STMicroelectronics

ST31P450 B02 including optional cryptographic library NESLIB, and optional technology MIFARE Plus® EV1 Security Target for composition

Common Criteria for IT security evaluation

SMD_ST31P450_ST_19_002 Rev B02.0

January 2020

www.st.com

BLANK

ST31P450 B02 platform Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: ST31P450 B02 including optional cryptographic library NesLib, and optional technology MIFARE Plus® EV1 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev B02.0, issued in January 2020.

3 Registration: registered at ST Microelectronics under number SMD_ST31P450_ST_19_002.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the **ST31P450 B02** Security Integrated Circuit (IC), designed on the **ST31 platform of STMicroelectronics**, with firmware version 3.1.1 and 3.1.2, optional cryptographic library **NesLib 6.4.7,** and optional technology **MIFARE Plus® EV1**[a] **1.1.2**.

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

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

a. MIFARE and MIFARE Plus are registered trademarks of NXP B.V. and are used under license.

Contents

List of tables

List of figures

1.3 Context

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

8 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by 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 "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*" (PP) registered and certified under the reference *BSI-CC-PP-0084-2014* in the German IT Security Evaluation and Certification Scheme, ***with the following augmentations***:

- Addition #1: “Support of Cipher Schemes” from *AUG*
- Addition #4: “Area based Memory Access Control” from *AUG*
- Additions specific to this Security Target, some in compliance with *ANSSI-CC-NOTE-06/2.0 EN* and *ANSSI-CC-CER/F/06.002*.

The original text of this PP is typeset as indicated here, its augmentations from *AUG* as indicated here, and text originating in *ANSSI-CC-NOTE-06/2.0 EN* and *ANSSI-CC-CER/F/06.002* as indicated here, when they are reproduced in this document.

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

- Authentication of the Security IC
- Loader dedicated for usage in secured environment only
- Loader dedicated for usage by authorized users only.

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

12 This ST makes various refinements to the above mentioned PP and *AUG*. They are all properly identified in the text typeset as ***indicated here*** or ~~here~~. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: ***BSI*** for *BSI-CC-PP-0084-2014*, ***AUG1*** for Addition #1 of *AUG*, ***AUG4*** for Addition #4 of *AUG*., and ***ANSSI*** for *ANSSI-CC-NOTE-06/2.0 EN* and *ANSSI-CC-CER/F/06.002*.

1.4 TOE identification

13 The Target of Evaluation (TOE) is the ST31P450 B02 platform.

14 “ST31P450 B02” completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 15: Guidance documentation*, and its development and production sites indicated in *Table 16: Sites list*.

15 B02 is the version of the evaluated platform. Any change in the TOE components, the guidance documentation and the list of sites leads to a new version of the evaluated platform, thus a new TOE.

Table 1. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	Optional NesLib crypto library version	Optional MIFARE Plus EV1 version
K410A	C	0x01F1	3.1.1 and 3.1.2	6.4.7	1.1.2

1. Part of the product information.

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

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

18 In this Security Target, the term "MFPlus" means MIFARE Plus® EV1 1.1.2.

1.5 TOE overview

19 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.

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

- either by ST during the manufacturing or packaging process,
- or by the customer during the packaging, or composite product integration, or personnalisation process.

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

22 The configuration of the derivative devices can impact the I/O mode, the available NVM size, and the availability of MIFARE support feature, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
I/O mode	Contact only, Dual mode, Contactless only
NVM size	320 or 450 Kbytes
MIFARE support (Crypto1)	Active if MIFARE, Inactive if not

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

24 The Master identification number is unique for all product configurations.
Each derivative device has a specific Child product identification number, also part of the

product information, and specified in the Data Sheet and in the Firmware User Manual, referenced in *Table 15*.

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

26 In a few words, the ST31P450 B02 offers a unique combination of high performances and very powerful features for high level security:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- Hardware 3-key Triple DES accelerator,
- Hardware AES accelerator,
- ISO/IEC 13239 CRC calculation block,
- NExt Step CRYPTography accelerator (NESCRYPT),
- optional cryptographic library (NesLib 6.4.7),
- optional secure MIFARE Plus® EV1 library.

1.6 TOE description

1.6.1 TOE hardware description

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

28 The AES (Advanced Encryption Standard *[6]*) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in Electronic CodeBook (ECB) or Cipher Block Chaining (CBC) modes.

29 The 3-key triple DES accelerator (EDES+) supports efficiently the Triple Data Encryption Standard (TDES *[2]*), enabling Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes and DES computation.
Note that a triple DES can be performed by a triple DES computation or by 3 single DES computations.

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

31 The TOE offers 10 Kbytes of User RAM and up to 450 Kbytes of secure User high-density Flash memory (NVM).

32 As randomness is a key stone in many applications, the ST31P450 B02 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 *[1]* and directly accessible thru dedicated registers.

33 Three general-purpose timers are available as well as a watchdog timer.

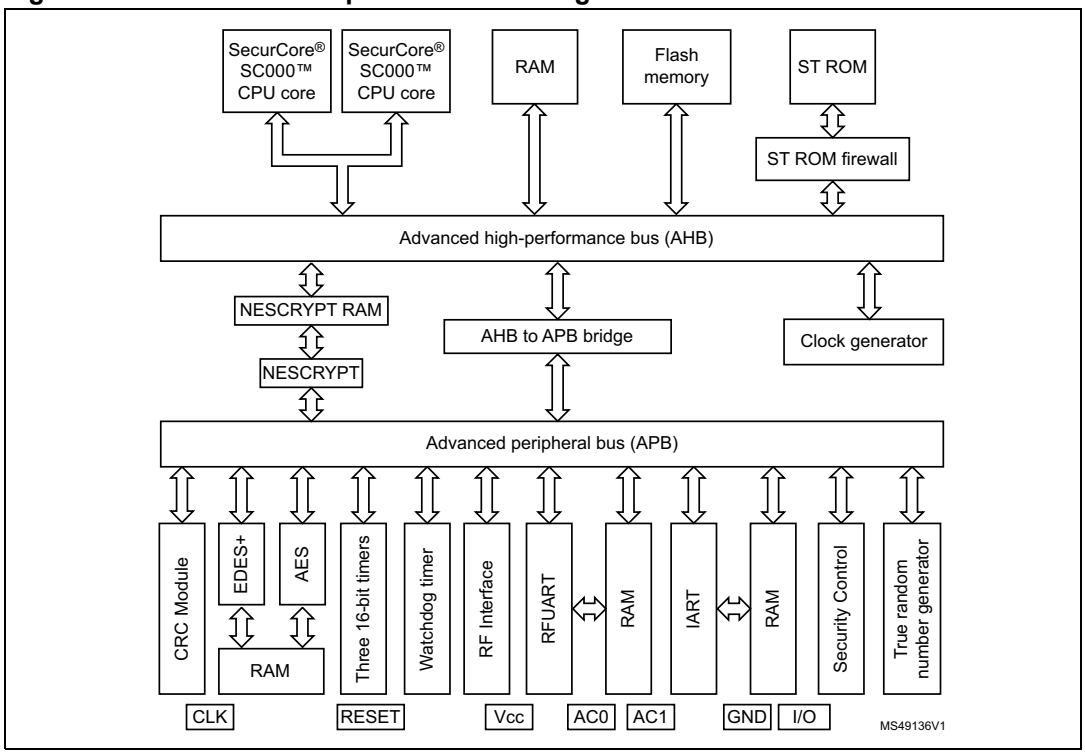
34 The TOE offers a contact serial communication interface fully compatible with the ISO/IEC 7816-3 standard, and a contactless interface including an RF Universal Asynchronous Receiver Transmitter (RF UART), enabling communication up to 848 Kbits/s compatible with

the ISO/IEC 14443 Type A and PayPass™ standard.
These interfaces can be used simultaneously (dual mode), or the contact interface can be deactivated (see *Table 2: Derivative devices configuration possibilities*).

35 The detailed features of this TOE are described in the Data Sheet and in the Cortex SC000 Technical Reference Manual, referenced in *Table 15*.

36 *Figure 1* provides an overview of the ST31P450 B02 platform.

Figure 1. ST31P450 B02 platform block diagram



1.6.2 TOE software description

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

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

- a Secure Flash Loader, enabling to securely and efficiently download the Security IC Embedded Software (ES) into the NVM. It also allows the evaluator to load software into the TOE for test purpose. The Secure Flash Loader is available in Admin

configuration. The customer can choose to activate it in any phase of the product life-cycle under highly secured conditions, or to deactivate it definitely at a certain step.

- low-level functions called Flash Drivers, enabling the Security IC Embedded Software (ES) to modify and manage the NVM contents. The Flash Drivers are available in User configuration.
- a set of protected commands for device testing and product profiling, not intended for the Security IC Embedded Software (ES) usage, and not available in User configuration.
- a very reduced set of uncritical commands for basic diagnostic purpose (field return analysis), only reserved to STMicroelectronics.
- a set of highly protected commands for secure diagnostic purpose (advanced quality investigations), that can only be activated by the customer and be operated by STMicroelectronics on its own audited sites. This feature is protected by specific strong access control, completed by environmental measures which prevent access to customer assets. Furthermore, it can be permanently deactivated by the customer.

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

NesLib is embedded by the ES developer in his applicative code.

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

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[17]*), and Diffie-Hellman *[23]*,
- an asymmetric key cryptographic support module that provides very efficient basic functions to build up protocols using Elliptic Curves Cryptography on prime fields GF(p) with elliptic curves in short Weierstrass form *[15]*, and provides support for ECDH key agreement *[21]* and ECDSA generation and verification *[5]*.
- a module for supporting elliptic curve cryptography on Edwards curve 25519, in particular ed25519 signature generation, verification and point decompression *[26]*.
- a cryptographic support module that provides hash functions (SHA-1[a], SHA-2 *[4]*), SHA-3, Keccak and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3 *[25]*,
- a symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard cryptographic algorithm (DES) *[2]*,
- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES) *[6]*,
- support for Deterministic Random Bit Generators *[19]*,
- prime number generation and RSA key pairs generation *[3]*.

40 The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is a MIFARE technology library.

41 This secure library is called MIFARE Plus® EV1. 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

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

and conditions.

MFPlus is embedded on the TOE by ST.
Note that MFPlus can only be used if MIFARE support is active.

42 MFPlus offers three different security levels. The higher the security level, the more secure the MFPlus Software is intended to be.
The main features of each security level are listed below:

- Security level 0 (SL0): The TOE does not provide any functionality besides initialization. The TOE is initialized in plaintext, especially keys for the further levels can be brought in. A TOE in SL0 is not usable for other purposes. After all mandatory keys and security attributes have been stored in the card, it can be switched to SL1 or SL3.
  Note: SL0 supports both ISO14443-3 and ISO1SO14443-4 protocol communication. ISO14443-3 communication is never in scope of the evaluation. Proximity Check, Virtual Card Architecture are also out of scope. Personalization and Originality Check are in scope.
- Security level 1 (SL1): Different functionality is provided in ISO14443-3 and ISO14443-4 communication.
  In ISO14443-3 communication (the MIFARE Classic compatibility mode), the card user can access the blocks in the TOE after an authentication procedure, update the security attributes, update the authentication data. 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. This mode does not implement any Security Functional Requirement and is therefore not in the scope of the evaluation.
  In ISO14443-4 communication, the TOE can be switched to SL3, dedicated Sectors can be switched to SL or SL1SL3Mix. Both actions require preceding authentication using the AES algorithm with the appropriate key. In addition some security attributes and authentication data can be updated using SL3 commands. For sectors in SL3 or SL1SL3Mix, their sector trailer and keys can be updated using SL3 commands.
  Note: The only functionality provided by SL1 that is within the scope of the evaluation, is the Originality Check, updating security attributes and authentication data and the switching of the Card or Sector Security Level. Proximity Check, Virtual Card Architecture, data access of sectors in SL3 or SL1SL3Mix, are out of scope.
- Security level 3 (SL3): The card user can access the data and value blocks in the TOE after an authentication procedure based on the AES algorithm. The communication with the card terminal can be protected with secure messaging. The authentication and the secure messaging are security services of the TOE. The TOE cannot be switched to a different Security Level. In SL3, the TOE offers two secure messaging modes: EV0 Secure Messaging and EV1 Secure Messaging. Only the ISO14443-4 protocol is supported.
  Note: All functionality provided by Security Level 3 is within the scope of the evaluation, except Proximity Check .

