESFire data confidentiality:  MIFARE DESFire EV1 Licensed product data must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the MIFARE DESFire EV1 licensed product data by another application. For example, the attacker executes an application that tries to read data belonging to MIFARE DESFire EV1 Licensed product.
T.Integ-Applic-Code- DESFire	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.Integ-Applic-Data- DESFire	DESFire data integrity:  MIFARE DESFire EV1 Licensed product data must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the MIFARE DESFire EV1 Licensed product data by another application. The attacker executes an application that tries to alter (part of) the DESFire EV1 Licensed product data.
T.Resource-DESFire	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

- 89 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.
- 90 ST applies the Protection policy during TOE Development and Production (*BSI.P.Process-TOE*) as specified below.
- 91 **ST** applies the Additional Specific Security Functionality policy (*AUG1.P.Add-Functions*) as specified below.
- 92 New Organisational Security Policies (OSPs) are defined here below:

- 93 P.Confidentiality, P.Transaction and P.No-Trace-DESFire are related to **DESFire**, and valid in case DESFire is embedded in the TOE.
- 94 P.MAC and P.No-Trace-MFPlus are related to **MFPlus**, and valid in case MFPlus is embedded in the TOE.
- 95 P.Plat-Appl and P.Resp-Appl are related to the ES that is part of the evaluation (**Neslib** and/or **DESFire** and/or **MFPlus**), and valid in case Neslib or DESFire or MFPlus are embedded 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),
- **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.MAC** Integrity during communication for MFPlus:

The TOE shall provide the possibility to protect the contact-less communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session.

**P.No-Trace-MFPlus** Un-traceability of end-users for MFPlus:

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.Confidentiality** Confidentiality during communication for DESFire:

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

P.Transaction	Transaction mechanism for DESFire:  The TOE shall provide the possibility to combine a number of data modification operations in one transaction, so that either all operations or no operation at all is performed.
P.No-Trace-DESFire	Un-traceability of end-users for DESFire:  The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised subjects without consent. Tracing of end-users may happen by performing a contact-less communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element.
P.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 <a href="#">BSI-PP-0035</a> .
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 <a href="#">BSI-PP-0035</a> .

## 5.4 Assumptions

96 The following 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

97 The following assumptions are defined for DESFire or MFPlus 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.

98 In consequence, the addition of these assumptions does not contradict with the strict conformance claim on the [BSI-PP-0035](#).

99 The following assumptions are valid in case [MFPlus](#) is embedded in the TOE.

A.Secure-Values-MFPlus Usage of secure values for MFPlus:  
  
Only confidential and secure keys shall be used to set up the authentication and access rights in MFPlus. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal-Support-MFPlus Terminal support to ensure integrity for MFPlus:  
  
The terminal verifies information sent by the TOE in order to ensure integrity of the communication.

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

A.Secure-Values-  
DESFire

Usage of secure values for DESFire:

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-  
DESFire

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.

## 6 Security objectives

- 101 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.
- 102 A summary of all security objectives is provided in [Table 5](#).
- 103 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	<b>Dynamic</b> Area based Memory Access Control
	O.Access-Control-MFPlus	Access Control for MFPlus
	O.Authentication-MFPlus	Authentication for MFPlus
	O.MAC-MFPlus	MFPlus integrity-protected Communication
	O.No-Trace-MFPlus	Preventing Traceability for MFPlus
	O.Plat-Appl-MFPlus	Usage of hardware platform for MFPlus
	O.Resp-Appl-MFPlus	Treatment of user data for MFPlus
	O.Resource-MFPlus	Resource availability for MFPlus
	O.Firewall-MFPlus	MFPlus firewall
	O.Shr-Var-MFPlus	MFPlus data cleaning for resource sharing
	O.Verification-MFPlus	MFPlus code integrity check
	O.Access-Control-DESFire	Access Control for DESFire
	O.Authentication-DESFire	Authentication for DESFire
	O.Confidentiality-DESFire	DESFire Confidential Communication
	O.Type-Consistency-DESFire	DESFire Data type consistency
	O.Transaction-DESFire	DESFire Transaction mechanism
	O.No-Trace-DESFire	Preventing Traceability for DESFire
	O.Plat-Appl-DESFire	Usage of hardware platform for DESFire
	O.Resp-Appl-DESFire	Treatment of user data for DESFire
	O.Resource-DESFire	Resource availability for DESFire
	O.Firewall-DESFire	DESFire firewall
	O.Shr-Res-DESFire	DESFire data cleaning for resource sharing
	O.Verification-DESFire	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.Secure-Values-MFPlus	Generation of secure values for MFPlus
	OE.Terminal-Support-MFPlus	Terminal support to ensure integrity for MFPlus
	OE.Secure-Values-DESFire	Generation of secure values for DESFire
	OE.Terminal-Support-DESFire	Terminal support to ensure integrity and confidentiality for DESFire

## 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	<p>Additional Specific Security Functionality:            The TOE must provide the following specific security functionality to the <b>Security IC</b> Embedded Software:</p> <ul style="list-style-type: none"> <li>– Data Encryption Standard (DES),</li> <li>– Triple Data Encryption Standard (3DES),</li> <li>– Advanced Encryption Standard (AES),</li> <li>– <i>Elliptic Curves Cryptography on GF(p)</i>, if Neslib is embedded only,</li> <li>– <i>Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)</i>, if Neslib is embedded only,</li> <li>– Rivest-Shamir-Adleman (RSA), if Neslib is embedded only,</li> <li>– <i>Prime Number Generation</i>, if Neslib is embedded only.</li> </ul>
AUG4.O.Mem-Access	<p><b>Dynamic</b> Area based Memory Access Control:            The TOE must provide the <b>Security IC</b> Embedded Software with the capability to define <b>dynamic memory segmentation and protection</b>. The TOE must then enforce <b>the defined access rules</b> so that access of software to memory areas is controlled as required, for example, in a multi-application environment.</p>

104

The following objectives are only valid in case MFPlus is embedded:

- O.Access-Control-MFPlus    Access Control for MFPlus:  
The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to all operations for data elements and to reading and modifying security attributes as well as authentication data. The cryptographic keys used for authentication shall never be output.
- O.Authentication-MFPlus    Authentication for MFPlus:  
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.MAC-MFPlus                MFPlus integrity-protected Communication:  
The TOE must be able to protect the communication by adding a MAC. This shall be mandatory for commands that modify data on the TOE and optional on read commands. In addition, a security attribute shall be available to mandate MAC on read commands, too. Usage of the protected communication shall also support the detection of injected and bogus commands within the communication session before the protected data transfer.
- O.No-Trace-MFPlus          Preventing Traceability for MFPlus:  
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 privacy-related information that is suitable for tracing an end-user by an unauthorised subject.
- O.Plat-Appl-MFPlus         Usage of hardware platform for MFPlus:  
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-MFPlus        Treatment of user data for MFPlus:  
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-MFPlus          Resource availability for MFPlus:  
The TOE shall control the availability of resources for MIFARE Plus Licensed product.

---

O.Firewall-MFPlus	MFPlus firewall : The TOE shall ensure isolation of data and code between MIFARE Plus and the other applications. An application shall not read, write, compare any piece of data or code belonging to the MIFARE Plus Licensed product.
O.Shr-Var-MFPlus	MFPlus data cleaning for resource sharing: It shall be ensured that any hardware resource, that is shared by MIFARE Plus and other applications or by any application which has access to such hardware resource, is always cleaned (using code that is part of the MIFARE Plus system and its certification) whenever MIFARE Plus 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 contactless interface. For example, no data shall remain in a hardware cryptographic coprocessor when MIFARE Plus is interrupted by another application. The cleaning must be done such that no information is leaking from this cleaning process allowing for among others timing or SPA/DPA attacks.
O.Verification-MFPlus	MFPlus code integrity check: The TOE shall ensure that MIFARE Plus code is verified for integrity and authenticity prior being executed.
105	The following objectives are only valid in case <b>DESFire</b> is embedded:
O.Access-Control-DESFire	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-DESFire	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	<p>DESFire Confidential Communication:</p> <p>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.</p>
O.Type-Consistency-DESFire	<p>DESFire Data type consistency:</p> <p>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.</p>
O.Transaction-DESFire	<p>DESFire Transaction mechanism:</p> <p>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.</p>
O.No-Trace-DESFire	<p>Preventing Traceability for DESFire:</p> <p>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.</p>
O.Plat-Appl-DESFire	<p>Usage of hardware platform for DESFire:</p> <p>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.</p>
O.Resp-Appl-DESFire	<p>Treatment of user data for DESFire:</p> <p>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.</p> <p>For example the Security IC Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.</p>
O.Resource-DESFire	<p>Resource availability for DESFire:</p> <p>The TOE shall control the availability of resources for MIFARE DESFire EV1 Licensed product.</p>
O.Firewall-DESFire	<p>DESFire firewall:</p> <p>The TOE shall ensure isolation of data and code between MIFARE DESFire EV1 and the other applications. An application shall not read, write, compare any piece of data or code belonging to the MIFARE DESFire EV1 Licensed product.</p>

O.Shr-Res-DESFire	<p>DESFire data cleaning for resource sharing:</p> <p>It shall be ensured that any hardware resource, that is shared by MIFARE DESFire EV1 and other applications or by any application which has access to such hardware resource, is always cleaned (using code that is part of the MIFARE DESFire EV1 system and its certification) whenever MIFARE DESFire EV1 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 contactless interface.</p> <p>For example, no data shall remain in a hardware cryptographic coprocessor when MIFARE DESFire EV1 is interrupted by another application.</p>
O.Verification-DESFire	<p>DESFire code integrity check:</p> <p>The TOE shall ensure that MIFARE DESFire EV1 code is verified for integrity and authenticity prior being executed.</p>

## 6.2 Security objectives for the environment

106	<p>Security Objectives for the Security IC Embedded Software development environment (phase 1):</p> <p><a href="#">BSI.OE.Plat-Appl</a>      <a href="#">Usage of Hardware Platform</a></p> <p><a href="#">BSI.OE.Resp-Appl</a>      <a href="#">Treatment of User Data</a></p>
107	<p>Security Objectives for the operational Environment (phase 4 up to 6):</p> <p><a href="#">BSI.OE.Process-Sec-IC</a>      <a href="#">Protection during composite product manufacturing</a></p>
108	<p>This section details the security objectives for the operational environment, related to DESFire, and to be enforced after TOE delivery up to phase 6.</p>
109	<p>The following security objectives for the operational environment are only valid if MFPlus is embedded in the TOE:</p> <p>OE.Secure-Values-MFPlus      Generation of secure values for MFPlus:</p> <p>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.</p>

	OE.Terminal-Support-MFPlus	Terminal support to ensure integrity and confidentiality for MFPlus: The terminal shall verify information sent by the TOE in order to ensure integrity 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.
110	The following security objectives for the operational environment are only valid if <b>DESFire</b> is embedded in the TOE:	
	OE.Secure-Values-DESFire	Generation of secure values for DESFire: The environment shall generate confidential and secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalisation or usage in phase 5 to 7.
	OE.Terminal-Support-DESFire	Terminal support to ensure integrity and confidentiality for DESFire: The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session.

### 6.3 Security objectives rationale

- 111 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.
- 112 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).
- 113 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](#))".
- 114 The augmentation made in this ST introduces the following security environment aspects:
- TOE threats "Unauthorised data modification for MFPlus, ([T.Data-Modification-MFPlus](#))", "Impersonating authorised users during authentication for MFPlus, ([T.Impersonate-MFPlus](#))", "Cloning for MFPlus, ([T.Cloning-MFPlus](#))", "MFPlus code confidentiality, ([T.Confid-Applic-Code-MFPlus](#))", " MFPlus data confidentiality, ([T.Confid-Applic-Data-MFPlus](#))", " MFPlus code integrity, ([T.Integ-Applic-Code-](#)

*MFPlus*"), "MFPlus data integrity, (*T.Integ-Applic-Data-MFPlus*)", "MFPlus resource unavailability, (*T.Application-Resource-MFPlus*)", "Unauthorised data modification for DESFire, (*T.Data-Modification-DESFire*)", "Impersonating authorised users during authentication for DESFire, (*T.Impersonate-DESFire*)", "Cloning for DESFire, (*T.Cloning-DESFire*)", "DESFire code confidentiality, (*T.Confid-Applic-Code-DESFire*)", "DESFire data confidentiality, (*T.Confid-Applic-Data-DESFire*)", "DESFire code integrity, (*T.Integ-Applic-Code-DESFire*)", "DESFire data integrity, (*T.Integ-Applic-Data-DESFire*)", and "DESFire resource unavailability, (*T.Resource-DESFire*)".