43 In all security levels, the TOE does additionally support the so-called originality function which allows verifying the authenticity of the TOE.

44 For SL1 the SecurityLevel for the TOE as a whole, as well as the SectorSecurityLevels for dedicated Sectors can be switched to a higher level. A migration, both at TOE or at Sector level, is only possible to a higher level and not to a lower one. In case dedicated sectors have been migrated to higher Sector Security Levels, the overall TOE behavior must remain by default according to the lowest Sector Security Level among all Sectors of the TOE. If the

TOE is in SL0, this must always hold for the whole TOE, which means that all Sectors are in Sector Security Level 0.

45 In MFPlus, the TOE supports the virtual card architecture by providing a selection mechanism for virtual cards. This allows using the TOE in a complex environment where multiple virtual cards are stored in one physical object, however the TOE does support only one virtual card.

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

47 **Note**: The ES is not part of the TOE and is out of scope of the evaluation, except NesLib and MIFARE Plus EV1 when they are embedded.

1.6.3 TOE documentation

48 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,
- the Firmware user manual,
- the Flash loader installation guide,
- optionally the NesLib user manual,
- optionally the MIFARE Plus EV1 user manual.

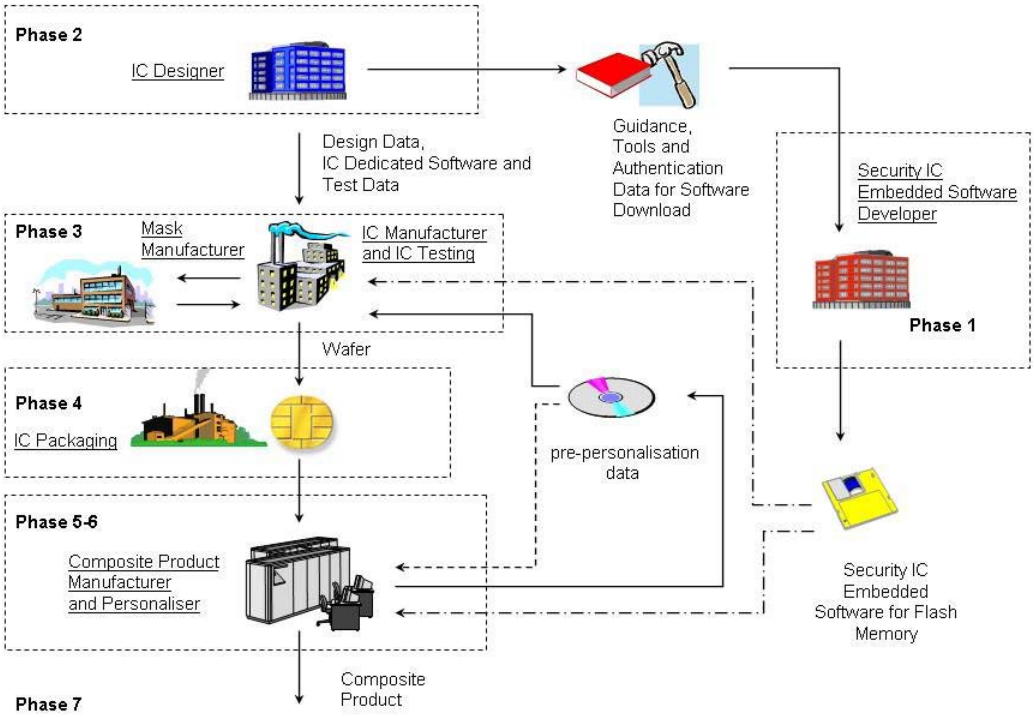
49 The complete list of guidance documents is detailed in *Table 15*.

1.7 TOE life cycle

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

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

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



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

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

54 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.

55 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.

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

57 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.

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

Table 3. Composite product life cycle phases

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

1.8 TOE environment

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

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

1.8.1 TOE Development Environment (Phase 2)

60 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.

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

62 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).

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

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

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

1.8.2 TOE production environment

66 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.

Phase 3

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

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

69 The authorized EWS plant potentially involved in the testing of the TOE are denoted by the activity “EWS” in *Table 16*.

70 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.

Phase 4

71 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.

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

73 All sites denoted by the activity “WHS” in *Table 16* can be involved for the logistics during phase 3 or 4.

1.8.3 TOE operational environment

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

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

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

2 Conformance claims (ASE_CCL, ASE_ECD)

2.1 Common Criteria conformance claims

77 The ST31P450 B02 platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

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

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

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

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

80 The assurance level for the ST31P450 B02 platform Security Target is ***EAL5*** augmented by ASE_TSS.2, ALC_DVS.2 and AVA_VAN.5.

2.2 PP Claims

2.2.1 PP Reference

81 The ST31P450 B02 platform Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

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

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

2.2.2 PP Additions

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

- Addition #4: “Area based Memory Access Control” from *AUG*,
- Addition #1: “Support of Cipher Schemes” from *AUG*,
- Specific additions for the Secure Flash Loader, to comply with *ANSSI-CC-NOTE-06/2.0 EN* and *ANSSI-CC-CER/F/06.002*,
- Specific additions for the Secure Diagnostic capability,
- Specific additions for MFPlus,
- Refinement of assurance requirements.

84 All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-CC-PP-0084-2014* being typeset as indicated here and ~~here~~. Text originating in *AUG* is typeset as indicated here. Text originating in *ANSSI-CC-NOTE-06/2.0 EN* and *ANSSI-CC-CER/F/06.002* is typeset as indicated here.

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

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

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

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

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

2.2.3 PP Claims rationale

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

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

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

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

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

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

3 Security problem definition (ASE_SPD)

96 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.

97 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3. Only those originating in *AUG* or in *ANSSI-CC-NOTE-06/2.0 EN* / *ANSSI-CC-CER/F/06.002*, and the ones introduced in this Security Target, are detailed in the following sections.

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

Table 4. Summary of security aspects

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
	BSI.T.Masquerade-TOE	Masquerade the TOE
	AUG4.T.Mem-Access	Memory Access Violation
	ANSSI.T.Open-Samples-Diffusion	Diffusion of open samples
	T.Data-Modification-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 availability

Table 4. Summary of security aspects (continued)

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

3.1 Description of assets

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

100 The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks and product in any form,
- the TOE correct operation,
- the Security IC Embedded Software, stored in the TOE's protected memories and in operation,
- the security services provided by the TOE for the Security IC Embedded Software,
- the cryptographic co-processors for Triple-DES and AES, the random number generator,
- the TSF Data.

101 Application note:
The TOE providing a functionality for Security IC Embedded Software secure loading into NVM, the ES is considered as User Data being stored in the TOE's memories at this step, and the Protection Profile corresponding packages are integrated, as well as the requirements from *ANSSI-CC-NOTE-06/2.0 EN*.

3.2 Threats

102 The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.
Only those originating in *AUG*, *ANSSI-CC-CER/F/06.002*, and those related to 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
BSI.T.Masquerade-TOE	Masquerade the TOE
AUG4.T.Mem-Access	Memory Access Violation: Parts of the ***Security IC*** Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the ***Security IC*** Embedded Software. Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access. Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

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

103 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: Application data and code 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	MFPlus data confidentiality: 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.
T.Integ-Applic-Code-MFPlus	MFPlus code integrity: 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.

T.Integ-Applic-Data-MFPlus	MFPlus data integrity: 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.
T.Application-Resource-MFPlus	MFPlus resource availability: 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.

3.3 Organisational security policies

104 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.

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

106 *BSI.P.Lim-Block-Loader* and *BSI.P.Ctrl-Loader* are dedicated to the Secure Flash Loader, and described in the *BSI-CC-PP-0084-2014* packages "Loader dedicated for usage in secured environment only" and "Loader dedicated for usage by authorized users only". *BSI.P.Ctrl-Loader* has been completed in accordance with *ANSSI-CC-NOTE-06/2.0 EN*.

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

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

109 P.Confidentiality, P.MAC and P.No-Trace are related to MFPlus, and valid in case MFPlus is embbeded in the TOE.

110 P.Resp-Appl are related to the ES that is part of the evaluation (NesLib and/or MFPlus), and valid in case NesLib or MFPlus is embedded in the TOE.

BSI.P.Process-TOE	Identification during TOE Development and Production: An accurate identification ***is*** established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

BSI.P.Lim-Block-Loader Limiting and blocking the loader functionality:

The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader(1) in order to protect stored data from disclosure and manipulation.

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

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

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

The activation of the loaded Additional ~~Code~~ ***user data*** is possible if:

– integrity and authenticity of the Additional ~~Code~~ ***user data*** have been successfully checked;

– the loaded ~~Additional Code~~ ***user data*** is targeted to the Initial TOE (Identification ~~Data~~ of the Additional ~~Code~~ ***user data*** and the Initial TOE will be used for this check).

Identification ~~Data~~ of the resulting Final TOE shall identify the Initial TOE and the ~~activated~~ Additional ~~Code~~ ***user data***. Identification Data shall be protected in integrity.

Note: Here, the term TOE denotes the TOE itself as well as the composite TOE which both may be maintained by loading of data.

AUG1.P.Add-Functions	Additional Specific Security Functionality: The TOE shall provide the following specific security functionality to the Security IC Embedded Software: – Triple Data Encryption Standard (TDES), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded**,** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded**,** – Rivest-Shamir-Adleman (RSA)**,** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, – ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded. Note that SHA-1 is no longer recommended as a cryptographic function. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.
P.Encryption	Confidentiality during communication (if MFPlus): The TOE shall provide the possibility to protect selected data elements from eavesdropping during contact-less communication.
P.MAC	Integrity during communication (if 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	Un-traceability of end-users (if 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.Resp-Appl	Treatment of user data: The Security IC Embedded Software, part of the TOE, treats user data according to the assumption A.Resp-Appl defined in *BSI-CC-PP-0084-2014*.

3.4 Assumptions

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

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

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

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

114 The following assumptions are valid in case MFPlus is embedded in the TOE.

A.Secure-Values	Usage of secure values (if 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	Terminal support to ensure integrity, confidentiality and use of random numbers (if MFPlus): The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. Furthermore, the terminal shall provide random numbers according to AIS20 or AIS31 *[1]*.

4 Security objectives (ASE_OBJ)

115 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.

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

117 Note that the origin of each objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *BSI-CC-PP-0084-2014*, sections 4.1 and 7.3. Only those which have been amended, those originating in *AUG*, those originating in *ANSSI-CC-NOTE-06/2.0 EN*, and the ones introduced in this Security Target, are detailed in the following sections.

Table 5. Summary of security objectives

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

Table 5. Summary of security objectives (continued)

	Label	Title
TOE	*O.Access-Control-MFPlus*	Access Control for MFPlus
	O.Authentication-MFPlus	Authentication for MFPlus
	O.Encryption-MFPlus	MFPlus Confidential Communication
	O.MAC-MFPlus	MFPlus integrity-protected Communication
	O.Type-Consistency-MFPlus	MFPlus Data type consistency
	O.No-Trace-MFPlus	Preventing Traceability 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
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader
	BSI.OE.Loader-Usage	Secure communication and usage of the Loader
	BSI.OE.TOE-Auth	External entities authenticating of the TOE
	OE.Composite-TOE-Id	Composite TOE identification
	OE.TOE-Id	TOE identification
	OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic
	OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic
	OE.Secure-Values	Generation of secure values
	OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers

4.1 Security objectives for the TOE

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

BSI.O.Phys-Probing Protection against Physical Probing

BSI.O.Malfunction Protection against Malfunctions

BSI.O.Phys-Manipulation	Protection against Physical Manipulation
BSI.O.Leak-Forced	Protection against Forced Information Leakage
BSI.O.Abuse-Func	Protection against Abuse of Functionality
BSI.O.Identification	TOE Identification
BSI.O.RND	Random Numbers
BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader
BSI.O.Authentication	Authentication to external entities
ANSSI.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF: The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit, …) through the use of a dedicated code loaded on open samples.
ANSSI.O.Secure-Load-ACode	Secure loading of the Additional Code: The Loader of the ~~Initial~~ TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure. Note: Concretely, the TOE manages the Additional Code as a Memory Image.
ANSSI.O.Secure-AC-Activation	Secure activation of the Additional Code: Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.