- organisational security policies "Integrity during communication for MFPlus, (*P.MAC*)", "Un-traceability of end-users for MFPlus, (*P.No-Trace-MFPlus*)", "Confidentiality during communication for DESFire, (*P.Confidentiality*)", "Transaction mechanism for DESFire, (*P.Transaction*)", "Un-traceability of end-users for DESFire, (*P.No-Trace-DESFire*)", "Usage of hardware platform, (*P.Plat-App*)", and "Treatment of user data, (*P.Resp-App*)".
- assumptions "Usage of secure values for MFPlus, (*A.Secure-Values-MFPlus*)", and "Terminal support to ensure integrity for MFPlus, (*A.Terminal-Support-MFPlus*)", "Usage of secure values for DESFire, (*A.Secure-Values-DESFire*)", and "Terminal support to ensure integrity and confidentiality for DESFire, (*A.Terminal-Support-DESFire*)".

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

116 In particular, the added assumptions and objectives on the environment do not contradict with the policies, threats and assumptions of the *BSI-PP-0035* Protection Profile, to which strict conformance is claimed, because they are all exclusively related to DESFire or MIFARE Plus, which are out of the scope of this protection profile.

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
<i>BSI.A.Plat-App</i>	<i>BSI.OE.Plat-App</i>	Phase 1
<i>BSI.A.Resp-App</i>	<i>BSI.OE.Resp-App</i>	Phase 1
<i>BSI.P.Process-TOE</i>	<i>BSI.O.Identification</i>	Phase 2-3 optional Phase 4
<i>BSI.A.Process-Sec-IC</i>	<i>BSI.OE.Process-Sec-IC</i>	Phase 4-6 optional Phase 4
<i>A.Secure-Values-DESFire</i>	<i>OE.Secure-Values-DESFire</i>	Phases 5-7
<i>A.Secure-Values-MFPlus</i>	<i>OE.Secure-Values-MFPlus</i>	Phases 5-7
<i>A.Terminal-Support-DESFire</i>	<i>OE.Terminal-Support-DESFire</i>	Phase 7
<i>A.Terminal-Support-MFPlus</i>	<i>OE.Terminal-Support-MFPlus</i>	Phase 7
<i>AUG1.P.Add-Functions</i>	<i>AUG1.O.Add-Functions</i>	

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

<b>Assumption, Threat or Organisational Security Policy</b>	<b>Security Objective</b>	<b>Notes</b>
<i>P.MAC</i>	<i>O.MAC-MFPlus</i> <i>OE.Terminal-Support-MFPlus</i>	
<i>P.No-Trace-MFPlus</i>	<i>O.No-Trace-MFPlus</i> <i>O.Access-Control-MFPlus</i> <i>O.Authentication-MFPlus</i>	
<i>P.Confidentiality</i>	<i>O.Confidentiality-DESFire</i> <i>OE.Terminal-Support-DESFire</i>	
<i>P.Transaction</i>	<i>O.Transaction-DESFire</i>	
<i>P.No-Trace-DESFire</i>	<i>O.No-Trace-DESFire</i> <i>O.Access-Control-DESFire</i> <i>O.Authentication-DESFire</i>	
<i>P.Plat-Appl</i>	<i>O.Plat-Appl-DESFire</i> <i>O.Plat-Appl-MFPlus</i>	
<i>P.Resp-Appl</i>	<i>O.Resp-Appl-DESFire</i> <i>O.Resp-Appl-MFPlus</i>	
<i>BSI.T.Leak-Inherent</i>	<i>BSI.O.Leak-Inherent</i>	
<i>BSI.T.Phys-Probing</i>	<i>BSI.O.Phys-Probing</i>	
<i>BSI.T.Malfunction</i>	<i>BSI.O.Malfunction</i>	
<i>BSI.T.Phys-Manipulation</i>	<i>BSI.O.Phys-Manipulation</i>	
<i>BSI.T.Leak-Forced</i>	<i>BSI.O.Leak-Forced</i>	
<i>BSI.T.Abuse-Func</i>	<i>BSI.O.Abuse-Func</i>	
<i>BSI.T.RND</i>	<i>BSI.O.RND</i>	
<i>AUG4.T.Mem-Access</i>	<i>AUG4.O.Mem-Access</i>	
<i>T.Data-Modification-MFPlus</i>	<i>O.Access-Control-MFPlus</i> <i>OE.Terminal-Support-MFPlus</i>	
<i>T.Impersonate-MFPlus</i>	<i>O.Authentication-MFPlus</i>	
<i>T.Cloning-MFPlus</i>	<i>O.Access-Control-MFPlus</i> <i>O.Authentication-MFPlus</i>	
<i>T.Confid-Applic-Code-MFPlus</i>	<i>O.Firewall-MFPlus</i>	
<i>T.Confid-Applic-Data-MFPlus</i>	<i>O.Firewall-MFPlus</i>	
<i>T.Integ-Applic-Code-MFPlus</i>	<i>O.Verification-MFPlus</i> <i>O.Firewall-MFPlus</i>	
<i>T.Integ-Applic-Data-MFPlus</i>	<i>O.Shr-Var-MFPlus</i> <i>O.Firewall-MFPlus</i>	
<i>T.Application-Resource-MFPlus</i>	<i>O.Resource-MFPlus</i>	



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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
<i>T.Data-Modification-DESFire</i>	<i>O.Access-Control-DESFire</i> <i>O.Type-Consistency-DESFire</i> <i>OE.Terminal-Support-DESFire</i>	
<i>T.Impersonate-DESFire</i>	<i>O.Authentication-DESFire</i>	
<i>T.Cloning-DESFire</i>	<i>O.Access-Control-DESFire</i> <i>O.Authentication-DESFire</i>	
<i>T.Confid-Applic-Code-DESFire</i>	<i>O.Firewall-DESFire</i>	
<i>T.Confid-Applic-Data-DESFire</i>	<i>O.Firewall-DESFire</i>	
<i>T.Integ-Applic-Code-DESFire</i>	<i>O.Verification-DESFire</i> <i>O.Firewall-DESFire</i>	
<i>T.Integ-Applic-Data-DESFire</i>	<i>O.Shr-Res-DESFire</i> <i>O.Firewall-DESFire</i>	
<i>T.Resource-DESFire</i>	<i>O.Resource-DESFire</i>	

### 6.3.1 Assumption "Usage of secure values for MFPlus"

117 The justification related to the assumption "Usage of secure values for MFPlus, ([A.Secure-Values-MFPlus](#))" is as follows:

118 Since [OE.Secure-Values-MFPlus](#) requires secure values for the configuration of the authentication and access control as assumed in [A.Secure-Values-MFPlus](#), the assumption is covered by the objective.

119 [A.Secure-Values-MFPlus](#) and [OE.Secure-Values-MFPlus](#) do not contradict with the security problem definition of the [BSI-PP-0035](#), because they are only related to MFPlus, which is out of the scope of this protection profile.

### 6.3.2 Assumption "Terminal support to ensure integrity for MFPlus"

120 The justification related to the assumption "Terminal support to ensure integrity for MFPlus, ([A.Terminal-Support-MFPlus](#))" is as follows:

121 The objective [OE.Terminal-Support-MFPlus](#) is an immediate transformation of the assumption [A.Terminal-Support-MFPlus](#), therefore it covers the assumption.

122 [A.Terminal-Support-MFPlus](#) and [OE.Terminal-Support-MFPlus](#) do not contradict with the security problem definition of the [BSI-PP-0035](#), because they are only related to MFPlus, which is out of the scope of this protection profile.

### 6.3.3 Assumption "Usage of secure values for DESFire"

123 The justification related to the assumption "Usage of secure values for DESFire, ([A.Secure-Values-DESFire](#))" is as follows:

124 Since [OE.Secure-Values-DESFire](#) requires from the Administrator, Application Manager or the Application User to use secure values for the configuration of the authentication and

access control as assumed in [A.Secure-Values-DESFire](#), the assumption is covered by the objective.

125 [A.Secure-Values-DESFire](#) and [OE.Secure-Values-DESFire](#) 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 "Terminal support to ensure integrity and confidentiality for DESFire"

126 The justification related to the assumption "Terminal support to ensure integrity and confidentiality for DESFire, ([A.Terminal-Support-DESFire](#))" is as follows:

127 The objective [OE.Terminal-Support-DESFire](#) is an immediate transformation of the assumption [A.Terminal-Support-DESFire](#), therefore it covers the assumption.

128 [A.Terminal-Support-DESFire](#) and [OE.Terminal-Support-DESFire](#) 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 TOE threat "Memory Access Violation"

129 The justification related to the threat "Memory Access Violation, ([AUG4.T.Mem-Access](#))" is as follows:

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

131 The added objective for the TOE [AUG4.O.Mem-Access](#) does not introduce any contradiction in the security objectives for the TOE.

#### 6.3.6 TOE threat "Unauthorised data modification for MFPlus"

132 The justification related to the threat "Unauthorised data modification for MFPlus, ([T.Data-Modification-MFPlus](#))" is as follows:

133 According to threat [T.Data-Modification-MFPlus](#), the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective [O.Access-Control-MFPlus](#) requires an access control mechanism that limits the ability to modify data elements stored by the TOE. The terminal must provide support by checking the TOE responses, which is required by [OE.Terminal-Support-MFPlus](#). Therefore [T.Data-Modification-MFPlus](#) is covered by these two objectives.

134 The added objective for the TOE [O.Access-Control-MFPlus](#) does not introduce any contradiction in the security objectives for the TOE.

#### 6.3.7 TOE threat "Impersonating authorised users during authentication for MFPlus"

135 The justification related to the threat "Impersonating authorised users during authentication for MFPlus, ([T.Impersonate-MFPlus](#))" is as follows:

- 136 The threat is related to the fact that an unauthorised subject may try to impersonate an authorised subject during authentication, e.g. by a man-in-the middle or replay attack. The goal of *O.Authentication-MFPlus* is that an authentication mechanism is implemented in the TOE that prevents these attacks. Therefore the threat is covered by *O.Authentication-MFPlus*.
- 137 The added objective for the TOE *O.Authentication-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.8 TOE threat "Cloning for MFPlus"

- 138 The justification related to the threat "Cloning for MFPlus, (*T.Cloning-MFPlus*)" is as follows:
- 139 The concern of *T.Cloning-MFPlus* is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objectives *O.Authentication-MFPlus* together with *O.Access-Control-MFPlus* require that unauthorised users cannot read any information that is restricted to the authorised subjects. The cryptographic keys used for the authentication are stored inside the TOE protected by *O.Access-Control-MFPlus*. This objective states that the TOE shall never output any keys used for authentication. Therefore the two objectives cover *T.Cloning-MFPlus*.

### 6.3.9 TOE threat "MFPlus resource unavailability"

- 140 The justification related to the threat "MFPlus resource unavailability, (*T.Application-Resource-MFPlus*)" is as follows:
- 141 The concern of *T.Application-Resource-MFPlus* is to prevent denial of service or malfunction of MFPlus, that may result from an unavailability of resources. The goal of *O.Resource-MFPlus* is to control the availability of resources for MFPlus. Therefore the threat is covered by *O.Resource-MFPlus*.
- 142 The added objective for the TOE *O.Resource-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.10 TOE threat "MFPlus code confidentiality"

- 143 The justification related to the threat "MFPlus code confidentiality, (*T.Confid-Applic-Code-MFPlus*)" is as follows:
- 144 Since *O.Firewall-MFPlus* requires that the TOE ensures isolation of code between MFPlus and the other applications, the code of MFPlus is protected against unauthorised disclosure, therefore *T.Confid-Applic-Code-MFPlus* is covered by *O.Firewall-MFPlus*.
- 145 The added objective for the TOE *O.Firewall-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.11 TOE threat "MFPlus data confidentiality"

- 146 The justification related to the threat "MFPlus data confidentiality, (*T.Confid-Applic-Data-MFPlus*)" is as follows:
- 147 Since *O.Firewall-MFPlus* requires that the TOE ensures isolation of data between MFPlus and the other applications, the data of MFPlus is protected against unauthorised disclosure, therefore *T.Confid-Applic-Data-MFPlus* is covered by *O.Firewall-MFPlus*.