ANSSI.O.TOE-Identification	Secure identification of the TOE: The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional TOE. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.
O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image: The Loader of the TOE shall check an evidence of authenticity and integrity of the loaded Memory Image. The Loader enforces that only the allowed version of the Additional Memory Image can be loaded after the Initial Memory Image. The Loader shall forbid the loading of an Additional Memory Image not intended to be assembled with the Initial Memory Image. Note: This objective is similar to ANSSI.O.Secure-Load-ACode, applied to user data (e.g. embedded software).
O.MemImage-Identification	Secure identification of the Memory Image: The Identification Data identifies the Initial Memory Image and Additional Memory Image. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. Storage of the Additional Memory Image and update of the Identification Data shall be performed at the same time in an Atomic way, otherwise (in case of interruption or incident which prevents this alignment), the Memory Image shall remain in its initial state or the TOE shall fail secure. The Identification Data of the Final Memory Image allows identifications of Initial Memory Image and Additional Memory Image. Note: This objective is similar to ANSSI.O.Secure-AC-Activation and ANSSI.O.TOE-Identification, applied to user data (e.g. embedded software).

AUG1.O.Add-Functions	Additional Specific Security Functionality: The TOE must provide the following specific security functionality to the ***Security IC*** Embedded Software: – Triple Data Encryption Standard (TDES), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded**,** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded**,** – Rivest-Shamir-Adleman (RSA)**,** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, **–** ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded**.** Note that SHA-1 is no longer recommended as a cryptographic function. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.
AUG4.O.Mem-Access	Area based Memory Access Control: The TOE must provide the ***Security IC*** Embedded Software with the capability to define access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

118 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 application elements and to reading and modifying security attributes. 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.Encryption-MFPlus	MFPlus Confidential Communication: The TOE must be able to protect the communication by encryption. This shall be implemented by security attributes that enforce encrypted communication for the respective data elements.
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.Type-Consistency-MFPlus	MFPlus Data type consistency: The TOE must provide a consistent handling of the different supported data types. This comprises over- and underflow checking for values and for block sizes.
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.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 contacless interface. For example, no data shall remain in a hardware cryptographic coprocessor (e.g. AES 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.

4.2 Security objectives for the environment

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

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

120 Clarification related to “Treatment of User Data of the Composite TOE (*BSI.OE.Resp-Appl*)”: By definition cipher or plain text data and cryptographic keys are User Data. The Security IC Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation. This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

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

BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	Up to phase 6
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader: The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and, ***if desired,*** terminate irreversibly the Loader after intended usage of the Loader. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.	Up to phase 6
BSI.OE.Loader-Usage	Secure communication and usage of the Loader: The authorized user must support the trusted communication channel with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader. The authorized user must organize the maintenance transactions to ensure that the additional code (loaded as data) is able to operate as in the Final composite TOE. The authorized user must manage and associate unique Identification to the loaded data.	Up to phase 7
BSI.OE.TOE-Auth	External entities authenticating of the TOE The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.	Up to phase 7
OE.Composite-TOE-Id	Composite TOE identification: The composite manufacturer must maintain a unique identification of a composite TOE under maintenance.	Up to phase 7
OE.TOE-Id	TOE identification: The IC manufacturer must maintain a unique identification of the TOE under maintenance.	Up to phase 7
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic: If desired, the Composite Product Manufacturer will enable (or disable) irreversibly the Secure Diagnostic capability, thus enabling the IC manufacturer (or disabling everyone) to exercise the Secure Diagnostic capability.	Up to phase 7

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

122 This section details the security objectives for the operational environment, related to MFPlus, and to be enforced after TOE delivery up to phase 7.

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

OE.Secure-Values	Generation of secure values: The environment shall generate confidential and cryptographically strong 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 up to phase 7.	
OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers: 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.Furthermore, the terminal shall provide random numbers according to AIS20 or AIS31 *[1]* for the authentication.	

4.3 Security objectives rationale

124 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* protection profile, together with those in *AUG*, and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 3* are addressed by the security objectives stated in this chapter.

125 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).

126 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*)".

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

- TOE threats "Diffusion of open samples, (*ANSSI.T.Open-Samples-Diffusion*)", "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 availability, (*T.Application-Resource-MFPlus*)".
- organisational security policies "Confidentiality during communication, (*P.Encryption*)", “Integrity during communication, (*P.MAC*)", "Un-traceability of end-users, (*P.No-Trace*)", and "Treatment of user data, (*P.Resp-Appl*)".
- assumptions "Usage of secure values, (*A.Secure-Values*)", and "Terminal support to ensure integrity and confidentiality, (*A.Terminal-Support*)".

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

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

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	
BSI.P.Ctrl-Loader	*BSI.O.Ctrl-Auth-Loader* *ANSSI.O.Secure-Load-ACode* *ANSSI.O.Secure-AC-Activation* *ANSSI.O.TOE-Identification* *O.Secure-Load-AMemImage* *O.MemImage-Identification* *BSI.OE.Loader-Usage* *OE.TOE-Id* *OE.Composite-TOE-Id*	
A.Secure-Values	*OE.Secure-Values*	Phases 5-7
A.Terminal-Support	*OE.Terminal-Support*	Phase 7
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
P.Encryption	*O.Encryption-MFPlus*	
P.MAC	*O.MAC-MFPlus*	
P.No-Trace	*O.No-Trace-MFPlus* *O.Access-Control-MFPlus* *O.Authentication-MFPlus*	
P.Resp-Appl	*O.Resp-Appl-MFPlus*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func* *OE.Enable-Disable-Secure-Diag* *OE.Secure-Diag-Usage*	
BSI.T.RND	*BSI.O.RND*	
BSI.T.Masquerade-TOE	*BSI.O.Authentication* *BSI.OE.TOE-Auth*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
ANSSI.T.Open-Samples-Diffusion	*ANSSI.O.Prot-TSF-Confidentiality* *BSI.O.Leak-Inherent* *BSI.O.Leak-Forced*	

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
T.Data-Modification-MFPlus	*O.Access-Control-MFPlus* *O.Type-Consistency-MFPlus* *OE.Terminal-Support*	
T.Impersonate-MFPlus	*O.Authentication-MFPlus*	
T.Cloning-MFPlus	*O.Access-Control-MFPlus* *O.Authentication-MFPlus*	
T.Confid-Applic-Code-MFPlus	*O.Firewall-MFPlus*	
T.Confid-Applic-Data-MFPlus	*O.Firewall-MFPlus*	
T.Integ-Applic-Code-MFPlus	*O.Verification-MFPlus* *O.Firewall-MFPlus*	
T.Integ-Applic-Data-MFPlus	*O.Shr-Var-MFPlus* *O.Firewall-MFPlus*	
T.Application-Resource-MFPlus	*O.Resource-MFPlus*	

4.3.1 Assumption "Usage of secure values"

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

131 *OE.Secure-Values* is an immediate transformation of this assumption, therefore it covers the assumption.

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

4.3.2 Assumption "Terminal support to ensure integrity, confidentiality and use of random numbers"

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

134 The objective *OE.Terminal-Support* is an immediate transformation of the assumption, therefore it covers the assumption. The TOE can only check the integrity of data received from the terminal. For data transferred to the terminal, the receiver must verify the integrity of the received data. Furthermore the TOE cannot verify the entropy of the random number sent by the terminal. The terminal itself must ensure that random numbers are generated with appropriate entropy for the authentication. This is assumed by the related assumption, therefore the assumption is covered.

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

4.3.3 TOE threat "Abuse of Functionality"

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

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

4.3.4 TOE threat "Memory Access Violation"

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

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

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

4.3.5 TOE threat "Diffusion of open samples"

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

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

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

4.3.6 TOE threat "Unauthorised data modification for MFPlus"

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

145 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 and code elements stored by the TOE. *O.Type-Consistency-MFPlus* ensures that data types are adhered, so that TOE data cannot be modified by abusing type-specific operations. The terminal must provide support by checking the TOE responses, which is required by *OE.Terminal-Support*. Therefore *T.Data-Modification-MFPlus* is covered by these three objectives.

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

4.3.7 TOE threat "Impersonating authorised users during authentication for MFPlus"

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

148 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. *O.Authentication-MFPlus* requires that the authentication mechanism provided by the TOE shall be resistant against attack scenarios targeting the impersonation of authorized users. Therefore the threat is covered by *O.Authentication-MFPlus*.

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

4.3.8 TOE threat "Cloning for MFPlus"

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

151 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.
O.Access-Control-MFPlus requires that unauthorized users can not read any information that is restricted to the authorized subjects. The cryptographic keys used for the authentication are stored inside the TOE and are protected by this objective. This objective states that no keys used for authentication shall ever be output. *O.Authentication-MFPlus* requires that users are authenticated before they can read any information that is restricted to authorized users. Therefore the two objectives cover *T.Cloning-MFPlus*.

4.3.9 TOE threat "MFPlus resource availability"

152 The justification related to the threat “MFPlus resource availability, (*T.Application-Resource-MFPlus*)” is as follows:

153 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*.

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

4.3.10 TOE threat "MFPlus code confidentiality"

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

156 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*.

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

4.3.11 TOE threat "MFPlus data confidentiality"

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

159 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*.

4.3.12 TOE threat "MFPlus code integrity"

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

161 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*.

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

4.3.13 TOE threat "MFPlus data integrity"

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

164 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*.

165 The added objective for the TOE *O.Shr-Var-MFPlus* does not introduce any contradiction in the security objectives for the TOE.

4.3.14 Organisational security policy "Controlled usage to Loader Functionality"

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

167 As stated in *BSI-CC-PP-0084-2014*, the organisational security policy “Controlled usage to Loader Functionality (*BSI.P.Ctrl-Loader*) is implemented by the security objective for the TOE “Access control and authenticity for the Loader (*BSI.O.Ctrl-Auth-Loader*)” and the security objective for the TOE environment “Secure communication and usage of the Loader (*BSI.OE.Loader-Usage*)”.
The security objectives “Secure loading of the Additional Code (*ANSSI.O.Secure-Load-ACode*)”, “Secure activation of the Additional Code (*ANSSI.O.Secure-AC-Activation*)”, and ”Secure identification of the TOE (*ANSSI.O.TOE-Identification*)” specified by *ANSSI-CC-NOTE-06/2.0 EN* additionally enforce this policy since they require authenticity, atomicity, identification of the loaded additional code, part of the TOE. ”Secure identification of the TOE (*ANSSI.O.TOE-Identification*)” is supported by the security objective for the TOE environment “TOE identification (*OE.TOE-Id*)”.
Similarly, the security objectives “Secure loading of the Additional Memory Image

(*O.Secure-Load-AMemImage*)", and "Secure identification of the Memory Image (*O.MemImage-Identification*)", enforce this policy since they require authenticity, atomicity, identification of the loaded additional memory image for the user data (embedded software). "Secure identification of Memory Image (*O.MemImage-Identification*)" is supported by the security objective for the TOE environment "Composite TOE identification (*OE.Composite-TOE-Id*)".
Therefore the policy is covered by these nine objectives.

4.3.15 Organisational security policy "Additional Specific Security Functionality"

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

169 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.

170 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*.

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

4.3.16 Organisational security policy "Confidentiality during communication"

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

173 For MFPlus, *O.Encryption-MFPlus* is an immediate transformation of the security policy, therefore it covers the Security Policy.

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

4.3.17 Organisational security policy "Integrity during communication"

175 The justification related to the organisational security policy "Integrity during communication for MFPlus, (*P.MAC*)" is as follows:

176 For MFPlus, *O.MAC-MFPlus* is an immediate transformation of the security policy, therefore it covers the Security Policy.

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

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

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

179 This 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.

180 For MFPlus, *O.Access-Control-MFPlus* provides means to implement access control to data elements on the TOE and *O.Authentication-MFPlus* provides means to implement authentication on the TOE, in order to prevent tracing based on freely accessible data elements. *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 unauthorized subject, which includes the UID. Therefore the policy is covered by these three objectives.

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

4.3.19 Organisational security policy "Treatment of user data"

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

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

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

5 Security requirements (ASE_REQ)

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

5.1 Security functional requirements for the TOE

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

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

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

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

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

189 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.

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

Table 7. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-CC-PP-0084-2014*	*CCMB-2017-04-002 R5*
FPT_FLS.1	Failure with preservation of secure state			

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

Label	Title	Addressing	Origin	Type
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality	*BSI-CC-PP-0084-2014*	Extended
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-CC-PP-0084-2014* Operated	
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing		*CCMB-2017-04-002 R5*
FDP_SDI.2	Stored data integrity monitoring and action			
FPT_PHP.3	Resistance to physical attack		*BSI-CC-PP-0084-2014*	
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1	Random number generation	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	*CCMB-2017-04-002 R5*
FCS_CKM.1 (if NesLib is embedded only)	Cryptographic key generation		Security Target Operated	
FDP_ACC.1 / Memories	Subset access control	Memory access violation	Security Target Operated	
FDP_ACF.1 / Memories	Security attribute based access control		*AUG* #4 Operated	
FMT_MSA.3 / Memories	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Memories	Management of security attribute			
FMT_SMF.1 / Memories	Specification of management functions		Security Target Operated	
FIA_API.1	Authentication Proof of Identity	Masquerade	*BSI-CC-PP-0084-2014* Operated	Extended

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

Label	Title	Addressing	Origin	Type
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality	*BSI-CC-PP-0084-2014* Operated	Extended
FMT_LIM.2 / Loader	Limited availability			
FTP_ITC.1 / Loader	Inter-TSF trusted channel - Loader	Loader violation		*CCMB-2017-04-002 R5*
FDP_UCT.1 / Loader	Basic data exchange confidentiality - Loader			
FDP_UIT.1 / Loader	Data exchange integrity - Loader			
FDP_ACC.1 / Loader	Subset access control - Loader			
FDP_ACF.1 / Loader	Security attribute based access control - Loader			
FMT_MSA.3 / Loader	Static attribute initialisation - Loader	Correct Loader operation	Security Target Operated	
FMT_MSA.1 / Loader	Management of security attribute - Loader			
FMT_SMR.1 / Loader	Security roles - Loader			
FIA_UID.1 / Loader	Timing of identification - Loader			
FIA_UAU.1 / Loader	Timing of authentication - Loader			
FMT_SMF.1 / Loader	Specification of management functions - Loader			
FPT_FLS.1 / Loader	Failure with preservation of secure state - Loader			
FAU_SAR.1 / Loader	Audit review - Loader	Lack of TOE identification		
FAU_SAS.1 / Loader	Audit storage - Loader			Extended

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

Label	Title	Addressing	Origin	Type
FMT_SMR.1 / MFPlus	Security roles	MFPlus access control (if MFPlus is embedded only)	Security Target Operated	CCMB-2017-04-002 R5
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 attributes			
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			
FTP_TRP.1 / MFPlus	Trusted path			
FCS_CKM.4 / MFPlus	Cryptographic key destruction			
FPT_RPL.1 / MFPlus	Replay detection	MFPlus robustness (if MFPlus is embedded only)		
FPR_UNL.1 / MFPlus	Unlinkability			
FRU_RSA.2 / MFPlus	Minimum and maximum quotas	MFPlus correct operation (if MFPlus is embedded only)		
FDP_RIP.1 / MFPlus	Subset residual information protection	MFPlus intrinsic confidentiality and integrity (if MFPlus is embedded only)		

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

Label	Title	Addressing	Origin	Type
FTP_ITC.1 / Sdiag	Inter-TSF trusted channel - Secure Diagnostic	Abuse of Secure Diagnostic functionality	Security Target Operated	CCMB-2017-04-002 R5
FAU_SAR.1 / Sdiag	Audit review - Secure Diagnostic			
FMT_LIM.1 / Sdiag	Limited capabilities - Secure Diagnostic			Extended
FMT_LIM.2 / Sdiag	Limited availability - Secure Diagnostic			

5.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

191 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)

192 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.***

193 ***Refinements:***

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

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

Regarding application note 15 of BSI-CC-PP-0084-2014, the TOE provides information on the operating conditions monitored during Security IC Embedded Software execution and after a warm reset. No audit requirement is however selected in this Security Target.

Limited capabilities (FMT_LIM.1) / Test

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

Limited availability (FMT_LIM.2) / Test

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

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

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

Audit storage (FAU_SAS.1)

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

Stored data confidentiality (FDP_SDC.1)

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

Stored data integrity monitoring and action (FDP_SDI.2)

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

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

Resistance to physical attack (FPT_PHP.3)

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

202 ***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)

203 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)

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

205 ***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)

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

207 *SFP_2: Data Processing Policy*

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

Random number generation (FCS_RNG.1)

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

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

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

- ***(PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.***
- ***(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.***

5.1.2 Additional Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

210 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]
None	TDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Triple Data Encryption Standard (TDES)	168 bits	*NIST SP 800-67* *NIST SP 800-38A*
None	AES	* encryption (cipher) * decryption (inverse cipher) - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS PUB 197*
Only if NesLib		* Message authentication Code computation (CMAC) * Authenticated encryption/decryption in Galois Counter Mode (GCM) * Authenticated encryption/decryption in Counter with CBC-MAC (CCM)			*NIST SP 800-38B* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38C*
Only if NesLib	RSA	* RSA public key operation * RSA private key operation without the Chinese Remainder Theorem * RSA private key operation with the Chinese Remainder Theorem * EMSA PSS and PKCS1 signature scheme coding * RSA Key Encapsulation Method (KEM)	Rivest, Shamir & Adleman’s	up to 4096 bits	*PKCS #1 V2.1*

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

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Only if NesLib	ECC on Weierstrass curves	* private scalar multiplication * prepare Jacobian * public scalar multiplication * point validity check * convert Jacobian to affine coordinates * general point addition * point expansion * point compression	Elliptic Curves Cryptography on GF(p) on curves in Weierstrass form	up to 640 bits	*IEEE 1363-2000*, *chapter 7* *IEEE 1363a-2004*
		* Diffie-Hellman (ECDH) key agreement computation			*NIST SP 800-56A*
		* digital signature algorithm (ECDSA) generation and verification			*FIPS PUB 186-4* *ANSI X9.62*, *section 7*
Only if NesLib	ECC on Edwards curves	* ed25519 generation * ed25519 verification * ed25519 point decompression	Elliptic Curves Cryptography on GF(p) on curves in Edwards form, with curve 25519	256 bits	*EdDSA rfc* *EDDSA* *EDDSA2*
Only if NesLib	SHA	* SHA-1(1) * SHA-224 * SHA-256 * SHA-384 * SHA-512 * Protected SHA-1(1) * Protected SHA-256 * Protected SHA-384 * Protected SHA-512	Secure Hash Algorithm	assignment pointless because algorithm has no key	*FIPS PUB 180-2*
		* HMAC using any of the above protected hash functions		up to 1024 bits	*FIPS PUB 198-1*

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

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Only if NesLib	Keccak and SHA-3	* SHAKE128, * SHAKE256, * SHA3-224, * SHA3-256, * SHA3-384, * SHA3-512, * Keccak[r,1600-r], * protected SHAKE128, * protected SHAKE256, * protected SHA3-224, * protected SHA3-256, * protected SHA3-384, * protected SHA3-512, * Protected Keccak[r,1600-r]	Keccak	no key for plain functions, variable key length up to security level for protected functions (security level is last number in function names and 1600-c for Keccak)	*FIPS PUB 202*
Only if NesLib	Keccak-p	* Keccak-p[1600,n_r = 24], * Keccak-p[1600, n_r=12], * protected Keccak-p[1600,n_r = 24], * protected Keccak-p[1600, n_r=12]	Keccak-p	no key for plain functions, any key length up to 256 bits for protected functions	*FIPS PUB 202*
Only if NesLib	Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	up to 4096 bits	*ANSI X9.42*
Only if NesLib	DRBG	* SHA-1(1) * SHA-224 * SHA-256 * SHA-384 * SHA-512	Hash-DRBG	None	*NIST SP 800-90* *FIPS PUB 180-2*
		*AES	CTR-DRBG	128, 192 and 256 bits	*NIST SP 800-90* *FIPS PUB 197*

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

Cryptographic key generation (FCS_CKM.1)

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

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

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

5.1.3 Additional Security Functional Requirements for the memories protection

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

Static attribute initialisation (FMT_MSA.3) / Memories

213 The TSF shall enforce the ***Memory Access Control Policy*** to provide ***minimally protective***[(b)] default values for security attributes that are used to enforce the SFP.

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

Management of security attributes (FMT_MSA.1) / Memories

215 The TSF shall enforce the ***Memory Access Control Policy*** to restrict the ability to ***modify*** the security attributes:

- ***Location of the Protected Application code and data*** to ***Nobody,***
- ***Location of the Protected Sectors*** to ***Anybody***.

Subset access control (FDP_ACC.1) / Memories

216 The TSF shall enforce the ***Memory Access Control Policy*** on ***the Protected Application code and data, Protected sectors.***

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

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

217 The TSF shall enforce the ***Memory Access Control Policy*** to objects based on the following: ***Protected Application code and data, Protected sectors***.

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

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

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

- ***in User configuration, any access (read, write, execute) to the OST ROM is denied,***
- ***in User configuration, any write access to the ST NVM is denied.***

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

222 *SFP_3: Memory Access Control Policy*

223 *Another application cannot read, write, compare any piece of data or code belonging to the Protected Application. A Protected sector cannot be programmed or erased.*

Application Note:
One only application can be protected by the LPU. MFPlus is the only Protected Application, when it is embedded.

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

- ***in User configuration, any access (read, write, execute) to the OST ROM is denied,***
- ***in User configuration, any write access to the ST NVM is denied.***

Specification of management functions (FMT_SMF.1) / Memories

225 The TSF will be able to perform the following management functions: ***define the protected sectors.***

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

Authentication Proof of Identity (FIA_API.1)

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

Limited capabilities (FMT_LIM.1) / Loader

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

228 *SFP_4: Loader Limited capability Policy*

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

Limited availability (FMT_LIM.2) / Loader

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

231 *SFP_5: Loader Limited availability Policy*

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

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

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

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

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

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

237 ***Refinement:***

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

Basic data exchange confidentiality (FDP_UCT.1) / Loader

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

Data exchange integrity (FDP_UIT.1) / Loader

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

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

Subset access control (FDP_ACC.1) / Loader

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

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

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

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

243 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***if the user authenticated role is allowed to***

perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.

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

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

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

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

247 SFP_6: Loader SFP

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

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

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

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

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

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

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

Static attribute initialisation (FMT_MSA.3) / Loader

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

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

Management of security attributes (FMT_MSA.1) / Loader

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

Specification of management functions (FMT_SMF.1) / Loader

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

Security roles (FMT_SMR.1) / Loader

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

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

Timing of identification (FIA_UID.1) / Loader

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

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

Timing of authentication (FIA_UAU.1) / Loader

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

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

Audit storage (FAU_SAS.1) / Loader

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

261 ***Refinement:***

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

Audit review (FAU_SAR.1) / Loader

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

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

5.1.5 Additional Security Functional Requirements related to the Secure Diagnostic capabilities

Limited capabilities (FMT_LIM.1) / Sdiag

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

265 *SFP_7: Sdiag Limited Capability Policy*

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

Limited availability (FMT_LIM.2) / Sdiag

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

268 *SFP_8: Sdiag Limited Availability Policy*

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

270 ***Refinement:***

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

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

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

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

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

274 ***Refinement:***

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

Audit review (FAU_SAR.1) / Sdiag

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

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

5.1.6 Additional Security Functional Requirements related to MFPlus

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

278 They are only valid in case MFPlus is embedded.

279 **Note**: MIFARE Plus 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 and check the code integrity in NVM,
- FCS_RNG.1 for the provision of random numbers,
- FCS_COP.1 / AES for AES cryptographic operations.

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

Security roles (FMT_SMR.1) / MFPlus

281 The TSF shall maintain the roles ***Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser, TransMACConfManager, Anybody and Nobody***.