### 6.3.12 TOE threat "MFPlus code integrity"

- 148 The justification related to the threat "MFPlus code integrity, (*T.Integ-Applic-Code-MFPlus*)" is as follows:
- 149 The threat is related to the alteration of MFPlus code by an attacker. *O.Verification-MFPlus* requires that the TOE verifies the code integrity before its execution. Complementary, *O.Firewall-MFPlus* requires that the TOE ensures isolation of code between MFPlus and the other applications, thus protecting the code of MFPlus against unauthorised modification. Therefore the threat is covered by *O.Verification-MFPlus* together with *O.Firewall-MFPlus*.
- 150 The added objective for the TOE *O.Verification-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.13 TOE threat "MFPlus data integrity"

- 151 The justification related to the threat "MFPlus data integrity, (*T.Integ-Applic-Data-MFPlus*)" is as follows:
- 152 The threat is related to the alteration of MFPlus data by an attacker. Since *O.Firewall-MFPlus* and *O.Shr-Var-MFPlus* require that the TOE ensures complete isolation of data between MFPlus and the other applications, the data of MFPlus is protected against unauthorised modification, therefore *T.Integ-Applic-Data-MFPlus* is covered by *O.Firewall-MFPlus* together with *O.Shr-Var-MFPlus*.
- 153 The added objective for the TOE *O.Shr-Var-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.14 TOE threat "Unauthorised data modification for DESFire"

- 154 The justification related to the threat "Unauthorised data modification for DESFire, (*T.Data-Modification-DESFire*)" is as follows:
- 155 According to threat *T.Data-Modification-DESFire*, the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective *O.Access-Control-DESFire* requires an access control mechanism that limits the ability to modify data elements stored by the TOE. *O.Type-Consistency-DESFire* ensures that data types are adhered, so that data cannot be modified by abusing type-specific operations. The terminal must support this by checking the TOE responses, which is required by *OE.Terminal-Support-DESFire*. Therefore *T.Data-Modification-DESFire* is covered by these three objectives.
- 156 The added objectives for the TOE *O.Access-Control-DESFire* and *O.Type-Consistency-DESFire* do not introduce any contradiction in the security objectives for the TOE.

### 6.3.15 TOE threat "Impersonating authorised users during authentication for DESFire"

- 157 The justification related to the threat "Impersonating authorised users during authentication for DESFire, (*T.Impersonate-DESFire*)" is as follows:
- 158 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-DESFire* is that an authentication mechanism is implemented in the TOE that prevents these attacks. Therefore the threat is covered by *O.Authentication-DESFire*.

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

### 6.3.16 TOE threat "Cloning for DESFire"

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

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

### 6.3.17 TOE threat "DESFire resource unavailability"

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

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

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

### 6.3.18 TOE threat "DESFire code confidentiality"

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

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

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

### 6.3.19 TOE threat "DESFire data confidentiality"

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

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

### 6.3.20 TOE threat "DESFire code integrity"

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

- 171 The threat is related to the alteration of DESFire code by an attacker. *O.Verification-DESFire* requires that the TOE verifies the code integrity before its execution. Complementary, *O.Firewall-DESFire* requires that the TOE ensures isolation of code between DESFire and the other applications, thus protecting the code of DESFire against unauthorised modification. Therefore the threat is covered by *O.Verification-DESFire* together with *O.Firewall-DESFire*.
- 172 The added objective for the TOE *O.Verification-DESFire* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.21 TOE threat "DESFire data integrity"

- 173 The justification related to the threat "DESFire data integrity, (*T.Integ-Applic-Data-DESFire*)" is as follows:
- 174 The threat is related to the alteration of DESFire data by an attacker. Since *O.Firewall-DESFire* and *O.Shr-Res-DESFire* require that the TOE ensures isolation of data between DESFire and the other applications, the data of DESFire is protected against unauthorised modification, therefore *T.Integ-Applic-Data-DESFire* is covered by *O.Firewall-DESFire* together with *O.Shr-Res-DESFire*.
- 175 The added objective for the TOE *O.Shr-Res-DESFire* does not introduce any contradiction in the security objectives for the TOE.

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

- 176 The justification related to the organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)" is as follows:
- 177 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.
- 178 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*.
- 179 The added objective for the TOE *AUG1.O.Add-Functions* does not introduce any contradiction in the security objectives for the TOE.

### 6.3.23 Organisational security policy "Integrity during communication for MFPlus"

- 180 The justification related to the organisational security policy "Integrity during communication for MFPlus, (*P.MAC*)" is as follows:
- 181 The policy *P.MAC* requires the TOE to provide the possibility to protect the contactless communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session. *O.MAC-MFPlus* requires that a security attribute for the card contains an option that the communication must be MACed. In



order to ensure the security the terminal must support the TOE by checking the MAC in the TOE responses, which is the goal of the objective *OE.Terminal-Support-MFPlus*. Therefore both objectives cover the policy.

182 The added objective for the TOE *O.MAC-MFPlus* does not introduce any contradiction in the security objectives.

#### 6.3.24 Organisational security policy "Un-traceability of end-users for MFPlus"

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

184 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-MFPlus* 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-MFPlus* and *O.Access-Control-MFPlus* 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.

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

#### 6.3.25 Organisational security policy "Confidentiality during communication for DESFire"

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

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

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

#### 6.3.26 Organisational security policy "Transaction mechanism for DESFire"

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

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

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

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

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

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

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

### 6.3.28 Organisational security policy "Usage of hardware platform"

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

196 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-DESFire* and *O.Plat-Appl-MFPlus* have the same objective as *BSI.OE.Plat-Appl* defined in the PP. Thus, the objectives *O.Plat-Appl-DESFire* and/or *O.Plat-Appl-MFPlus* cover the policy *P.Plat-Appl*.

197 The added objectives for the TOE *O.Plat-Appl-DESFire* and *O.Plat-Appl-MFPlus* do not introduce any contradiction in the security objectives.

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

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

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

200 The added objectives for the TOE *O.Plat-Appl-DESFire* and *O.Plat-Appl-MFPlus* do not introduce any contradiction in the security objectives.



## 7 Security requirements

201 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

202 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.

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

204 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.

205 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.

206 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	<a href="#">BSI-PP-0035</a>	<a href="#">CCMB-2012-09-002</a>
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1	Limited capabilities	Abuse of TEST functionality	<a href="#">BSI-PP-0035</a>	Extended
FMT_LIM.2	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	<a href="#">BSI-PP-0035</a> Operated	

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

Label	Title	Addressing	Origin	Type
FPT_PHP.3	Resistance to physical attack	Physical manipulation & probing	<i>BSI-PP-0035</i>	<i>CCMB-2012-09-002</i>
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	<i>BSI-PP-0035</i> Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	<i>AUG #1</i> Operated	<i>CCMB-2012-09-002</i>
FCS_CKM.1 (if <i>Neslib</i> is embedded only)	Cryptographic key generation		Security Target Operated	
FDP_ACC.2 [Memories]	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1 [Memories]	Security attribute based access control			
FMT_MSA.3 [Memories]	Static attribute initialisation	Correct operation	<i>AUG #4</i> Operated	
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
FMT_SMR.1 [MFPlus]	Security roles	MFPlus access control (if MFPlus is embedded only)	Security Target Operated	CCMB-2012-09-002
FDP_ACC.1 [MFPlus]	Subset access control			
FDP_ACF.1 [MFPlus]	Security attribute based access control			
FMT_MSA.3 [MFPlus]	Static attribute initialisation			
FMT_MSA.1 [MFPlus]	Management of security attribute			
FMT_SMF.1 [MFPlus]	Specification of management functions			
FDP_ITC.2 [MFPlus]	Import of user data with security attributes			
FPT_TDC.1 [MFPlus]	Inter-TSF basic TSF data consistency			
FIA_UID.2 [MFPlus]	User identification before any action	MFPlus confidentiality and authentication (if MFPlus is embedded only)		
FIA_UAU.2 [MFPlus]	User authentication before any action			
FIA_UAU.5 [MFPlus]	Multiple authentication mechanisms			
FMT_MTD.1 [MFPlus]	Management of TSF data			
FPT_TRP.1 [MFPlus]	Trusted path			
FCS_CKM.4 [MFPlus]	Cryptographic key destruction			
FPT_RPL.1 [MFPlus]	Replay detection			
FPR_UNL.1 [MFPlus]	Unlinkability	MFPlus robustness (if MFPlus is embedded only)		
FRU_RSA.2 [MFPlus]	Minimum and maximum quotas	MFPlus correct operation (if MFPlus is embedded only)		

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

Label	Title	Addressing	Origin	Type
FDP_RIP.1 [MFPlus]	Subset residual information protection	MFPlus intrinsic confidentiality and integrity (if MFPlus is embedded only)	Security Target Operated	CCMB-2012-09-002
FMT_SMR.1 [DESFire]	Security roles	DESFire access control (if DESFire is embedded only)		
FDP_ACC.1 [DESFire]	Subset access control			
FDP_ACF.1 [DESFire]	Security attribute based access control			
FMT_MSA.3 [DESFire]	Static attribute initialisation			
FMT_MSA.1 [DESFire]	Management of security attribute			
FMT_SMF.1 [DESFire]	Specification of management functions			
FDP_ITC.2 [DESFire]	Import of user data with security attributes			
FPT_TDC.1 [DESFire]	Inter-TSF basic TSF data consistency			
FIA_UID.2 [DESFire]	User identification before any action	DESFire confidentiality and authentication (if DESFire is embedded only)		
FIA_UAU.2 [DESFire]	User authentication before any action			
FIA_UAU.5 [DESFire]	Multiple authentication mechanisms			
FMT_MTD.1 [DESFire]	Management of TSF data			
FPT_TRP.1 [DESFire]	Trusted path			
FCS_CKM.4 [DESFire]	Cryptographic key destruction			

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

Label	Title	Addressing	Origin	Type
FDP_ROL.1 [DESFire]	Basic rollback	DESFire robustness (if <b>DESFire</b> is embedded only)	Security Target Operated	CCMB-2012-09-002
FPT_RPL.1 [DESFire]	Replay detection			
FPR_UNL.1 [DESFire]	Unlinkability			
FPT_TST.1 [DESFire]	TSF testing	DESFire correct operation (if <b>DESFire</b> is embedded only)		
FRU_RSA.2 [DESFire]	Minimum and maximum quotas			
FDP_RIP.1 [DESFire]	Subset residual information protection	DESFire intrinsic confidentiality and integrity (if <b>DESFire</b> is embedded only)		
FDP_ACC.1 [MIFARE_FWL]	Subset access control	DESFire or MFPlus intrinsic confidentiality and integrity (if <b>DESFire</b> or <b>MFPlus</b> is embedded only)		
FDP_ACF.1 [MIFARE_FWL]	Security attribute based access control			
FMT_MSA.3 [MIFARE_FWL]	Static attribute initialisation			

### 7.1.1 Security Functional Requirements from the Protection Profile

#### Limited fault tolerance (FRU\_FLT.2)

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

#### Failure with preservation of secure state (FPT\_FLS.1)

208 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.**

209 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.

**Limited capabilities (FMT\_LIM.1)**

- 210 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.

**Limited availability (FMT\_LIM.2)**

- 211 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.

- 212 *SFP\_1: Limited capability and availability Policy*

*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.*

**Audit storage (FAU\_SAS.1)**

- 213 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**.