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

Subset access control (FDP_ACC.1) / MFPlus

283 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

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

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

- ***In SL0 the Personaliser is allowed to perform Block.Write on all Blocks except Block 0.***
- ***In SL3 the CardUser is allowed to perform Block.Read and Block.Write for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.***
- ***In SL3 the CardUser is allowed to perform Value.Increase, Value.Decrease, Value.Transfer and Value.Restore for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.***

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

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

- ***No one but Nobody is allowed to perform Block.Write on Block 0 (first Block of the first Sector).***
- ***The OriginalityKeyUser is not allowed to perform any operation on objects.***

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

289 *SFP_9: MFPlus Access Control Policy*

The Security Function Policy (SFP) MFPlus Access Control Policy uses the subsequent definitions including the subjects defined as follows:

- *Personaliser: Personaliser*
  The Personaliser is the subject that owns or has access to all cryptographic keys in order to provide them to the TOE. Note that all actions performed by the Personaliser are restricted to SL0 and that those actions do not require an active authentication.
- *CardAdmin: Card Administrator*
  The CardAdmin is the subject that owns or has access to the CardMasterKey.
- *CardManager: Card Manager*
  The CardManager is the subject that owns or has access to the CardConfigurationKey.
- *SecurityLevelManager: Card Security Level Manager*
  The SecurityLevelManager is the subject that owns or has access to the Level3SwitchKey.
- *SectorSecurityLevelManager: Sector Security Level Manager*
  The SectorSecurityLevelManager is the subject that owns or has access to the Level3SectorSwitchKey or Level1Level3MixSectorSwitchKey, and one or more AESSectorKeys.
- *CardUser: Card User*
  The CardUser is the subject that owns or has access to one or more AESSectorKeys. Note that the CardUser does not necessarily need to know both AESSectorKeys.KeyA and AESSectorKeys.KeyB of a particular Sector.
- *OriginalityKeyUser: Originality Key User*
  The OriginalityKeyUser is the subject that owns or has access to one or more OriginalityKeys.
- *TransMACConfManager: Transaction MAC Configuration Manager*
  The TransMACConfManager is the subject that owns or has access to one or moreTransMACConfKeys.
- *Anybody: Anybody*
  Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser or TransMACConfManager, belongs to the role Anybody. This role includes the card holder (also referred to as end-user), and any other subject like an attacker for instance. The subjects belonging to Anybody do not possess any key and therefore are not able to perform any operation that is restricted to one of the roles which are explicitly excluded from the role Anybody.
- *Nobody: Nobody*
  Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser, TransMACConfManager or Anybody, belongs to the role Nobody. Due to the definition of Anybody, the set of all subjects belonging to the role Nobody is the empty set.

Note that multiple subjects may have the same role, e.g. for every Sector there are two CardUsers (identified by the respective AESSectorKeys.KeyA and AESSectorKeys.KeyB for this Sector). The assigned rights to the CardUsers can be different, which allows having more or less powerful CardUsers. There are also more than one OriginalityKeyUser and SecurityLevelManager.

The objects are defined as follows:

- *Block: Block*
  Data is organized in Blocks of 16 bytes, which are accessed as elementary data units. Several instances of a Block are grouped into Sectors.
- *Sector: Sector*
  Each Sector consists of 4 or 16 Blocks.
- *Value: Value*
  One specific type of data stored in a Block is called Value.
- *CardMasterKey: Card Master Key*
  The key to manage keys and parameters for items of the TOE that do not require being changed in the field.
- *CardConfigurationKey :Card Configuration Key*
  The key to manage keys and parameters for items of the TOE that may require being changed in the field.
- *Level3SwitchKey: Level 3 Switch Key*
  Key to change SecurityLevel from SL1 to SL3.
- *Level3SectorSwitchKey: Level 3 Sector Switch Key*
  Key to switch dedicated Sectors from SectorSecurityLevel1to SectorSecurityLevel3.
- *Level1Level3MixSectorSwitchKey: Level 1 Level 3 Mix Sector Switch Key*
  Key to switch dedicated sectors from SectorSecurityLevel1 to SectorSecurityLevel1Level3Mix.
- *TransMACKey: Transaction MAC Key*
  Key to derive session keys that are used in the actual Transaction MAC computation. Note that there exists four of these keys in total.
- *TransMACConfKey:Transaction MAC Configuration Key*
  Each TransMACKey is assigned a TransMACConfKey. An active authentication with the TransMACConfKey is required to enable the Transaction MAC feature for one or more dedicated Blocks.
- *TransMACConfBlock: Transaction MAC Configuration Block*
  Each TransMACKey is related with several TransMACConfBlocks.
- *AESSectorKeys: AES Sector Keys*
  The keys to manage access to Sectors. Since there are two keys for every Sector the keys are called AESSectorKeys.KeyA and AESSectorKeys.KeyB.
- *OriginalityKey: Originality Key*
  The key to check the originality of the TOE.

The security attributes are:

- *SectorTrailer: Sector Trailer*
  The security attribute SectorTrailer is a specific Block that contains the access conditions for the corresponding Sector.
- *MFPConfigurationBlock: MFP Configuration Block.*
- *FieldConfigurationBlock: Field Configuration Block.*
- *SectorSecurityLevel: Sector Security Level*
  The sector security level of a designated Sector of the TOE.
- *SecurityLevel: Card Security Level*
  The Security Level of the TOE.

The operations that can be performed with the objects are:

- *Block.Read: Read data from a Block,*
- *Block.Write: Write data to a Block,*
- *Value.Increase: Increase a Value,*
- *Value.Decrease: Decrease a Value,*
- *Value.Transfer: Transfer a Value,*
- *Value.Restore: Restore a Value,*
- *CardMasterKey.Change: Change the CardMasterKey,*
- *CardConfigurationKey.Change: Change the CardConfigurationKey.,*
- *Level3SwitchKey.Change: Change the Level3SwitchKey,*
- *Level3SectorSwitchKey.Change: Change the Level3SectorSwitchKey,*
- *Level1Level3MixSectorSwitchKey.Change: Change the Level1Level3MixSectorSwitchKey,*
- *TransMACKey.Change: Change the TransMACKey,*
- *TransMACConfKey.Change: Change the TransMACConfKey,*
- *TransMACConfBlock.Write: Write data to TransMACConfBlock,*
- *AESSectorKeys.Change: Change the AESSectorKeys,*
- *OriginalityKey.Change: Change the OriginalityKey,*
- *SectorTrailer.Read: Read the security attribute SectorTrailer,*
- *SectorTrailer.Modify: Modify the security attribute SectorTrailer,*
- *MFPConfigurationBlock.Modify: Modify the security attribute MFPConfigurationBlock,*
- *FieldConfigurationBlock.Modify: Modify the security attribute FieldConfigurationBlock,*
- *SectorSecurityLevel.Switch: Switch the SectorSecurityLevel,*
- *SecurityLevel.Switch: Switch the SecurityLevel.*

Note that subjects are authorised by cryptographic keys by applying an authentication procedure. These keys are considered as authentication data and not as security attributes of the subjects.

Implications of the MFPlus Access Control Policy:

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 usually does not belong to the group of authorised users (consisting of CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser and OriginalityKeyUser), 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 SL0. The Personaliser is allowed to perform Block.Write on all Blocks and therefore change all data, all the keys (except the OriginalityKeys), and all SectorTrailers, MFPConfigurationBlocks and FieldConfigurationBlocks.*
- *Switching of the SecurityLevel is an integral part of the TOE security. The TOE is switched from SL0 to SL1 or SL3 at the end of the personalisation phase. Afterwards the SecurityLevel of the TOE can be increased by the SecurityLevelManager, the*

SectorSecurityLevels of dedicated Sectors of the TOE can be increased by the SectorSecurityLevelManager.

Static attribute initialisation (FMT_MSA.3) / MFPlus

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

291 The TSF shall allow ***no one but Nobody*** 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

292 The TSF shall enforce the ***MFPlus Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***MFPConfigurationBlock, FieldConfigurationBlock, SecurityTrailer*** and ***SecurityLevel*** to ***the Personaliser, CardManager, CardAdmin, SecurityLevelManager, and CardUser***.

293 ***Refinement:***

The detailed management abilities are:

- ***In SL0 the Personaliser is allowed to perform MFPConfigurationBlock.Modify.***
- ***In SL0 the Personaliser is allowed to perform FieldConfigurationBlock.Modify.***
- ***In SL0 the Personaliser is allowed to perform SectorTrailer.Modify.***
- ***In SL0 the Personaliser is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL1 or SL3.***
- ***The CardAdmin is allowed to perform MFPConfigurationBlock.Modify.***
- ***In SL1 the SecurityLevelManager is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL3.***
- ***The CardUser is allowed to perform SectorTrailer.Read and SectorTrailer.Modify if the access conditions in the corresponding SectorTrailer grant him these rights.***

Specification of Management Functions (FMT_SMF.1) / MFPlus

294 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 SecurityLevel of the TOE or the SectorSecurityLevel of dedicated Sectors, DESELECT according to ISO 14443-3, explicit authentication request;***
- ***Finishing the personalisation phase by explicit request of the Personaliser,***
- ***Changing a security attribute.***
- ***Selection and Deselection of the virtual card.***

Import of user data with security attributes (FDP_ITC.2) / MFPlus

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

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

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

298 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.

299 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

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

301 The TSF shall use ***the rules: data Blocks can always be modified by the Block.Write operation. If a data Block is in the data Value format it can be modified by all dedicated Value-specific operations honouring the Value-specific boundaries. SectorTrailers 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. Instead, the TOE distinguishes different types of Blocks and ensures that type-specific boundaries cannot be violated, e.g. Values do not overflow. For SectorTrailers the TOE enforces a specific format.

Cryptographic key destruction (FCS_CKM.4) / MFPlus

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

User identification before any action (FIA_UID.2) / MFPlus

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

User authentication before any action (FIA_UAU.2) / MFPlus

304 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

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

306 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 SL0. The 'none' authentication implicitly and solely authorises the Personaliser.***
- ***The cryptographic authentication is used in SL0 to authenticate the OriginalityKeyUser.***
- ***The cryptographic authentication is used in SL1 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager, the SecurityLevelManager, the SectorSecurityLevelManager, and the CardUser.***
- ***The cryptographic authentication is used in SL3 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager and the CardUser.***

Management of TSF data (FMT_MTD.1) / MFPlus

307 The TSF shall restrict the ability to ***modify*** the ***authentication data*** to ***the Personaliser, CardAdmin, CardManager, SecurityLevelManager and Card User***.

308 ***Refinement:***

The detailed management abilities are:

- ***No one but Nobody is allowed to perform OriginalityKey.Change.***
- ***The Personaliser is allowed to perform CardMasterKey.Change.***
- ***The Personaliser is allowed to perform CardConfigurationKey.Change.***
- ***The Personaliser is allowed to perform Level3SwitchKey.Change.***
- ***The Personaliser is allowed to perform AESSectorKeys.Change.***
- ***The CardAdmin is allowed to perform CardMasterKey.Change.***
- ***The CardAdmin is allowed to perform Level3SwitchKey.Change.***
- ***The CardAdmin is allowed to perform Level3SectorSwitchKey.Change.***
- ***The CardAdmin is allowed to perform Level1Level3MixSectorSwitchKey.Change.***
- ***The CardAdmin is allowed to perform TransMACConfKey.Change.***
- ***The CardManager is allowed to perform CardConfigurationKey.Change.***
- ***The CardUser is allowed to perform AESSectorKeys.Change if the access conditions in the corresponding SectorTrailer grant him this right.***
- ***The TransMACConfManager is allowed to perform TransMACKey.Change.***

Trusted path (FTP_TRP.1) / MFPlus

309 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 and disclosure or only modification***.

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

311 The TSF shall require the use of the trusted path for ***authentication requests, confidentiality and/or data integrity verification for data transfers based on the settings in the MFPConfigurationBlock and the SectorTrailers***.

Replay detection (FPT_RPL.1) / MFPlus

312 The TSF shall detect replay for the following entities: ***authentication requests, confidentiality and/or integrity verification for data transfers based on the settings in the MFPConfigurationBlock and the SectorTrailers***.

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

Unlinkability (FPR_UNL.1) / MFPlus

314 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

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

316 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

317 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***.

5.2 TOE security assurance requirements

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

- ***ASE-TSS.2,*** ALC_DVS.2 and AVA_VAN.5.

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

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

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

Table 10. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*

Table 10. TOE security assurance requirements (continued)

Label	Title	Origin
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/*BSI-CC-PP-0084-2014*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	*BSI-CC-PP-0084-2014*
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	EAL5/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_INT.1	ST introduction	EAL5/*BSI-CC-PP-0084-2014*
ASE_OBJ.2	Security objectives	EAL5/*BSI-CC-PP-0084-2014*
ASE_REQ.2	Derived security requirements	EAL5/*BSI-CC-PP-0084-2014*
ASE_SPD.1	Security problem definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_TSS.2	TOE summary specification with architectural design summary	Security Target
ATE_COV.2	Analysis of coverage	EAL5/*BSI-CC-PP-0084-2014*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-CC-PP-0084-2014*
ATE_IND.2	Independent testing - sample	EAL5/*BSI-CC-PP-0084-2014*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-CC-PP-0084-2014*

5.3 Refinement of the security assurance requirements

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

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

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

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

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

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

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

5.3.1 Refinement regarding functional specification (ADV_FSP)

327 ~~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.***

328 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.