**Resistance to physical attack (FPT\_PHP.3)**

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

- 215 Refinement:

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

**Basic internal transfer protection (FDP\_ITT.1)**

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

**Basic internal TSF data transfer protection (FPT\_ITT.1)**

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

- 218 Refinement:

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

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

**Subset information flow control (FDP\_IFC.1)**

219 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**.

220 *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.*

**Random number generation (FCS\_RNG.1)**

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

222 The TSF shall provide random numbers that meet **P2 class of BSI-AIS31**.

**7.1.2 Additional Security Functional Requirements for the cryptographic services**

**Cryptographic operation (FCS\_COP.1)**

223 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	Data Encryption Standard (DES)	56 bits	<a href="#">FIPS PUB 46-3</a> <a href="#">ISO/IEC 9797-1</a> <a href="#">ISO/IEC 10116</a>
		- in Electronic Code Book (ECB) mode * MAC computation in CBC-MAC	Triple Data Encryption Standard (3DES)	168 bits	
Even without Neslib	AES	* encryption (cipher) * decryption (inverse cipher) * key expansion * randomize	Advanced Encryption Standard	128, 192 and 256 bits	<a href="#">FIPS PUB 197</a>

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	RSA	<ul style="list-style-type: none"> <li>* RSA public key operation</li> <li>* RSA private key operation without the Chinese Remainder Theorem</li> <li>* RSA private key operation with the Chinese Remainder Theorem</li> </ul>	Rivest, Shamir & Adleman's	up to 4096 bits	<i>PKCS #1 V2.1</i>
If Neslib	ECC	<ul style="list-style-type: none"> <li>* private scalar multiplication</li> <li>* prepare Jacobian</li> <li>* public scalar multiplication</li> <li>* point validity check</li> <li>* convert Jacobian to affine coordinates</li> <li>* general point addition</li> <li>* point expansion</li> <li>* point compression</li> </ul>	Elliptic Curves Cryptography on GF(p)	up to 640 bits	<i>IEEE 1363-2000, chapter 7</i> <i>IEEE 1363a-2004</i>
If Neslib	SHA	<ul style="list-style-type: none"> <li>* SHA-1</li> <li>* SHA-224</li> <li>* SHA-256</li> <li>* SHA-384</li> <li>* SHA-512</li> <li>* Protected SHA-1</li> </ul>	Secure Hash Algorithm	assignment pointless because algorithm has no key	<i>FIPS PUB 180-1</i> <i>FIPS PUB 180-2</i> <i>ISO/IEC 10118-3:1998</i>

**Cryptographic key generation (FCS\_CKM.1)**

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

### 7.1.3 Additional Security Functional Requirements for the memories protection

225 The following SFRs are extensions to "[BSI-PP-0035](#)" Protection Profile (PP), related to the memories protection.

#### Static attribute initialisation (FMT\_MSA.3) [Memories]

226 The TSF shall enforce the **Dynamic Memory Access Control Policy** to provide **minimally protective**<sup>(a)</sup> default values for security attributes that are used to enforce the SFP.

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

Application note:

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

#### Management of security attributes (FMT\_MSA.1) [Memories]

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

#### Complete access control (FDP\_ACC.2) [Memories]

229 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.

a. See the Datasheet referenced in [Section 9](#) for actual values.

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

#### **Security attribute based access control (FDP\_ACF.1) [Memories]**

231 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.**

232 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.**

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

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

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

236 *SFP\_3: Dynamic Memory Access Control Policy*

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

#### **Specification of management functions (FMT\_SMF.1) [Memories]**

238 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.**

### **7.1.4 Additional Security Functional Requirements related to MFPlus**

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

240 They are only valid in case **MFPlus** is embedded.

241 **Note:** MIFARE Plus S 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 and check the code integrity in ROM,
- FCS\_RNG.1 for the provision of random numbers,
- FCS\_COP.1 [AES] for AES cryptographic operations (AES accelerator).

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

**Security roles (FMT\_SMR.1) [MFPlus]**

243 The TSF shall maintain the roles *Personaliser, Card Administrator, Card Manager, Card Security Level Manager, Card User and Originality Key User*.

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

**Subset access control (FDP\_ACC.1) [MFPlus]**

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

**Security attribute based access control (FDP\_ACF.1) [MFPlus]**

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

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

- *The Personaliser can change all blocks.*
- *For every sector the Card User can read or write a data block based on the access control settings in the respective sector trailer.*

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

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

- *The block 0 (first block of the first sector) cannot be modified.*

250 The following SFP *MFPlus Access Control Policy* is defined for the requirement "Security attribute based access control (FDP\_ACF.1) [MFPlus]":

251 *SFP\_4: MFPlus Access Control Policy*

252 *The Security Function Policy (SFP) MFPlus Access Control Policy uses the following definitions:*

253 *The following roles are supported:*

- *The Personaliser who can personalise the TOE.*
- *The Card Administrator who can change security attributes which do not require being changed in the field.*
- *The Card Manager who can change security attributes which may require being changed in the field.*
- *The Card Security Level Manager who can switch the card to security level 3.*
- *The Card User who can perform operations with blocks.*
- *The Originality Key User who can authenticate himself to prove the authenticity of the Card.*

254 *Note that multiple subjects may have the same role, e.g. for every sector there are 2 Card Users (identified by the respective "Key A" and "Key B" for this sector). The assigned rights to the Card Users can be different, which allows having more or less powerful Card Users. There are also more than one Originality Key Users.*

255 *Any other subject belongs to the role Anybody which is not modelled explicitly in the policy because no access rights are granted to this role. This role includes the card holder (i.e. end-user) and any other subject e.g. an attacker.*

- 256 *The objects are:*
- *Blocks that are grouped in sectors. Each sector consists of either 4 or 16 blocks. One block of each sector contains the access conditions and is called Sector Trailer.*
- 257 *The operations that can be performed with the objects are:*
- *read data from a block,*
  - *write data to a block and*
  - *read or modify the security attributes.*
- 258 *The security attributes are:*
- *the Field Configuration Block,*
  - *the sector trailer for a sector and*
  - *the security level of the TOE.*
- 259 *Note that subjects are authorised by cryptographic keys. These keys are considered as authentication data and not as security attributes. The TOE stores a dedicated cryptographic key for every subject. The key of the Card Administrator is called "Card Master Key" and the key for the Card Manager is called "Card Configuration Key". The Card Security Level Manager key is called "Level 3 Switch Key". The keys of the Card Users are called "AES Sector Keys". Since there are two keys for every sector the keys are called "AES Sector Key A" and "AES Sector Key B" or in short "Key A" and "Key B". The keys of the Originality Key User are called "Originality Keys".*
- 260 *Implications of the MFPlus Access Control Policy:*
- 261 *The MFPlus 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 (card holder) does normally not belong to the group of authorised users (Card Administrator, Card Manager, Card Security Level Manager, Card User, Originality Key User), but is regarded as 'Anybody' 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 Personaliser is very powerful, although the role is limited to Security Level 0. The Personaliser can write all blocks and therefore change all data and the sector trailers.*
  - *Switching of the security level is an integral part of the TOE security. The TOE is switched from security level 0 to security level 1 or 3 at the end of the personalisation phase. The security level can be increased by the Card Security Level Manager afterwards.*

### **Static attribute initialisation (FMT\_MSA.3) [MFPlus]**

- 262 The TSF shall enforce the **MFPlus Access Control Policy** to provide **permissive** default values for security attributes that are used to enforce the SFP.
- 263 The TSF shall allow **no subject** to specify alternative initial values to override the default values when an object or information is created.

### **Management of security attributes (FMT\_MSA.1) [MFPlus]**

- 264 The TSF shall enforce the **MFPlus Access Control Policy** to restrict the ability to **modify** the security attributes **Field Configuration Block, security level and sector trailers** to the **Card Manager, Card Administrator, Card Security Level Manager and Card User, respectively**.

**Specification of Management Functions (FMT\_SMF.1) [MFPlus]**

- 265 The TSF shall be capable of performing the following security management functions:
- **Authenticate a user,**
  - **Invalidating the current authentication state based on the functions: Issuing a request for authentication, Occurrence of any error during the execution of a command, Reset, Switching the security level of the TOE, DESELECT according to ISO 14443-3, explicit authentication request;**
  - **Finishing the personalisation phase by explicit request of the Personaliser,**
  - **Changing a security attribute.**

**Import of user data with security attributes (FDP\_ITC.2) [MFPlus]**

- 266 The TSF shall enforce the **MFPlus Access Control Policy** when importing user data, controlled under the SFP, from outside of the TOE.
- 267 The TSF shall use the security attributes associated with the imported user data.
- 268 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
- 269 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.
- 270 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **no additional rules.**

**Inter-TSF basic TSF data consistency (FPT\_TDC.1) [MFPlus]**

- 271 The TSF shall provide the capability to consistently interpret **data blocks** when shared between the TSF and another trusted IT product.
- 272 The TSF shall use **the rules: data blocks can always be modified by the write operation. Sector trailers must have a specific format** 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 cannot determine if data stored in a specific block is an identification number that adheres to a specific format. For sector trailers the TOE enforces a specific format.

**Cryptographic key destruction (FCS\_CKM.4) [MFPlus]**

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

**User identification before any action (FIA\_UID.2) [MFPlus]**

- 274 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 key block number. For example, if an authentication request for key number 0x9000 is issued after selecting the Card, the user is identified as the Card Administrator.

**User authentication before any action (FIA\_UAU.2) [MFPlus]**

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

**Multiple authentication mechanisms (FIA\_UAU.5) [MFPlus]**

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

277 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 in security level 0. The 'none' authentication implicitly and solely authorises the Personaliser subject.*
- *The cryptographic authentication is used in security level 0 to authenticate the Originality Key User.*
- *The cryptographic authentication is used in security level 1 to authenticate the Originality Key User and the Card Security Level Manager.*
- *The cryptographic authentication is used in security level 3 to authenticate the Originality Key User, Card Administrator, Card Manager and the Card User.*

**Management of TSF data (FMT\_MTD.1) [MFPlus]**

278 The TSF shall restrict the ability to *modify* the *security attributes and authentication data* to *the Personaliser, Card Administrator, Card Manager, Card Security Level Manager and Card User*.

279 Refinement:

The detailed management abilities are:

- The Personaliser can change all security attributes as well as all keys except the keys of the Originality Key User.
- The Card Administrator can change the Level 3 Switch Key and the Card Master Key.
- The Card Manager can change the Field Configuration Block and the Card Configuration Key.
- The Card Security Level Manager can switch the security level of the TOE to security level 3.
- The Card User may change the AES Sector Keys and the sector trailer if the access conditions in the corresponding sector trailer grants him rights.

**Trusted path (FTP\_TRP.1) [MFPlus]**

280 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*.

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

282 The TSF shall require the use of the trusted path for *authentication requests, data integrity verification for data transfers*.

**Replay detection (FPT\_RPL.1) [MFPlus]**

283 The TSF shall detect replay for the following entities: *authentication requests, data integrity verification for data transfers*.



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

#### **Unlinkability (FPR\_UNL.1) [MFPlus]**

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

#### **Minimum and maximum quotas (FRU\_RSA.2) [MFPlus]**

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

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

#### **Subset residual information protection (FDP\_RIP.1) [MFPlus]**

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

### **7.1.5 Additional Security Functional Requirements related to DESFire**

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

290 They are only valid in case *DESFire* is embedded.

291 **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,
- FCS\_COP.1 [AES] for AES cryptographic operations (AES accelerator).

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

#### **Security roles (FMT\_SMR.1) [DESFire]**

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

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

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

#### **Subset access control (FDP\_ACC.1) [DESFire]**

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

**Security attribute based access control (FDP\_ACF.1) [DESFire]**

- 297 The TSF shall enforce the **DESFire Access Control Policy** to objects based on the following: **all subjects, objects and attributes**.
- 298 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 files 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.**
- 299 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.**
- 300 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.**
- 301 The following SFP **DESFire Access Control Policy** is defined for the requirement "Security attribute based access control (FDP\_ACF.1) [DESFire]":
- 302 *SFP\_5: DESFire Access Control Policy*
- 303 *The Security Function Policy (SFP) DESFire Access Control Policy uses the following definitions:*
- 304 *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.*



- 305      *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.*
- 306      *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.*
- 307      *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 prevents any further modify.*
- 308      *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.*
- 309      *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.*
- 310      *Implications of the DESFire Access Control Policy:*
- 311      *The DESFire Access Control Policy has some implications, that can be drawn from the policy and that are essential parts of the TOE security functions.*
- *The TOE end-user does normally not belong to the group of authorised users (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.*

### **Static attribute initialisation (FMT\_MSA.3) [DESFire]**

- 312 The TSF shall enforce the **DESFire Access Control Policy** to provide **permissive** default values for security attributes that are used to enforce the SFP.
- 313 The TSF shall allow **no subject** to specify alternative initial values to override the default values when an object or information is created.
- 314 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.

### **Management of security attributes (FMT\_MSA.1) [DESFire]**

- 315 The TSF shall enforce the **DESFire 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**.
- 316 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.

### **Specification of Management Functions (FMT\_SMF.1) [DESFire]**

- 317 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.**

### **Import of user data with security attributes (FDP\_ITC.2) [DESFire]**

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

- 319 The TSF shall use the security attributes associated with the imported user data.
- 320 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
- 321 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.
- 322 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***no additional rules***.

#### **Inter-TSF basic TSF data consistency (FPT\_TDC.1) [DESFire]**

- 323 The TSF shall provide the capability to consistently interpret ***data files and values*** when shared between the TSF and another trusted IT product.
- 324 The TSF shall use ***the rule: data files or values can only be modified by their dedicated type-specific operations honouring the type-specific boundaries*** when interpreting the TSF data from another trusted IT product.

##### **Application note:**

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

#### **Cryptographic key destruction (FCS\_CKM.4) [DESFire]**

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

#### **User identification before any action (FIA\_UID.2) [DESFire]**

- 326 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'.

#### **User authentication before any action (FIA\_UAU.2) [DESFire]**

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

#### **Multiple authentication mechanisms (FIA\_UAU.5) [DESFire]**

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

- 329 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.**

#### **Management of TSF data (FMT\_MTD.1) [DESFire]**

- 330 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**.

- 331 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.

#### **Trusted path (FTP\_TRP.1) [DESFire]**

- 332 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**.
- 333 The TSF shall permit **remote users** to initiate communication via the trusted path.
- 334 The TSF shall require the use of the trusted path for **authentication requests with DES and AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes**.

#### **Basic rollback (FDP\_ROL.1) [DESFire]**

- 335 The TSF shall enforce **the DESFire Access Control Policy** to permit the rollback of the **operations that modify the value or data file objects** on the **backup files**.
- 336 The TSF shall permit operations to be rolled back within the **scope of the current transaction, which is defined by the following limitative events: chip reset, (re-) authentication (either successful or not), select command, explicit commit, explicit abort, command failure**.

**Replay detection (FPT\_RPL.1) [DESFire]**

- 337 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.***
- 338 The TSF shall perform ***rejection of the request*** when replay is detected.

**Unlinkability (FPR\_UNL.1) [DESFire]**

- 339 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.***

**TSF testing (FPT\_TST.1) [DESFire]**

- 340 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.***
- 341 The TSF shall provide authorised users with the capability to verify the integrity of ***the DESFire code.***
- 342 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.

**Minimum and maximum quotas (FRU\_RSA.2) [DESFire]**

- 343 The TSF shall enforce maximum quotas of the following resources ***NVM and RAM*** that ***subjects*** can use ***simultaneously.***
- 344 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.

**Subset residual information protection (FDP\_RIP.1) [DESFire]**

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

**7.1.6 Additional Security Functional Requirements common to DESFire and MFPlus****Subset access control (FDP\_ACC.1) [MIFARE\_FWL]**

- 346 The TSF shall enforce the ***MIFARE Firewall Access Control Policy*** on ***the DESFire and MFPlus code and data.***

**Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]**

- 347 The TSF shall enforce the ***MIFARE Firewall Access Control Policy*** to objects based on the following: ***DESFire and MFPlus code and data.***
- 348 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***An application cannot read, write, compare any piece of data or code belonging to DESFire or MFPlus.***

- 349 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.
  - 350 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
    - **An application cannot read, write, compare any piece of data or code belonging to DESFire or MFPlus.**
  - 351 The following SFP **MIFARE Firewall Access Control Policy** is defined for the requirement "Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]":
  - 352 *SFP\_6: MIFARE Firewall Access Control Policy*
  - 353 *An application cannot read, write, compare any piece of data or code belonging to DESFire or MFPlus.*
- Static attribute initialisation (FMT\_MSA.3) [MIFARE\_FWL]**
- 354 The TSF shall enforce the **MIFARE Firewall Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.
  - 355 The TSF shall allow **no subject** to specify alternative initial values to override the default values when an object or information is created.

## 7.2 TOE security assurance requirements

- 356 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level **5 (EAL5)** and augmented by taking the following components:
  - **ASE\_TSS.2, ALC\_DVS.2 and AVA\_VAN.5.**
- 357 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.
- 358 The component ASE\_TSS.2 is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.
- 359 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/ <a href="#">BSI-PP-0035</a>
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/ <a href="#">BSI-PP-0035</a>
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/ <a href="#">BSI-PP-0035</a>
AGD_PRE.1	Preparative procedures	EAL5/ <a href="#">BSI-PP-0035</a>

Table 10. TOE security assurance requirements (continued)

Label	Title	Origin
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/ <a href="#">BSI-PP-0035</a>
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/ <a href="#">BSI-PP-0035</a>
ALC_DVS.2	Sufficiency of security measures	<a href="#">BSI-PP-0035</a>
ALC_LCD.1	Developer defined life-cycle model	EAL5/ <a href="#">BSI-PP-0035</a>
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_ECD.1	Extended components definition	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_INT.1	ST introduction	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_OBJ.2	Security objectives	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_REQ.2	Derived security requirements	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_SPD.1	Security problem definition	EAL5/ <a href="#">BSI-PP-0035</a>
ASE_TSS.2	TOE summary specification with architectural summary	ST
ATE_COV.2	Analysis of coverage	EAL5/ <a href="#">BSI-PP-0035</a>
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/ <a href="#">BSI-PP-0035</a>
ATE_IND.2	Independent testing - sample	EAL5/ <a href="#">BSI-PP-0035</a>
AVA_VAN.5	Advanced methodical vulnerability analysis	<a href="#">BSI-PP-0035</a>

### 7.3 Refinement of the security assurance requirements

- 360 As [BSI-PP-0035](#) defines refinements for selected SARs, these refinements are also claimed in this Security Target.
- 361 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.
- 362 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.
- 363 The text of the impacted refinements of [BSI-PP-0035](#) is reproduced in the next sections.
- 364 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	<i>BSI-PP-0035</i> 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)

- 365 ~~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.**~~
- 366 ~~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.~~
- 367 ~~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.~~
- 368 ~~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.~~
- 369 ~~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.~~



370 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)

371 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).

372 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).

373 ~~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

374 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.

375 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in [Table 7](#), 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.

376 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 twenty two additional objectives ([O.Access-Control-MFPlus](#), [O.MAC-MFPlus](#), [O.Authentication-MFPlus](#), [O.No-Trace-MFPlus](#), [O.Plat-Appl-MFPlus](#), [O.Resp-Appl-MFPlus](#), [O.Resource-MFPlus](#), [O.Verification-MFPlus](#), [O.Firewall-MFPlus](#), [O.Shr-Var-MFPlus](#), [O.Access-Control-DESFire](#), [O.Authentication-DESFire](#), [O.Confidentiality-DESFire](#), [O.Type-Consistency-DESFire](#), [O.Transaction-DESFire](#), [O.No-Trace-DESFire](#), [O.Plat-Appl-DESFire](#), [O.Resp-Appl-DESFire](#), [O.Resource-DESFire](#), [O.Verification-DESFire](#), [O.Firewall-DESFire](#) and

[O.Shr-Res-DESFire](#)) introduced in this Security Target. This rationale must show that security requirements suitably address these twenty four.

377 Furthermore, a more careful observation of the requirements listed in [Table 7](#) 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\\_SMF.1](#) [[Memories](#)], [FMT\\_SMR.1](#) [[MFPlus](#)], [FDP\\_ACC.1](#) [[MFPlus](#)], [FDP\\_ACF.1](#) [[MFPlus](#)], [FMT\\_MSA.3](#) [[MFPlus](#)], [FMT\\_MSA.1](#) [[MFPlus](#)], [FMT\\_SMF.1](#) [[MFPlus](#)], [FDP\\_ITC.2](#) [[MFPlus](#)], [FPT\\_TDC.1](#) [[MFPlus](#)], [FIA\\_UID.2](#) [[MFPlus](#)], [FIA\\_UAU.2](#) [[MFPlus](#)], [FIA\\_UAU.5](#) [[MFPlus](#)], [FMT\\_MTD.1](#) [[MFPlus](#)], [FPT\\_TRP.1](#) [[MFPlus](#)], [FCS\\_CKM.4](#) [[MFPlus](#)], [FPT\\_RPL.1](#) [[MFPlus](#)], [FPR\\_UNL.1](#) [[MFPlus](#)], [FRU\\_RSA.2](#) [[MFPlus](#)], [FDP\\_RIP.1](#) [[MFPlus](#)], [FMT\\_SMR.1](#) [[DESFire](#)], [FDP\\_ACC.1](#) [[DESFire](#)], [FDP\\_ACF.1](#) [[DESFire](#)], [FMT\\_MSA.3](#) [[DESFire](#)], [FMT\\_MSA.1](#) [[DESFire](#)], [FMT\\_SMF.1](#) [[DESFire](#)], [FDP\\_ITC.2](#) [[DESFire](#)], [FPT\\_TDC.1](#) [[DESFire](#)], [FIA\\_UID.2](#) [[DESFire](#)], [FIA\\_UAU.2](#) [[DESFire](#)], [FIA\\_UAU.5](#) [[DESFire](#)], [FMT\\_MTD.1](#) [[DESFire](#)], [FPT\\_TRP.1](#) [[DESFire](#)], [FCS\\_CKM.4](#) [[DESFire](#)], [FDP\\_ROL.1](#) [[DESFire](#)], [FPT\\_RPL.1](#) [[DESFire](#)], [FPR\\_UNL.1](#) [[DESFire](#)], [FPT\\_TST.1](#) [[DESFire](#)], [FRU\\_RSA.2](#) [[DESFire](#)], [FDP\\_RIP.1](#) [[DESFire](#)], [FDP\\_ACC.1](#) [[MIFARE\\_FWL](#)], [FDP\\_ACF.1](#) [[MIFARE\\_FWL](#)], and [FMT\\_MSA.3](#) [[MIFARE\\_FWL](#)], and various assurance requirements of EAL5).

378 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.

379 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](#))”

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

381 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.

382 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*)"

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

384 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 "Access control for MFPlus (*O.Access-Control-MFPlus*)"

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

386 The security functional requirement "*Security roles (FMT\_SMR.1) [MFPlus]*" defines the roles of the MFPlus Access Control Policy.  
The security functional requirements "*Subset access control (FDP\_ACC.1) [MFPlus]*" and "*Security attribute based access control (FDP\_ACF.1) [MFPlus]*" define the rules and "*Static attribute initialisation (FMT\_MSA.3) [MFPlus]*" and "*Management of security attributes (FMT\_MSA.1) [MFPlus]*" the attributes that the access control is based on.  
The security functional requirement "*Management of TSF data (FMT\_MTD.1) [MFPlus]*" provides the rules for the management of the authentication data.  
The management functions are defined by "*Specification of Management Functions (FMT\_SMF.1) [MFPlus]*".  
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) [MFPlus]*". The security functional requirement "*Inter-TSF basic TSF data consistency (FPT\_TDC.1) [MFPlus]*" requires the TOE to constantly interpret data blocks (sector trailers). The TOE will honour the respective file formats and boundaries.  
Since cryptographic keys are used for authentication (refer to *O.Authentication-MFPlus*), these keys have to be removed if they are no longer needed for the access control. This is required by "*Cryptographic key destruction (FCS\_CKM.4) [MFPlus]*".  
These ten SFRs together provide an access control mechanism as required by the objective *O.Access-Control-MFPlus*.