329 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.

330 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.

331 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.

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

5.3.2 Refinement regarding test coverage (ATE_COV)

333 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~~ ***NVM*** writing).

334 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).

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

5.4 Security Requirements rationale

5.4.1 Rationale for the Security Functional Requirements

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

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Inherent	*Basic internal transfer protection FDP_ITT.1* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.Phys-Probing	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Malfunction	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.Phys-Manipulation	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* *Limited capabilities - Secure Diagnostic FMT_LIM.1 / Sdiag* *Limited availability - Secure Diagnostic FMT_LIM.2 / Sdiag* *Inter-TSF trusted channel - Secure Diagnostic FTP_ITC.1 / Sdiag* *Audit review - Secure Diagnostic FAU_SAR.1 / Sdiag* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FDP_SDI.2*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.O.Identification	*Audit storage FAU_SAS.1*
BSI.O.RND	*Random number generation FCS_RNG.1* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDI.2*, *FDP_SDC.1*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.OE.Resp-Appl	Not applicable
BSI.OE.Process-Sec-IC	Not applicable
BSI.OE.Lim-Block-Loader	Not applicable
BSI.OE.Loader-Usage	Not applicable
BSI.OE.TOE-Auth	Not applicable
OE.Enable-Disable-Secure-Diag	Not applicable
OE.Secure-Diag-Usage	Not applicable
BSI.O.Authentication	*Authentication Proof of Identity FIA_API.1*
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Ctrl-Auth-Loader	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*
ANSSI.O.Prot-TSF-Confidentiality	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*
ANSSI.O.Secure-Load-ACode	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader* "*Audit storage - Loader*" *FAU_SAS.1 / Loader*
ANSSI.O.Secure-AC-Activation	"*Failure with preservation of secure state - Loader*" *FPT_FLS.1 / Loader*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
ANSSI.O.TOE-Identification	"*Audit storage - Loader*" *FAU_SAS.1 / Loader* "*Audit review - Loader*" *FAU_SAR.1 / Loader* "*Stored data integrity monitoring and action*" *FDP_SDI.2*
O.Secure-Load-AMemImage	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader* "*Audit storage - Loader*" *FAU_SAS.1 / Loader*
O.MemImage-Identification	"*Failure with preservation of secure state - Loader*" *FPT_FLS.1 / Loader* "*Audit storage - Loader*" *FAU_SAS.1 / Loader* "*Audit review - Loader*" *FAU_SAR.1 / Loader* "*Stored data integrity monitoring and action*" *FDP_SDI.2*
OE.Composite-TOE-Id	Not applicable
OE.TOE-Id	Not applicable
AUG1.O.Add-Functions	*Cryptographic operation FCS_COP.1* *Cryptographic key generation FCS_CKM.1*
AUG4.O.Mem-Access	*Subset access control FDP_ACC.1 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories* *Management of security attribute FMT_MSA.1 / Memories* *Specification of management functions FMT_SMF.1 / Memories*
O.Access-Control-MFPlus	*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 management functions FMT_SMF.1 / MFPlus* *Import of user data with security attributes FDP_ITC.2 / MFPlus* *Cryptographic key destruction FCS_CKM.4 / MFPlus* *Management of TSF data FMT_MTD.1 / MFPlus*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
O.Authentication-MFPlus	*Cryptographic operation FCS_COP.1* / AES *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* *Specification of management functions FMT_SMF.1 / MFPlus* *Trusted path FTP_TRP.1 / MFPlus* *Replay detection FPT_RPL.1 / MFPlus*
O.Encryption-MFPlus	*Cryptographic operation FCS_COP.1* / AES *Cryptographic key destruction FCS_CKM.4 / MFPlus* *Trusted path FTP_TRP.1 / MFPlus*
O.MAC-MFPlus	*Cryptographic operation FCS_COP.1* / AES *Cryptographic key destruction FCS_CKM.4 / MFPlus* *Trusted path FTP_TRP.1 / MFPlus* *Replay detection FPT_RPL.1 / MFPlus*
O.Type-Consistency-MFPlus	*Inter-TSF basic TSF data consistency FPT_TDC.1 / MFPlus*
O.No-Trace-MFPlus	*Unlinkability FPR_UNL.1 / MFPlus*
O.Resp-Appl-MFPlus	All SFRs defined additionnaly in the ST for MFPlus (... / MFPlus)
O.Resource-MFPlus	*Minimum and maximum quotas FRU_RSA.2 / MFPlus*
O.Verification-MFPlus	*Failure with preservation of secure state FPT_FLS.1* *Subset access control FDP_ACC.1 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories*
O.Firewall-MFPlus	*Subset access control FDP_ACC.1 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories*
O.Shr-Var-MFPlus	*Subset residual information protection FDP_RIP.1 / MFPlus*
OE.Secure-Values	Not applicable
OE.Terminal-Support	Not applicable

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

338 From *Table 5*, it is straightforward to identify additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem-Access*) tracing back to *AUG*, additional objectives (*ANSSI.O.Prot-TSF-Confidentiality*, *ANSSI.O.Secure-Load-ACode*, *ANSSI.O.Secure-AC-Activation* and *ANSSI.O.TOE-Identification*) tracing back to *ANSSI-CC-NOTE-06/2.0 EN* / *ANSSI-CC-CER/F/06.002*, and additional objectives (*O.Secure-Load-AMemImage*, *O.MemImage-Identification*, *O.Access-Control-MFPlus*, *O.Authentication-MFPlus*, *O.Encryption-MFPlus*, *O.MAC-MFPlus*, *O.Type-Consistency-*

MFPlus, *O.No-Trace-MFPlus*, *O.Resp-Appl-MFPlus*, *O.Resource-MFPlus*, *O.Verification-MFPlus*, *O.Firewall-MFPlus*, and *O.Shr-Var-MFPlus*) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

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

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

340 Though it remains to show that:

- security objectives from this Security Target, from *ANSSI-CC-NOTE-06/2.0 EN* / *ANSSI-CC-CER/F/06.002* and from *AUG* are addressed by security requirements stated in this chapter,
- additional security requirements from this Security Target and from *AUG* are mutually supportive with the security requirements from the *BSI-CC-PP-0084-2014* protection profile, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

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

5.4.2 Additional security objectives are suitably addressed

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

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

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

344 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*)"

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

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

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

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

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

Security objective "Access control and authenticity for the Loader (*BSI.O.Ctrl-Auth-Loader*)"

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

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

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

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

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

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

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

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

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

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

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

Security objective “Secure identification of the TOE (*ANSSI.O.TOE-Identification*)”

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

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

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

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

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

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

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

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

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

365 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*".
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 nine SFRs together provide an access control mechanism as required by the objective *O.Access-Control-MFPlus*.

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

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

367 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.
"*Specification of Management Functions (FMT_SMF.1) / MFPlus*" defines security management functions the TSF shall be capable to perform.
"*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 seven security functional requirements fulfill the objective *O.Authentication-MFPlus*.

Security objective “Confidential Communication (*O.Encryption-MFPlus*)”

368 The justification related to the security objective “Confidential Communication (*O.Encryption-MFPlus*)” is as follows:

369 The security functional requirement "*Cryptographic operation (FCS_COP.1)*/ AES" requires that the TOE provides the basic cryptographic algorithms that can be used to protect the communication by encryption.
"*Trusted path (FTP_TRP.1) / MFPlus*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 especially requires a trusted path for “authentication request, confidentiality and/or data integrity verification for data transfers on request based

on a setting in the MFP Configuration Block".
"*Cryptographic key destruction (FCS_CKM.4) / MFPlus*" requires that cryptographic keys used for encryption have to be removed after usage.
These three security functional requirements fulfill the objective *O.Encryption-MFPlus*.

Security objective "MFPlus Integrity-protected Communication (*O.MAC-MFPlus*)"

370 The justification related to the security objective "MFPlus Integrity-protected Communication (*O.MAC-MFPlus*)" is as follows:

371 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 "confidentiality and/or data integrity verification for data transfers on request of the file owner".
"*Cryptographic key destruction (FCS_CKM.4) / MFPlus*" requires that cryptographic keys used for MAC operations have to be removed after usage.
Together with "*Replay detection (FPT_RPL.1) / MFPlus*" which requires a replay detection for these data transfers, the four security functional requirements fulfill the objective *O.MAC-MFPlus*.

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

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

373 The security functional requirement "*Inter-TSF basic TSF data consistency (FPT_TDC.1) / MFPlus*" requires the TOE to consistently interpret data blocks. 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-MFPlus*.

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

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

375 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 was caused by the same user.
This meets the objective *O.No-Trace-MFPlus*.

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

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

377 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*)”

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

379 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*)”

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

381 The security functional requirements "*Subset access control (FDP_ACC.1) / Memories*" and "*Security attribute based access control (FDP_ACF.1) / Memories*", supported by "*Static attribute initialisation (FMT_MSA.3) / Memories*", 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 NVM, MFPlus execution is stopped. This meets the objective *O.Verification-MFPlus*.

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

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

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

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

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

385 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*.

5.4.3 Additional security requirements are consistent

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

386 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.1 / Memories*),
Security attribute based access control (*FDP_ACF.1 / Memories*)"

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

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

388 These security requirements have already been argued in *Section : Security objective "Protection against Abuse of Functionality (BSI.O.Abuse-Func)"* and *Section : Security objectives "Protection of the confidentiality of the TSF (ANSSI.O.Prot-TSF-Confidentiality)", "Secure loading of the Additional Code (ANSSI.O.Secure-Load-ACode)" and "Secure loading of the Additional Memory Image (O.Secure-Load-AMemImage)"* above.

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

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

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

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

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

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

"Security roles (*FMT_SMR.1 / 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*)
Cryptographic key destruction (*FCS_CKM.4 / MFPlus*)"

392 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*)"

393 These security requirements have already been argued in *Section : Security objective "Authentication for MFPlus (O.Authentication-MFPlus)"* and *Section : Security objective "Confidential Communication (O.Encryption-MFPlus)"* above.

"Trusted path (*FTP_TRP.1 / MFPlus*),
Replay detection (*FPT_RPL.1 / MFPlus*)"

394 These security requirements have already been argued in *Section : Security objective "MFPlus Integrity-protected Communication (O.MAC-MFPlus)"* above.

Inter-TSF basic TSF data consistency (*FPT_TDC.1 / MFPlus*)

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

"Unlinkability (*FPR_UNL.1 / MFPlus*)"

396 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*)"

397 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*)"

398 This security requirement has already been argued in *Section : Security objective "MFPlus data cleaning for resource sharing (O.Shr-Var-MFPlus)"* above.