### Security objective "Authentication for MFPlus (*O.Authentication-MFPlus*)"

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

388 The security functional requirement "*Cryptographic operation (FCS\_COP.1)[AES]*" requires that the TOE provides the basic cryptographic algorithm that can be used to perform the authentication.  
The security functional requirements "*User identification before any action (FIA\_UID.2) [MFPlus]*", "*User authentication before any action (FIA\_UAU.2) [MFPlus]*" and "*Multiple authentication mechanisms (FIA\_UAU.5) [MFPlus]*" together define that users must be identified and authenticated before any action.  
"*Trusted path (FTP\_TRP.1) [MFPlus]*" 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) [MFPlus]*" which requires a replay detection

for these authentication requests, the six security functional requirements fulfil the objective [O.Authentication-MFPlus](#).

**Security objective “MFPlus Integrity-protected Communication ([O.MAC-MFPlus](#))”**

389 The justification related to the security objective “MFPlus Integrity-protected Communication ([O.MAC-MFPlus](#))” is as follows:

390 The security functional requirement "[Cryptographic operation \(FCS\\_COP.1\)](#)[AES]" requires that the TOE provides the basic cryptographic algorithms that can be used to compute a MAC which can protect the integrity of the communication.

"[Trusted path \(FTP\\_TRP.1\)](#) [MFPlus]" requires a trusted communication path between the TOE and remote users; FTP\_TRP.1.3 especially requires “data integrity verification for data transfers on request of the file owner”.

Together with "[Replay detection \(FPT\\_RPL.1\)](#) [MFPlus]" which requires a replay detection for these data transfers, the three security functional requirements fulfil the objective [O.MAC-MFPlus](#).

**Security objective “Preventing traceability for MFPlus ([O.No-Trace-MFPlus](#))”**

391 The justification related to the security objective “Preventing traceability for MFPlus ([O.No-Trace-MFPlus](#))” is as follows:

392 The security functional requirement "[Unlinkability \(FPR\\_UNL.1\)](#) [MFPlus]" 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-MFPlus](#).

**Security objective “Usage of hardware platform for MFPlus ([O.Plat-Appl-MFPlus](#))”**

393 The justification related to the security objective “Usage of hardware platform for MFPlus ([O.Plat-Appl-MFPlus](#))” is as follows:

394 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 for MFPlus ([O.Resp-Appl-MFPlus](#))”**

395 The justification related to the security objective “Treatment of user data for MFPlus ([O.Resp-Appl-MFPlus](#))” is as follows:

396 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-MFPlus* is fulfilled by the additional ST SFRs.

**Security objective “NVM resource availability for MFPlus (*O.Resource-MFPlus*)”**

397 The justification related to the security objective “Resource availability for MFPlus (*O.Resource-MFPlus*)” is as follows:

398 The security functional requirement "*Minimum and maximum quotas (FRU\_RSA.2) [MFPlus]*" requires that sufficient parts of the NVM and RAM are reserved for MFPlus use. This fulfils the objective *O.Resource-MFPlus*.

**Security objective “MFPlus code integrity check (*O.Verification-MFPlus*)”**

399 The justification related to the security objective “MFPlus code integrity check (*O.Verification-MFPlus*)” is as follows:

400 The security functional requirements "*Subset access control (FDP\_ACC.1) [MIFARE\_FWL]*" and "*Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]*", supported by "*Static attribute initialisation (FMT\_MSA.3) [MIFARE\_FWL]*", require that MFPlus code integrity is protected. In addition, the security functional requirement "*Failure with preservation of secure state (FPT\_FLS.1)*" requires that in case of error on ROM, MFPlus execution is stopped. This meets the objective *O.Verification-MFPlus*.

**Security objective “MFPlus firewall (*O.Firewall-MFPlus*)”**

401 The justification related to the security objective “MFPlus firewall (*O.Firewall-MFPlus*)” is as follows:

402 The security functional requirements "*Subset access control (FDP\_ACC.1) [MIFARE\_FWL]*" and "*Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]*", supported by "*Static attribute initialisation (FMT\_MSA.3) [MIFARE\_FWL]*", require that no application can read, write, compare any piece of data or code belonging to MFPlus. This meets the objective *O.Firewall-MFPlus*.

**Security objective “MFPlus data cleaning for resource sharing (*O.Shr-Var-MFPlus*)”**

403 The justification related to the security objective “MFPlus data cleaning for resource sharing (*O.Shr-Var-MFPlus*)” is as follows:

404 The security functional requirement "*Subset residual information protection (FDP\_RIP.1) [MFPlus]*" requires that the information content of a resource is made unavailable upon its deallocation from MFPlus. This meets the objective *O.Shr-Var-MFPlus*.

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

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

406 The security functional requirement "*Security roles (FMT\_SMR.1) [DESFire]*" defines the roles of the DESFire Access Control Policy. The security functional requirements "*Subset access control (FDP\_ACC.1) [DESFire]*" and "*Security attribute based access control (FDP\_ACF.1) [DESFire]*" define the rules and "*Static attribute initialisation (FMT\_MSA.3) [DESFire]*" and "*Management of security attributes (FMT\_MSA.1) [DESFire]*" the attributes that the access control is based on.



The security functional requirement "*Management of TSF data (FMT\_MTD.1) [DESFire]*" provides the rules for the management of the authentication data.

The management functions are defined by "*Specification of Management Functions (FMT\_SMF.1) [DESFire]*".

Since the TOE stores data on behalf of the authorised subjects, import of user data with security attributes is defined by "*Import of user data with security attributes (FDP\_ITC.2) [DESFire]*".

Since cryptographic keys are used for authentication (refer to *O.Authentication-DESFire*), these keys have to be removed if they are no longer needed for the access control (i.e. an application is deleted). This is required by "*Cryptographic key destruction (FCS\_CKM.4) [DESFire]*". These nine SFRs together provide an access control mechanism as required by the objective *O.Access-Control-DESFire*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

416 The security functional requirement "*Unlinkability (FPR\_UNL.1) [DESFire]*" requires that unauthorised subjects other than the card holder are unable to determine whether any operation of the TOE were caused by the same user. This meets the objective *O.No-Trace-DESFire*.

**Security objective "Usage of hardware platform for DESFire (*O.Plat-Appl-DESFire*)"**

417 The justification related to the security objective "Usage of hardware platform for DESFire (*O.Plat-Appl-DESFire*)" is as follows:

418 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 for DESFire (*O.Resp-Appl-DESFire*)"**

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

420 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-DESFire* is fulfilled by the additional ST SFRs.

**Security objective “NVM resource availability for DESFire (*O.Resource-DESFire*)”**

421 The justification related to the security objective “Resource availability for DESFire (*O.Resource-DESFire*)” is as follows:

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

**Security objective “DESFire code integrity check (*O.Verification-DESFire*)”**

423 The justification related to the security objective “DESFire code integrity check (*O.Verification-DESFire*)” is as follows:

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

**Security objective “DESFire firewall (*O.Firewall-DESFire*)”**

425 The justification related to the security objective “DESFire firewall (*O.Firewall-DESFire*)” is as follows:

426 The security functional requirements "*Additional Security Functional Requirements common to DESFire and MFPlus*" and "*Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]*", supported by "*Static attribute initialisation (FMT\_MSA.3) [MIFARE\_FWL]*", require that no application can read, write, compare any piece of data or code belonging to DESFire. This meets the objective *O.Firewall-DESFire*.

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

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

428 The security functional requirement "*Subset residual information protection (FDP\_RIP.1) [DESFire]*" requires that the information content of a resource is made unavailable upon its deallocation from DESFire. This meets the objective *O.Shr-Res-DESFire*.

### 7.4.3 Additional security requirements are consistent

**"Cryptographic operation (*FCS\_COP.1*) & key generation (*FCS\_CKM.1*)"**

429 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]*)"**

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



**"Security roles ([FMT\\_SMR.1 \[MFPlus\]](#)),  
Subset access control ([FDP\\_ACC.1 \[MFPlus\]](#)),  
Security attribute based access control ([FDP\\_ACF.1 \[MFPlus\]](#)),  
Static attribute initialisation ([FMT\\_MSA.3 \[MFPlus\]](#)),  
Management of security attributes ([FMT\\_MSA.1 \[MFPlus\]](#)),  
Specification of TSF data ([FMT\\_MTD.1 \[MFPlus\]](#))  
Specification of management function ([FMT\\_SMF.1 \[MFPlus\]](#))  
Import of user data with security attributes ([FDP\\_ITC.2 \[MFPlus\]](#))  
Inter-TSF basic TSF data consistency ([FPT\\_TDC.1 \[MFPlus\]](#))  
Cryptographic key destruction ([FCS\\_CKM.4 \[MFPlus\]](#))"**

431 These security requirements have already been argued in [Section : Security objective "Access control for MFPlus \(O.Access-Control-MFPlus\)"](#) above.

**"User identification before any action ([FIA\\_UID.2 \[MFPlus\]](#)),  
User authentication before any action ([FIA\\_UAU.2 \[MFPlus\]](#)),  
Multiple authentication mechanisms ([FIA\\_UAU.5 \[MFPlus\]](#))"**

432 These security requirements have already been argued in [Section : Security objective "Authentication for MFPlus \(O.Authentication-MFPlus\)"](#) above.

**"Trusted path ([FPT\\_TRP.1 \[MFPlus\]](#)),  
Replay detection ([FPT\\_RPL.1 \[MFPlus\]](#))"**

433 These security requirements have already been argued in [Section : Security objective "MFPlus Integrity-protected Communication \(O.MAC-MFPlus\)"](#) above.

**"Unlinkability ([FPR\\_UNL.1 \[MFPlus\]](#))"**

434 This security requirement has already been argued in [Section : Security objective "Preventing traceability for MFPlus \(O.No-Trace-MFPlus\)"](#) above.

**"Minimum and maximum quotas ([FRU\\_RSA.2 \[MFPlus\]](#))"**

435 This security requirement has already been argued in [Section : Security objective "NVM resource availability for MFPlus \(O.Resource-MFPlus\)"](#) above.

**"Subset residual information protection ([FDP\\_RIP.1 \[MFPlus\]](#))"**

436 This security requirement has already been argued in [Section : Security objective "MFPlus data cleaning for resource sharing \(O.Shr-Var-MFPlus\)"](#) above.

**"Security roles ([FMT\\_SMR.1 \[DESFire\]](#)),  
Subset access control ([FDP\\_ACC.1 \[DESFire\]](#)),  
Security attribute based access control ([FDP\\_ACF.1 \[DESFire\]](#)),  
Static attribute initialisation ([FMT\\_MSA.3 \[DESFire\]](#)),  
Management of security attributes ([FMT\\_MSA.1 \[DESFire\]](#)),  
Specification of TSF data ([FMT\\_MTD.1 \[DESFire\]](#))  
Specification of management function ([FMT\\_SMF.1 \[DESFire\]](#))  
Import of user data with security attributes ([FDP\\_ITC.2 \[DESFire\]](#))  
Cryptographic key destruction ([FCS\\_CKM.4 \[DESFire\]](#))"**

437 These security requirements have already been argued in [Section : Security objective "Access control for DESFire \(O.Access-Control-DESFire\)"](#) above.

**"User identification before any action ([FIA\\_UID.2 \[DESFire\]](#)),  
User authentication before any action ([FIA\\_UAU.2 \[DESFire\]](#)),  
Multiple authentication mechanisms ([FIA\\_UAU.5 \[DESFire\]](#))"**

438 These security requirements have already been argued in [Section : Security objective "Authentication for DESFire \(O.Authentication-DESFire\)"](#) above.

**"Trusted path ([FPT\\_TRP.1 \[DESFire\]](#)),  
Replay detection ([FPT\\_RPL.1 \[DESFire\]](#))"**

439 These security requirements have already been argued in [Section : Security objective "DESFire Confidential Communication \(O.Confidentiality-DESFire\)"](#) above.