5.4.4 Dependencies of Security Functional Requirements

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

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

400 Details are provided in *Table 13* below.

Table 13. Dependencies of security functional requirements

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

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FDP_ITC.1 and FCS_CKM.1, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.4	No, see discussion below	
FCS_CKM.1	[FDP_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.1	
	FCS_CKM.4	No, see discussion below	
FDP_ACC.1 / Memories	FDP_ACF.1 / Memories	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes, by FDP_ACC.1 / Memories	Yes, *AUG* ***#4***
	FMT_MSA.3 / Memories	Yes	
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	
FMT_MSA.1 / Memories	[FDP_ACC.1 / Memories or FDP_IFC.1]	Yes, by FDP_ACC.1 / Memories and FDP_IFC.1	Yes, *AUG* ***#4***
	FMT_SMF.1 / Memories	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	Yes, *AUG* ***#4***
FMT_SMF.1 / Memories	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_API.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FTP_ITC.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_UCT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FDP_UIT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002 R5*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FIA_UID.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_SMF.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FPT_FLS.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FAU_SAS.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FAU_SAR.1 / Loader	FAU_GEN.1	No, by FAU_SAS.1 / Loader instead, see discussion below	***No,*** *CCMB-2017-04-002 R5*
FTP_ITC.1 / Sdiag	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FAU_SAR.1 / Sdiag	FAU_GEN.1	No, see discussion below	***No,*** *CCMB-2017-04-002 R5*

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FMT_SMR.1 / MFPlus	FIA_UID.1 / MFPlus	Yes, by FIA_UID.2 / MFPlus	***No,*** *CCMB-2017-04-002 R5*
FDP_ACC.1 / MFPlus	FDP_ACF.1 / MFPlus	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / MFPlus	FDP_ACC.1 / MFPlus	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / MFPlus	Yes	
FMT_MSA.3 / MFPlus	FMT_MSA.1 / MFPlus	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / MFPlus	Yes	
FMT_MSA.1 / MFPlus	[FDP_ACC.1 / MFPlus or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFPlus	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMF.1 / MFPlus	Yes	
	FMT_SMR.1 / MFPlus	Yes	
FMT_SMF.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FDP_ITC.2 / MFPlus	[FDP_ACC.1 / MFPlus or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFPlus	***No,*** *CCMB-2017-04-002 R5*
	[FTP_ITC.1 or FTP_TRP.1 / MFPlus]	Yes, by FTP_TRP.1 / MFPlus	
	FPT_TDC.1 / MFPlus	Yes	
FPT_TDC.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UID.2 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.2 / MFPlus	FIA_UID.1	Yes, by FIA_UID.2 / MFPlus	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.5 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FMT_MTD.1 / MFPlus	FMT_SMR.1 / MFPlus	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMF.1 / MFPlus	Yes	
FTP_TRP.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FCS_CKM.4 / MFPlus	[FDP_ITC.1 or FDP_ITC.2 / MFPlus or FCS_CKM.1]	Yes, by FDP_ITC.2 / MFPlus	***No,*** *CCMB-2017-04-002 R5*
FPT_RPL.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FPR_UNL.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FRU_RSA.2 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FDP_RIP.1 / MFPlus	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

401 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.

402 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.

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

404 Part 2 of the Common Criteria defines the dependency of "*Audit review (FAU_SAR.1) / Sdiag*" on "Audit data generation (FAU_GEN.1)". In this particular TOE, there is no specific function for audit data generation, the data to be audited are just stored. Therefore, FAU_GEN.1 is not defined in this ST.

5.4.5 Rationale for the Assurance Requirements

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

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

406 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.

407 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. All dependencies introduced by the requirements chosen for augmentation are fulfilled. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

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

Dependencies of assurance requirements

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

410 The augmentation to this package identified in paragraph *318* does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ASE_TSS.2 dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this ST,
- ALC_DVS.2 and AVA_VAN.5 dependencies have been justified in *BSI-CC-PP-0084-2014*.

6 TOE summary specification (ASE_TSS)

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

6.1 Limited fault tolerance (FRU_FLT.2)

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

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

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

- Die integrity violation detection,
- Errors on memories,
- Glitches,
- High voltage supply,
- CPU errors,
- Sequence control,
- etc..

414 The ES can generate a software reset.

6.3 Limited capabilities (FMT_LIM.1) / Test, Limited capabilities (FMT_LIM.1) / Sdiag, Limited capabilities (FMT_LIM.1) / Loader, Limited availability (FMT_LIM.2) / Test, Limited availability (FMT_LIM.2) / Sdiag & Limited availability (FMT_LIM.2) / Loader

415 The TOE is either in Test, Admin or User configuration.

416 The TOE may also be in Basic Diagnostic (aka Diagnostic), Secure Diagnostic or Genuine Check volatile configuration.

417 The Test and Diagnostics configurations are reserved to ST.

418 The possible transitions are: Test to Admin, Admin to User, Admin to Genuine Check, Admin to Test, Admin to Basic Diagnostic, User to Admin, User to Genuine Check, User to Basic Diagnostic, Basic Diagnostic to Secure Diagnostic, Secure Diagnostic to Test.

419 The TSF ensures the switching and the control of TOE configuration, the corresponding access control and the control of the corresponding capabilities.The transition controls rely on several strong mechanisms including fuse, authentication and control registers. Part of the transitions are only possible in the STMicroelectronics audited environment.

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

421 The customer can choose to disable irreversibly the Loading capability.

422 The customer can choose to irreversibly enable or disable the Secure Diagnostic capability. Only if the customer enables it, for quality investigation purpose, ST can exercise the Secure Diagnostic capability with a secure protocol, in an audited environment.

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

423 In Secure Diagnostic volatile configuration, the System Firmware provides a secure channel to allow another IT product to operate a Secure Diagnostic transaction.

6.5 Audit review (FAU_SAR.1) / Sdiag

424 The System Firmware allows to read the Secure Diagnostic status (permanently disabled, permanently enabled, disabled but still configurable).

6.6 Stored data confidentiality (FDP_SDC.1)

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

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

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

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

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

6.8 Audit storage (FAU_SAS.1)

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

6.9 Resistance to physical attack (FPT_PHP.3)

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

- The TOE implements a set of countermeasures that reduce the exploitability of physical probing.
- The TOE is physically protected by active shields that command an automatic reaction on die integrity violation detection.

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

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

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment,
- Leakage protection in libraries.

6.11 Random number generation (FCS_RNG.1)

430 The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the *BSI-AIS20/AIS31* standard for a PTG.2 class device.

6.12 Cryptographic operation: TDES operation (FCS_COP.1) / TDES

431 The TOE provides an EDES+ accelerator that has the capability to perform 3-key Triple DES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode conformant to *NIST SP 800-67* and *NIST SP 800-38A*.

If NesLib is embedded, the cryptographic library NesLib instantiates the same standard DES cryptographic operations.

6.13 Cryptographic operation: AES operation (FCS_COP.1) / AES

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

- cipher,
- inverse cipher,

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

434 If NesLib is embedded, the cryptographic library NesLib instantiates the same standard AES cryptographic operations, and additionally provides:

- message authentication Code computation (CMAC),
- authenticated encryption/decryption in Galois Counter Mode (GCM),
- authenticated encryption/decryption in Counter with CBC-MAC (CCM).

435 The MFPlus library uses AES as cryptographic operation (AES accelerator). Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

6.14 Cryptographic operation: RSA operation (FCS_COP.1) / RSA only if NesLib

436 The cryptographic library NesLib provides to the ES developer the following RSA functions, all conformant to *PKCS #1 V2.1*:

- RSA public key cryptographic operation for modulus sizes up to 4096 bits,
- RSA private key cryptographic operation with or without CRT for modulus sizes up to 2048 bits,
- RSA signature formatting,
- RSA Key Encapsulation Method.

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

437 The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Weierstrass form, all conformant to *IEEE 1363-2000* and *IEEE 1363a-2004*, including:

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

438 Additionally, the cryptographic library NesLib provides functions dedicated to the two most used elliptic curves cryptosystems:

- Elliptic Curve Diffie-Hellman (ECDH), as specified in *NIST SP 800-56A*,
- Elliptic Curve Digital Signature Algorithm (ECDSA) generation and verification, as stipulated in *FIPS PUB 186-4* and specified in *ANSI X9.62*, section 7.

439 The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Edwards form, with curve 25519, all conformant to *EdDSA rfc*, including:

- generation,
- verification,
- point decompression.

6.16 Cryptographic operation: SHA-1 & SHA-2 operation (FCS_COP.1) / SHA, only if NesLib

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

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

442 Additionally, the cryptographic library NesLib offers support for the HMAC mode of use, as specified in *FIPS PUB 198-1*, to be used in conjunction with the protected versions of SHA-1, SHA-256, SHA-384, and SHA-512.

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

443 The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

444 The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

445 The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

446 The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

6.18 Cryptographic operation: Keccak-p operation (FCS_COP.1) / Keccak-p, only if NesLib

447 The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202*:

- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].
- The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:
- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].

6.19 Cryptographic operation: Diffie-Hellman operation (FCS_COP.1) / Diffie-Hellman, only if NesLib

448 The cryptographic library NesLib provides the Diffie-Hellman key establishment operation over GF(p) for size of modulus p up to 4096 bits, conformant to *ANSI X9.42*.

6.20 Cryptographic operation: DRBG operation (FCS_COP.1) / DRBG, only if NesLib

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

450 The cryptographic library NesLib implements two of the DRBG specified in *NIST SP 800-90*:

- Hash-DRBG,
- CTR-DRBG.

6.21 Cryptographic key generation: Prime generation (FCS_CKM.1) / Prime-generation, only if NesLib

451 The cryptographic library NesLib provides prime numbers generation for prime sizes up to 2048 bits conformant to *FIPS PUB 140-2* and *FIPS PUB 186-4*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

6.22 Cryptographic key generation: RSA key generation (FCS_CKM.1) / RSA-key-generation, only if NesLib

452 The cryptographic library NesLib provides standard RSA public and private key computation for key sizes upto 4096 bits conformant to *FIPS PUB 140-2, ISO/IEC 9796-2* and *PKCS #1 V2.1*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

6.23 Static attribute initialisation (FMT_MSA.3) / Memories

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

454 If MFPlus is part of the TOE, at product start all the LPU static attributes are initialised, allowing to protect the segments where MFPlus code and data are stored.

455 If MFPlus is not part of the TOE, the customer can use the LPU to protect segments where part of its code and data are stored.

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

456 The TOE provides memory protections: NVM sector protection, limitation in unprivileged mode, optionally the LPU.

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

457 The TOE enforces the memory management policy for data access and code access thanks to a Library Protection Unit (LPU), and for sector protection, programmed by the ES.

458 In case MFPlus is part of the TOE, the Library Protection Unit is reserved to ST usage to isolate the MFPlus firmware (code and data) from the rest of the code embedded in the device.

459 Overriding the LPU set of access rights, depending on the TOE configuration, the TOE enforces additional protections on specific parts of the memories.

6.26 Authentication Proof of Identity (FIA_API.1)

460 In Admin configuration or Genuine check configuration, the System Firmware provides commands based on a cryptographic mechanism which allows another IT product to check that the TOE is a genuine TOE.

6.27 Inter-TSF trusted channel (FTP_ITC.1) / Loader, Basic data exchange confidentiality (FDP_UCT.1) / Loader, Data exchange integrity (FDP_UIT.1) / Loader & Audit storage (FAU_SAS.1) / Loader

461 In Admin configuration, the System Firmware provides a secure channel to allow another IT product to operate a maintenance transaction.

462 The ciphered data is automatically decrypted then stored in the requested memory.

463 A maintenance transaction can end only after a successful integrity check of the loaded data or an erase. The identification data associated with the memory update is automatically logged during the session,

6.28 Subset access control (FDP_ACC.1) / Loader & Security attribute based access control (FDP_ACF.1) / Loader

464 In Admin configuration, during a maintenance transaction, the System Firmware verifies if the Loader access conditions are satisfied and returns an error when this is not the case.

465 In particular, the additional memory update must be intended to be assembled with the memory update previously loaded.

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

466 In Admin configuration, the System Firmware enforces that a maintenance transaction can only end when it is consistent or canceled by an erase.

6.30 Static attribute initialisation (FMT_MSA.3) / Loader

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

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

468 In Admin configuration, the System Firmware provides the capability for an authorized user to change part of the Flash Loader security attributes.

6.32 Security roles (FMT_SMR.1) / Loader

469 The System Firmware supports the assignment of roles to users through the assignment of different keys for the different roles. This allows to distinguish between the roles of ST Loader, User Loader, Delegated Loader, Secure Diagnostic, and Everybody.

6.33 Timing of identification (FIA_UID.1) / Loader & Timing of authentication (FIA_UAU.1) / Loader

470 The System Firmware identifies the user through the key selected for authentication. This is performed by verifying an encryption, thus preventing to unveil the key.

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

472 A limited number of operations is allowed on behalf of the user before the user is identified and authenticated, such as boot, authentication and non-critical queries.

6.34 Audit review (FAU_SAR.1) / Loader

473 In Admin configuration, the System Firmware allows to read the product information and the identification data of all memory updates previously loaded on the TOE.

6.35 Security roles (FMT_SMR.1) / MFPlus

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

475 In SL0 when the TOE is in a secure environment, MFPlus identifies and authenticates the role Personaliser by default; in addition the role OriginalityKeyUser can be identified with an explicit authentication request.

476 In the other security levels, MFPlus identifies and authenticates the role Anybody by default and before any authentication request.
The roles CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, TransMACConfManager, CardUser and OriginalityKeyUser are authenticated during the authentication request by the knowledge of the respective cryptographic keys.

6.36 Subset access control (FDP_ACC.1) / MFPlus

477 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.

6.37 Security attribute based access control (FDP_ACF.1) / MFPlus

478 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:

479 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.

480 The OriginalityKeyUser is not allowed to perform any action on objects, but with a successful authentication he can prove the authenticity of the Card.

6.38 Static attribute initialisation (FMT_MSA.3) / MFPlus

481 The MFPlus library initialises all the static attributes to the values defined by MFPlus EV1 interface specifications before they can be used by the Embedded Software.

6.39 Management of security attributes (FMT_MSA.1) / MFPlus

482 The MFPlus library verifies the MFPlus roles and security attributes during the execution of MFPlus commands to enforce the Access Control Policy on the security attributes.

6.40 Specification of Management Functions (FMT_SMF.1) / MFPlus

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

6.41 Import of user data with security attributes (FDP_ITC.2) / MFPlus

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

6.42 Inter-TSF basic TSF data consistency (FPT_TDC.1) / MFPlus

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

6.43 Cryptographic key destruction (FCS_CKM.4) / MFPlus

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

6.44 User identification before any action (FIA_UID.2) / MFPlus

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

6.45 User authentication before any action (FIA_UAU.2) / MFPlus

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

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

6.46 Multiple authentication mechanisms (FIA_UAU.5) / MFPlus

490 The MFPlus library implements the MFPlus Interface Specification, that has a mechanism to authenticate CardAdmin, CardManager, SecurityLevelManager, CardUser, and OriginalityKeyUser, while Anybody is assumed when there is no valid authentication state.

6.47 Management of TSF data (FMT_MTD.1) / MFPlus

491 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.

492 The CardManager is allowed to change the CardConfigurationKey.
The CardAdmin can change the Level3SwitchKey, the Level3SectorSwitchKey and the CardMasterKey itself.
The CardAdmin can also change the TransMACConfKey.

6.48 Trusted path (FTP_TRP.1) / MFPlus

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

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

6.49 Replay detection (FPT_RPL.1) / MFPlus

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

6.50 Unlinkability (FPR_UNL.1) / MFPlus

496 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.

6.51 Minimum and maximum quotas (FRU_RSA.2) / MFPlus

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

6.52 Subset residual information protection (FDP_RIP.1) / MFPlus

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

7 Identification

Table 14. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	Optional NesLib crypto library version	Optional MIFARE Plus EV1 version
K410A	C	0x01F1	3.1.1 and 3.1.2	6.4.7	1.1.2

1. Part of the product information.

Table 15. Guidance documentation

Component description	Reference	Version
Secure dual interface MCU with enhanced security and up to 450 Kbytes of Flash memory- ST31P450 datasheet	DS_ST31P450	2.0
ARM® Cortex SC000 Technical Reference Manual	ARM DDI 0456	A
ARMv6-M Architecture Reference Manual	ARM DDI 0419	C
ST31P450 Firmware V3 - User Manual	UM_ST31P450_FWv3	6.0
ST31P secure MCU platform Security guidance - Application note	AN_SECU_ST31P	1.0
Cryptographic library NesLib 6.4 - User manual	UM_NesLib_6.4	3.0
ST31P secure MCU platforms NesLib 6.4 security recommendations - Application note	AN_SECU_ST31P_NESLIB_6.4	4.0
NesLib 6.4 for ST31 Platforms - Release note	RN_ST31P_NESLIB_6.4.7	3.0
MIFARE Plus EV1 library v1.1 for the ST31P platform devices - User manual	UM_ST31P_MFP_EV1	3.0
MIFARE Plus EV1 library 1.1.2 on ST31P450 : Release Note	RN_ST31P_MFP_EV1_1.1.2	1.0
ST31P platform random number generation - User manual	UM_ST31P_TRNG	2.0
ST31P platform TRNG reference implementation: compliance tests	AN_ST31P_TRNG	1.0

Table 16. Sites list

Site	Address	Activities[1]
Amkor ATP1	AMKOR Technologies ATP1: Km 22 East Service Rd. South Superhighway, Muntinlupa City 1771 Philippines	BE
Amkor ATP3/4	AMKOR Technologies ATP3/4: 119 N. Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines	BE
Amkor ATT1	AMKOR Technologies Taiwan Inc. - T1 No. 1, Kao-Ping Sec, Chung-Feng Road, Longtan District, Taoyuan City 325, Taiwan R.O.C.	BE
Amkor ATT3	AMKOR Technologies Taiwan Inc. - T3 No.11 Guangfu Road, Hsinchu Industrial Park, Hukou Township, Hsinchu County 303, Taiwan, R.O.C.	BE
AMTC / Toppan Germany	Advanced Mask Technology Center Gmbh & Co KG Rahnitzer Allee 9, 01109 Dresden, Germany	MASK
Chipbond JY	Chipbond Technology Corporation No. 10, Prosperity 1 Road, Science Park, HSINCHU, Taiwan ROC	BE
Chipbond LH	Chipbond Technology Corporation No. 3, Li Hsin 5 Road, Science Park, HSINCHU, Taiwan ROC	BE
DNP	Dai Nippon Printing Co., Ltd 2-2-1 Kami-Fukuoka, Fujimino-shi Saitama 356-8507 Japan	MASK
DPE	Dai Printing Europe Via C. Olivetti 2/A I-20041 Agrate Italy	MASK

Table 16. Sites list (continued)

Site	Address	Activities[1]
Feiliks	Feili Logistics (Shenzhen) Co., Ltd. Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHS
Samsung Giheung	Samsung Electronics. Co., Ltd. Samsung-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 17113 Republic of Korea	FE
Samsung Hwaseong	Samsung Electronics. Co., Ltd. Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, 18448 Republic of Korea	MASK
Samsung Onyang	Samsung Electronics. Co., Ltd. 158 Baebang-ro Baebang-eup Asan-City, Chungcheongnam-Do, Korea	FE
Smartflex	Smartflex Technologies 37A Tampines Street 92, Singapore 528886	BE
ST Ang Mo Kio 1	STMicroelectronics 5A Serangoon North Avenue 5 554574 Singapore	DEV
ST Ang Mo Kio 6	STMicroelectronics 18 Ang Mo Kio Industrial park 2 554574 Singapore	WHS
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers – BP97 20180 Bouskoura Maroc	BE WHS
ST Crolles	STMicroelectronics 850 rue Jean Monnet 38926 Crolles France	DEV FE MASK
ST Gardanne	CMP Georges Charpak 880 Avenue de Mimet 13541 Gardanne France	BE

Table 16. Sites list (continued)

Site	Address	Activities[1]
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	DEV
ST Ljubljana	Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive 508938 Singapore	WHS
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark 35700 Rennes France	DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex FRANCE	DEV EWS WHS
ST Shenzen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone 518048 Shenzhen P.R. China	BE
ST Sophia	635 route des lucioles, 06560 Valbonne, France	DEV
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh 319521 Singapore	EWS
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT

Table 16. Sites list (continued)

Site	Address	Activities[1]
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B 3d floor 1831 Diegem/Machelen Belgium	DEV
Toppan Icheon	Toppan Photomasks Korea Ltd. 345-1, Sooha-Ri ShinDoon-Myon, 467-840 Icheon, Korea	MASK
UTAC UTL1	UTAC Thai Limited 1 237 Lasalle Road, Bangna, Bangkok, 10260 Thailand	BE
UTAC UTL3	UTAC Thai Limited 3 73 Moo5, Bangsamak, Bangpakong, Chachoengsao, 24180 Thailand	BE
Winstek	Winstek - STATS ChipPAC (SCT) No 176-5, 6 Lane, Hualung Chun, Chiung Lin, 307 Hsinchu, Taiwan	BE

1. DEV = development, FE = front end manudacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask manufacturing, WHS = warehouse, IT = Network infrastructure

8 References

Table 17. Common Criteria

Component description	Reference	Version
Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017	CCMB-2017-04-001 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2017-04-002 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017	CCMB-2017-04-003 R5	3.1 Rev 5

Table 18. Protection Profile

Component description	Reference	Version
Eurosmart - Security IC Platform Protection Profile with Augmentation Packages	BSI-CC-PP-0084-2014	1.0

Table 19. Other standards

Ref	Identifier	Description
[1]	BSI-AIS20/AIS31	A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler BSI, Version 2.0, 18-09-2011
[2]	NIST SP 800-67	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002
[4]	FIPS PUB 180-2	FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004
[5]	FIPS PUB 186-4	FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), July 2013
[6]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[7]	ISO/IEC 9796-2	ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002
[8]	NIST SP 800-38A	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010

Table 19. Other standards

Ref	Identifier	Description
[9]	NIST SP 800-38B	NIST special publication 800-38B, Recommandation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), May 2005
[10]	NIST SP 800-38C	NIST special publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, National Institute of Standards and Technology (NIST), May 2004
[11]	NIST SP 800-38D	NIST special publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter mode (GCM) and GMAC, National Institute of Standards and Technology (NIST), November 2007
[12]	ISO/IEC 14888	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[13]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[14]	MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
[15]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[16]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[17]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[18]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[19]	NIST SP 800-90	NIST Special Publication 800-90, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), March 2007
[20]	FIPS PUB 198-1	FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[21]	NIST SP 800-56A	NIST SP 800-90A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), May 2013
[22]	ANSI X9.31	ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), American National Standard for Financial Services, 1998

Table 19. Other standards

Ref	Identifier	Description
[23]	ANSI X9.42	ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, American National Standard for Financial Services, 2003 (R2013)
[24]	ANSI X9.62	ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard for Financial Services, 2005
[25]	FIPS PUB 202	FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015
[26]	EdDSA rfc	S. Josefsson and I. Liusvaara,, Edwards-curve Digital Signature Algorithm (EdDSA) draft-irtf-cfrg-eddsa-08, Network Working Group Internet-Draft, IETF, August 19, 2016, available from *https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-08*
[27]	EDDSA	Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "High-speed high-security signatures", *http://ed25519.cr.yp.to/ed25519-20110926.pdf* September 2011
[28]	EDDSA2	Bernstein, D., Josefsson, S., Lange, T., Schwabe, P., and B. Yang, "EdDSA for more curves", WWW *http://ed25519.cr.yp.to/eddsa-20150704.pdf* July 2015
[29]	NOTE 12.1	Note d'application: Modélisation formelle des politiques de sécurité d'une cible d'évaluation NOTE/12.1, N°587/SGDN/DCSSI/SDR DCSSI, 25-03-2008
[30]	ANSSI-CC-NOTE-06/2.0 EN	Security requirements for post-delivery code loading, ANSSI, January 2015
[31]	ANSSI-CC-CER/F/06.002	PP0084: Interpretations, ANSSI, April 2016

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. If "Package 2: Loader dedicated for usage by authorized users only" is used the Pre-personalisation Data

may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.

Secret

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security IC

Composition of the TOE, the Security IC Embedded Software, User Data, and the package.

Security IC Embedded SoftWare (ES)

Software embedded in the Security IC and not developed by the IC designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3.

Security IC embedded software (ES) developer

Institution (or its agent) responsible for the security IC embedded software development and the specification of IC pre-personalization requirements, if any.

Security attribute

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Sensitive information

Any information identified as a security relevant element of the TOE such as:

– the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
– the security IC embedded software,
– the IC dedicated software,
– the IC specification, design, development tools and technology.

Smartcard

A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

Subject

An entity within the TSC that causes operations to be performed.

Test features

All features and functions (implemented by the IC Dedicated Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

TOE Delivery

The period when the TOE is delivered which is after Phase 3 ***or Phase 4 in this Security target***.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data

All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

A.2 Abbreviations

Table 20. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI).
BE	Back End manufacturing.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1. R5.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information.
DES	Data Encryption Standard.
DEV	Development.
DIP	Dual-In-Line Package.
DRBG	Deterministic Random Bit Generator.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
ES	Security IC Embedded Software.
EWS	Electrical Wafer Sort.
FE	Front End manufacturing.
FIPS	Federal Information Processing Standard.
I/O	Input / Output.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
LPU	Library Protection Unit.
MASK	Mask manufacturing.
MFPlus	MIFARE Plus® EV1.
NESCRYPT	Next Step Cryptography Accelerator.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.

Table 20. List of abbreviations (continued)

Term	Meaning
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or Security Target.
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.
WHS	Warehouse.