**"Inter-TSF basic TSF data consistency ([FPT\\_TDC.1 \[DESFire\]](#))"**

440 This security requirement has already been argued in [Section : Security objective "DESFire Data type consistency \(O.Type-Consistency-DESFire\)"](#) above.

**"Basic rollback ([FDP\\_ROL.1 \[DESFire\]](#))"**

441 This security requirement has already been argued in [Section : Security objective "DESFire Transaction mechanism \(O.Transaction-DESFire\)"](#) above.

**"Unlinkability ([FPR\\_UNL.1 \[DESFire\]](#))"**

442 This security requirement has already been argued in [Section : Security objective "Preventing traceability for DESFire \(O.No-Trace-DESFire\)"](#) above.

**"Minimum and maximum quotas ([FRU\\_RSA.2 \[DESFire\]](#))"**

443 This security requirement has already been argued in [Section : Security objective "NVM resource availability for DESFire \(O.Resource-DESFire\)"](#) above.

**"TSF testing ([FPT\\_TST.1 \[DESFire\]](#))"**

444 This security requirement has already been argued in [Section : Security objective "DESFire code integrity check \(O.Verification-DESFire\)"](#) above.

**"Subset access control ([FDP\\_ACC.1 \[MIFARE\\_FWL\]](#)),  
Security attribute based access control ([FDP\\_ACF.1 \[MIFARE\\_FWL\]](#)),  
Static attribute initialisation ([FMT\\_MSA.3 \[MIFARE\\_FWL\]](#)),**

445 These security requirements have already been argued in [Section : Security objective "DESFire firewall \(O.Firewall-DESFire\)"](#) above.

**"Subset residual information protection ([FDP\\_RIP.1 \[DESFire\]](#))"**

446 This security requirement has already been argued in [Section : Security objective "DESFire data cleaning for resource sharing \(O.Shr-Res-DESFire\)"](#) above.

#### 7.4.4 Dependencies of Security Functional Requirements

447 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 justified in [AUG](#) security requirements rationale,
- the dependency of [FCS\\_COP.1](#) and [FCS\\_CKM.1](#) on [FCS\\_CKM.4](#) (see discussion below).
- the dependency of [FMT\\_MSA.3 \[MIFARE\\_FWL\]](#) on [FMT\\_MSA.1](#) and [FMT\\_SMR.1](#) (see discussion below).

448 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 <a href="#">BSI-PP-0035</a> or in <a href="#">AUG</a>
FRU_FLT.2	FPT_FLS.1	Yes	Yes, <a href="#">BSI-PP-0035</a>
FPT_FLS.1	None	No dependency	Yes, <a href="#">BSI-PP-0035</a>
FMT_LIM.1	FMT_LIM.2	Yes	Yes, <a href="#">BSI-PP-0035</a>
FMT_LIM.2	FMT_LIM.1	Yes	Yes, <a href="#">BSI-PP-0035</a>
FAU_SAS.1	None	No dependency	Yes, <a href="#">BSI-PP-0035</a>
FPT_PHP.3	None	No dependency	Yes, <a href="#">BSI-PP-0035</a>
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, <a href="#">BSI-PP-0035</a>
FPT_ITT.1	None	No dependency	Yes, <a href="#">BSI-PP-0035</a>
FDP_IFC.1	FDP_IFF.1	No, see <a href="#">BSI-PP-0035</a>	Yes, <a href="#">BSI-PP-0035</a>
FCS_RNG.1	None	No dependency	Yes, <a href="#">BSI-PP-0035</a>
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, <a href="#">AUG #1</a>
	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	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_ACF.1 [Memories]	FDP_ACC.1 [Memories]	Yes, by FDP_ACC.2 [Memories]	Yes, <a href="#">AUG #4</a>
	FMT_MSA.3 [Memories]	Yes	

**Table 12. Dependencies of security functional requirements (continued)**

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FMT_MSA.3 [Memories]	FMT_MSA.1 [Memories]	Yes	Yes, <i>AUG #4</i>
	FMT_SMR.1 [Memories]	No, see <i>AUG #4</i>	
FMT_MSA.1 [Memories]	[FDP_ACC.1 [Memories] or FDP_IFC.1]	Yes, by FDP_ACC.2 [Memories] and FDP_IFC.1	Yes, <i>AUG #4</i>
	FMT_SMF.1 [Memories]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMR.1 [Memories]	No, see <i>AUG #4</i>	Yes, <i>AUG #4</i>
FMT_SMF.1 [Memories]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>
FMT_SMR.1 [MFPlus]	FIA_UID.1 [MFPlus]	Yes, by FIA_UID.2 [MFPlus]	<b>No</b> , <i>CCMB-2012-09-002</i>
FDP_ACC.1 [MFPlus]	FDP_ACF.1 [MFPlus]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
FDP_ACF.1 [MFPlus]	FDP_ACC.1 [MFPlus]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_MSA.3 [MFPlus]	Yes	
FMT_MSA.3 [MFPlus]	FMT_MSA.1 [MFPlus]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMR.1 [MFPlus]	Yes	
FMT_MSA.1 [MFPlus]	[FDP_ACC.1 [MFPlus] or FDP_IFC.1]	Yes, by FDP_ACC.1 [MFPlus]	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMF.1 [MFPlus]	Yes	
	FMT_SMR.1 [MFPlus]	Yes	
FMT_SMF.1 [MFPlus]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FDP_ITC.2 [MFPlus]	FDP_ACC.1 [MFPlus] or FDP_IFC.1	Yes, by FDP_ACC.1 [MFPlus]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
	FPT_ITC.1 or FPT_TRP.1 [MFPlus]	Yes, by FPT_TRP.1 [MFPlus]	
	FPT_TDC.1 [MFPlus]	Yes	
FPT_TDC.1 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FIA_UID.2 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FIA_UAU.2 [MFPlus]	FIA_UID.1	Yes, by FIA_UID.2 [MFPlus]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FIA_UAU.5 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FMT_MTD.1 [MFPlus]	FMT_SMR.1 [MFPlus]	Yes	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
	FMT_SMF.1 [MFPlus]	Yes	
FPT_TRP.1 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FCS_CKM.4 [MFPlus]	[FDP_ITC.1 or FDP_ITC.2 [MFPlus] or FCS_CKM.1]	Yes, by FDP_ITC.2 [MFPlus]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FPT_RPL.1 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FPR_UNL.1 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FRU_RSA.2 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_RIP.1 [MFPlus]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FMT_SMR.1 [DESFire]	FIA_UID.1 [DESFire]	Yes, by FIA_UID.2 [DESFire]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_ACC.1 [DESFire]	FDP_ACF.1 [DESFire]	Yes	<b>No</b> , <a href="#">CCMB-2012-09-002</a>

**Table 12. Dependencies of security functional requirements (continued)**

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FDP_ACF.1 [DESFire]	FDP_ACC.1 [DESFire]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_MSA.3 [DESFire]	Yes	
FMT_MSA.3 [DESFire]	FMT_MSA.1 [DESFire]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMR.1 [DESFire]	Yes	
FMT_MSA.1 [DESFire]	[FDP_ACC.1 [DESFire] or FDP_IFC.1]	Yes, by FDP_ACC.1 [DESFire]	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMF.1 [DESFire]	Yes	
	FMT_SMR.1 [DESFire]	Yes	
FMT_SMF.1 [DESFire]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>
FDP_ITC.2 [DESFire]	FDP_ACC.1 [DESFire] or FDP_IFC.1	Yes, by FDP_ACC.1 [DESFire]	<b>No</b> , <i>CCMB-2012-09-002</i>
	FPT_ITC.1 or FPT_TRP.1 [DESFire]	Yes, by FPT_TRP.1 [DESFire]	
	FPT_TDC.1 [DESFire]	Yes	
FPT_TDC.1 [DESFire]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>
FIA_UID.2 [DESFire]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>
FIA_UAU.2 [DESFire]	FIA_UID.1	Yes, by FIA_UID.2 [DESFire]	<b>No</b> , <i>CCMB-2012-09-002</i>
FIA_UAU.5 [DESFire]	None	No dependency	<b>No</b> , <i>CCMB-2012-09-002</i>
FMT_MTD.1 [DESFire]	FMT_SMR.1 [DESFire]	Yes	<b>No</b> , <i>CCMB-2012-09-002</i>
	FMT_SMF.1 [DESFire]	Yes	

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FPT_TRP.1 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FCS_CKM.4 [DESFire]	[FDP_ITC.1 or FDP_ITC.2 [DESFire] or FCS_CKM.1]	Yes, by FDP_ITC.2 [DESFire]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_ROL.1 [DESFire]	FDP_ACC.1 [DESFire] or FDP_IFC.1	Yes, by FDP_ACC.1 [DESFire]	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FPT_RPL.1 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FPR_UNL.1 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FPT_TST.1 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FRU_RSA.2 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_ACC.1 [MIFARE_FWL]	FDP_ACF.1 [MIFARE_FWL]	Yes	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
FDP_ACF.1 [MIFARE_FWL]	FDP_ACC.1 [MIFARE_FWL]	Yes	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
	FMT_MSA.3 [MIFARE_FWL]	Yes	
FMT_MSA.3 [MIFARE_FWL]	FMT_MSA.1	No, see discussion below	<b>No</b> , <a href="#">CCMB-2012-09-002</a>
	FMT_SMR.1	No, see discussion below	
FDP_RIP.1 [DESFire]	None	No dependency	<b>No</b> , <a href="#">CCMB-2012-09-002</a>

449 Part 2 of the Common Criteria defines the dependency of "[Cryptographic operation \(FCS\\_COP.1\)](#)" on "Import of user data without security attributes (FDP\_ITC.1)" or "Import of user data with security attributes (FDP\_ITC.2)" or "Cryptographic key generation (FCS\_CKM.1)". In this particular TOE, "[Cryptographic key generation \(FCS\\_CKM.1\)](#)" may be used for the purpose of creating cryptographic keys, but also, the ES has all possibilities to implement its own creation function, in conformance with its security policy.

450 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.

451 Part 2 of the Common Criteria defines the dependency of "[Static attribute initialisation \(FMT\\_MSA.3\) \[MIFARE\\_FWL\]](#)" on "Management of security attributes (FMT\_MSA.1)" and "Security roles (FMT\_SMR.1)". For this particular instantiation of the access control attributes aimed at protecting DESFire and MFPlus code and data from unauthorised accesses, the security attributes are only static, initialized at product start. Therefore, there is no need to identify management capabilities and associated roles in form of Security Functional Requirements "FMT\_MSA.1" and "FMT\_SMR.1".

## 7.4.5 Rationale for the Assurance Requirements

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

452 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.

453 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.

454 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.

455 In addition, the component ASE\_TSS.2 is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE. ASE\_TSS.2 is hierarchical to ASE\_TSS.1 which is part of all EAL defined in the Common Criteria.

456 Note that detailed and updated refinements for assurance requirements are given in [Section 7.3](#).

### Dependencies of assurance requirements

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

458 Since also ASE\_TSS.2 dependencies (ASE\_INT.1, ASE\_REQ.1 and ADV\_ARC.1) are fulfilled by the assurance requirements claimed by this ST, it is considered as consistent augmentation.

459 Augmentation to this package are identified in paragraph [356](#) and do not introduce dependencies not already satisfied by the EAL5 package.



## 8 TOE summary specification

460 This section demonstrates how the TOE meets each Security Functional Requirement, which will be further detailed in the ADV\_FSP documents.

461 The complete TOE summary specification has been presented and evaluated in the ST31 - K330A version H (dual or contactless mode only) with optional cryptographic library Neslib 3.2, and optional technology MIFARE® DESFire® EV1 2.2 , and optional technology MIFARE® Plus® S 1.3 SECURITY TARGET.

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

### 8.1 Limited fault tolerance (FRU\_FLT.2)

463 The TSF provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to random number generation, power supply, data flows and cryptographic operations, thus preventing risk of malfunction.

### 8.2 Failure with preservation of secure state (FPT\_FLS.1)

464 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,
- Sequence control,
- etc..

465 The ES can generate a software reset.

### 8.3 Limited capabilities (FMT\_LIM.1)

466 The TSF ensures that only very limited test capabilities are available in USER configuration, in accordance with SFP\_1: Limited capability and availability Policy.

### 8.4 Limited availability (FMT\_LIM.2)

467 The TOE is either in TEST or USER configuration.

468 The only authorised TOE configuration modification is:

- TEST to USER configuration.

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

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

## 8.5 Audit storage (FAU\_SAS.1)

471 In User configuration, the TOE provides commands to store data and/or pre-personalisation data and/or supplements of the ES in the NVM. These commands are only available to authorized processes, and only until phase 6.

## 8.6 Resistance to physical attack (FPT\_PHP.3)

472 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.

## 8.7 Basic internal transfer protection (FDP\_ITT.1), Basic internal TSF data transfer protection (FPT\_ITT.1) & Subset information flow control (FDP\_IFC.1)

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

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

## 8.8 Random number generation (FCS\_RNG.1)

474 The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the [BSI-AIS31](#) standard for a P2 class device.

## 8.9 Cryptographic operation: DES / 3DES operation (FCS\_COP.1 [EDES])

475 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](#).

476 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](#).

## 8.10 Cryptographic operation: AES operation (FCS\_COP.1 [AES])

477 The AES accelerator provides the following standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to [FIPS PUB 197](#) with intrinsic counter-measures against attacks:

- randomize,
- key expansion,
- cipher,
- inverse cipher.

## 8.11 Cryptographic operation: RSA operation (FCS\_COP.1 [RSA]) if **Neslib** only

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

479 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: Elliptic Curves Cryptography operation (FCS\_COP.1 [ECC]) if **Neslib** only

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

- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check,
- Jacobian conversion to affine coordinates,
- general point addition,
- point expansion and compression.

## 8.13 Cryptographic operation: SHA operation (FCS\_COP.1 [SHA]) if **Neslib** only

481 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](#).

482 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.

### 8.14 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

483 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.

### 8.15 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

484 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.

### 8.16 Static attribute initialisation (FMT\_MSA.3) [Memories]

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

### 8.17 Management of security attributes (FMT\_MSA.1) [Memories] & Specification of management functions (FMT\_SMF.1) [Memories]

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

### 8.18 Complete access control (FDP\_ACC.2) [Memories] & Security attribute based access control (FDP\_ACF.1) [Memories]

487 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.

### 8.19 Security roles (FMT\_SMR.1) [MFPlus]

488 MFPlus identifies the user to be authenticated by the key block number indicated in the authentication request.

- 489 In security level 0 when the TOE is in a secure environment, MFPlus identifies and authenticates the role Personaliser by default ; in addition the role Originality Key User can be identified with an explicit authentication request.
- 490 In the other security levels, MFPlus identifies and authenticates the role Anybody by default and before any authentication request.  
The roles Card Administrator, Card Manager, Card Security Level Manager, Card User and Originality Key User are authenticated during the authentication request by the knowledge of the respective cryptographic keys.

## 8.20 Subset access control (FDP\_ACC.1) [MFPlus]

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

## 8.21 Security attribute based access control (FDP\_ACF.1) [MFPlus]

- 492 The MFPlus library verifies the MFPlus security attributes during the execution of MFPlus commands to enforce the MFPlus Access Control Policy defined by the MFPlus interface specification:
- 493 MFPlus assigns Card Users to 2 different groups of operations on blocks. The operations are "read" or "write".  
There are several sets of predefined access conditions which may be assigned to each sector. These sets can also contain the access condition "never" for one group of operations. Card Users can also modify the sector trailer or the AES sector keys, if the access conditions allow this.
- 494 The Originality Key User is not allowed to perform any action on objects, but with a successful authentication he can prove the authenticity of the Card.
- 495 The Card Administrator can change the Level 3 Switch Key and the Card Master Key.
- 496 The Card Manager can modify the Field Configuration Block, which are attributes that may have to be changed in the field. He is also allowed to change the Card Configuration Key.
- 497 The Card Security Level Manager can switch the security level of the card to level 3 by authenticating with the corresponding key.

## 8.22 Static attribute initialisation (FMT\_MSA.3) [MFPlus]

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

## 8.23 Management of security attributes (FMT\_MSA.1) [MFPlus]

- 499 The MFPlus library verifies the MFPlus security attributes during the execution of MFPlus commands to enforce the Access Control Policy on the security attributes.

## 8.24 Specification of Management Functions (FMT\_SMF.1) [MFPlus]

500 The MFPlus library implements the management functions defined by the MFPlus interface specifications for authentication, and changing security attributes.

## 8.25 Import of user data with security attributes (FDP\_ITC.2) [MFPlus]

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

## 8.26 Inter-TSF basic TSF data consistency (FPT\_TDC.1) [MFPlus]

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

## 8.27 Cryptographic key destruction (FCS\_CKM.4) [MFPlus]

503 The MFPlus library erases key values from memory after their context becomes obsolete.

## 8.28 User identification before any action (FIA\_UID.2) [MFPlus]

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

## 8.29 User authentication before any action (FIA\_UAU.2) [MFPlus]

505 During the authentication, the MFPlus library verifies that the user knows the selected key. This is performed by verifying an encryption, thus preventing to unveil the key.

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

## 8.30 Multiple authentication mechanisms (FIA\_UAU.5) [MFPlus]

507 The MFPlus library implements the MFPlus Interface Specification, that has a mechanism to authenticate Card Administrator, Card Manager, Card Security Level Manager, Card User, and Originality Key User, while Everybody is assumed when there is no valid authentication state.

## 8.31 Management of TSF data (FMT\_MTD.1) [MFPlus]

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

### 8.32 Trusted path (FTP\_TRP.1) [MFPlus]

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

510 The mechanisms include encryption of keys and CMAC on commands and responses.

### 8.33 Replay detection (FPT\_RPL.1) [MFPlus]

511 The MFPlus library implements the MFPlus authentication command, and authenticated commands, that allow replay detection.

### 8.34 Unlinkability (FPR\_UNL.1) [MFPlus]

512 MFPlus provides an Administrator option to use random UID during the ISO 14443 anti-collision sequence, preventing the traceability through UID. At higher level, the MFPlus access control - when configured for this purpose - provides traceability protection.

### 8.35 Minimum and maximum quotas (FRU\_RSA.2) [MFPlus]

513 The MFPlus library ensures the memory required for its operation is available.

### 8.36 Subset residual information protection (FDP\_RIP.1) [MFPlus]

514 At the end of commands execution or upon interrupt, the MFPlus library cleans the confidential data from registers it uses.

### 8.37 Security roles (FMT\_SMR.1) [DESFire]

515 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.

### 8.38 Subset access control (FDP\_ACC.1) [DESFire]

516 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.

### 8.39 Security attribute based access control (FDP\_ACF.1) [DESFire]

517 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.

**8.40 Static attribute initialisation (FMT\_MSA.3) [DESFire]**

518 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.

**8.41 Management of security attributes (FMT\_MSA.1) [DESFire]**

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

**8.42 Specification of Management Functions (FMT\_SMF.1) [DESFire]**

520 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.

**8.43 Import of user data with security attributes (FDP\_ITC.2) [DESFire]**

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

**8.44 Inter-TSF basic TSF data consistency (FPT\_TDC.1) [DESFire]**

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

**8.45 Cryptographic key destruction (FCS\_CKM.4) [DESFire]**

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

**8.46 User identification before any action (FIA\_UID.2) [DESFire]**

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

**8.47 User authentication before any action (FIA\_UAU.2) [DESFire]**

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

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



## 8.48 Multiple authentication mechanisms (FIA\_UAU.5) [DESFire]

527 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.

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

## 8.49 Management of TSF data (FMT\_MTD.1) [DESFire]

529 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.

## 8.50 Trusted path (FTP\_TRP.1) [DESFire]

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

## 8.51 Basic rollback (FDP\_ROL.1) [DESFire]

531 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.

## 8.52 Replay detection (FPT\_RPL.1) [DESFire]

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

## 8.53 Unlinkability (FPR\_UNL.1) [DESFire]

533 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.

## 8.54 TSF testing (FPT\_TST.1) [DESFire]

534 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.

## 8.55 Minimum and maximum quotas (FRU\_RSA.2) [DESFire]

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

**8.56 Subset residual information protection (FDP\_RIP.1) [DESFire]**

536 At the end of commands execution or upon interrupt, the DESFire library cleans the confidential data from registers it uses.

**8.57 Subset access control (FDP\_ACC.1) [MIFARE\_FWL] & Security attribute based access control (FDP\_ACF.1) [MIFARE\_FWL]**

537 The Library Protection Unit is used to isolate the DESFire and MFPlus firmware (code and data) from the rest of the code embedded in the device.

**8.58 Static attribute initialisation (FMT\_MSA.3) [MIFARE\_FWL]**

538 At product start, all the static attributes are initialised, which are needed to protect the segments where DESFire and MFPlus code and data are stored.

## 9 References

### 539 Protection Profile references

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

### 540 ST31 - K330A Security Target reference

Component description	Reference
ST31 - K330A version H (dual or contactless mode only) with optional cryptographic library Neslib 3.2, and optional technology MIFARE® DESFire® EV1 2.2 , and optional technology MIFARE® Plus® S 1.3 SECURITY TARGET	SMD_MR31Zxxx_ST_13_001

### 541 Guidance documentation references

Component description	Reference	Revision
ST31 - K330 platform - Sx31Zxxx, Mx31Zxxx - Secure dual interface microcontroller with enhanced security and up to 52 Kbytes of EEPROM - Datasheet	DS_SR31Z052	4
ST31 - K330 platform die description	DD_31Z052	4
ARM SC000 Technical Reference Manual - R0P0	ARM DDI 0456	A
ARM v6-M Architecture Reference Manual	ARM DDI 0419	C
ST31 - K330 Security guidance	AN_SECU_ST31_K330	4
ST31 - AIS31 Compliant Random Number user manual	UM_31_AIS31	2
ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note	AN_31_AIS31	2
ST31 NesLib cryptographic library User manual	UM_31_NESLIB_3.2	7
ST31-K330 and ST33-K8H0 secure microcontrollers - Power supply glitch detector characteristics	AN_31_GLITCH	2
Application note - ST31-K330 Dual Interface Secure MCUs - Recommendation for contactless operations	AN_31_RCMD	2
MIFARE DESFire EV1 library 2.2 - User manual	UM_MIFARE_DESFire_EV1_2.2	2
MIFARE DESFire EV1 interface specification	UM_MIFARE_DESFire_EV1_Interface	2

Component description	Reference	Revision
MIFARE Plus S library 1.3 for ST31-K330 - User manual	UM_31_MIFARE_PLUS_S_1.3.0	1
MIFARE Plus S interface specification	UM_MIFARE_PLUS_S	1

542

## Standards references

Ref	Identifier	Description
[1]	BSI-AIS31	A proposal for functionality classes and evaluation methodology for true (physical) random number generators, W. Killmann & W. Schindler BSI, Version 3.1, 25-09-2001
[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
[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

Ref	Identifier	Description
[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.
DESFire	MIFARE® DESFire® EV1.
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.
MFPlus	MIFARE® Plus® S.
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.



**Table 13. List of abbreviations (continued)**

Term	Meaning
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or <a href="#">Security Target</a> .
TOE	<a href="#">Target of Evaluation</a> .
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	<a href="#">TSF Scope of Control</a> .
TSF	<a href="#">TOE Security Functionality</a> .
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.

## 10 Revision history

**Table 14. Document revision history**

Date	Revision	Changes
19-Mar-2013	01.00	Initial release.
06-Jun-2013	01.01	Change in references.
28-Mar-2014	02.00	Addition of MIFARE Plus S. Changes in site list.
28-Aug-2014	02.01	Changes in site list. Change in TOE identification table format. Change in revisions.
12-Dec-2014	02.02	Typo correction.

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.

© 2014 STMicroelectronics - All rights reserved

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](http://www.st.com)

