STMicroelectronics

MIFARE® DESFire® EV3 on ST31R480 A01
Security Target for composition

Common Criteria for IT security evaluation

SMD_MFDFEV3_ST31R480_ST_24_002 Rev 01.2

June 2025

life.augmented

BLANK

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: MIFARE DESFire EV3 on ST31R480 A01 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev 01.2, issued in June 2025.

3 Registration: registered at ST Microelectronics under number SMD_MFDFEV3_ST31R480_ST_24_002.

1.2 TOE reference

4 This document presents **the Security Target for composition (ST)** of the technology library **MIFARE® DESFire® EV3**[a] on the Security IC **ST31R480 A01.**

5 This TOE is a composite TOE, built up with the combination of:

- The Security IC **ST31R480 A01**, designed by STMicroelectronics, and used as certified platform,
- The technology library **MIFARE DESFire EV3**, developed by STMicroelectronics, and built to operate with this Security IC platform.

6 Therefore, this Security Target is built on the Security IC Security Target *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*, referenced *BSI-CC-PP-0084-2014*.
The Security IC Security Target is called “Platform Security Target” in the following.

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

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

[a] MIFARE and DESFire are registered trademarks of NXP B.V. and are used under license.

Contents

List of tables

List of figures

1.3 Context

9 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 Connected Security sub-group of STMicroelectronics (ST).

10 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by ASE_TSS.2, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and the composite product package (COMP).

11 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE, and to summarise its chosen TSF services and assurance measures.
Since the TOE is a composite TOE, this Security Target is built on the Security IC Security Target *ST31R480 A01 Security Target for composition*, referenced *SMD_ST31R480_ST_23_002*.

12 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.

13 The Platform Security Target introduces the following augmentations:

- Addition #1: “Support of Cipher Schemes” from *[AUG]*
- Addition #4: “Area based Memory Access Control” from *[AUG]*.
- Additions specific to the Platform Security Target, some in compliance with *[JILSR]* and *ANSSI-PP0084.03*.

14 This Security Target introduces augmentations dedicated to MIFARE DESFire EV3.

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

15 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 ***JIL*** for *[JILSR]*.

1.4 TOE identification

16 The Target of Evaluation (TOE) is the technology library MIFARE DESFire EV3 on ST31R480 A01.

17 “MIFARE DESFire EV3 on ST31R480 A01” completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 16: Guidance documentation*, and its development and production sites indicated in *Table 17: Sites list*.
Refer also to the corresponding tables in the *ST31R480 A01 Security Target for composition*.

Table 1. TOE components

Platform identification				Library identification
IC Maskset name	IC version	Master identification number	Firmware version	MIFARE DESFire EV3 version
K4H0A	B	0x0299	3.0.6	1.0.3

18 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 the *ST31R480 A01 Security Target for composition*.

19 In this Security Target, the term "MFDF" means MIFARE® DESFire® EV3 1.0.3.

20 The MIFARE DESFire EV3 User Manual, referenced in *Table 16: Guidance documentation,* details how to check the library integrity and version.

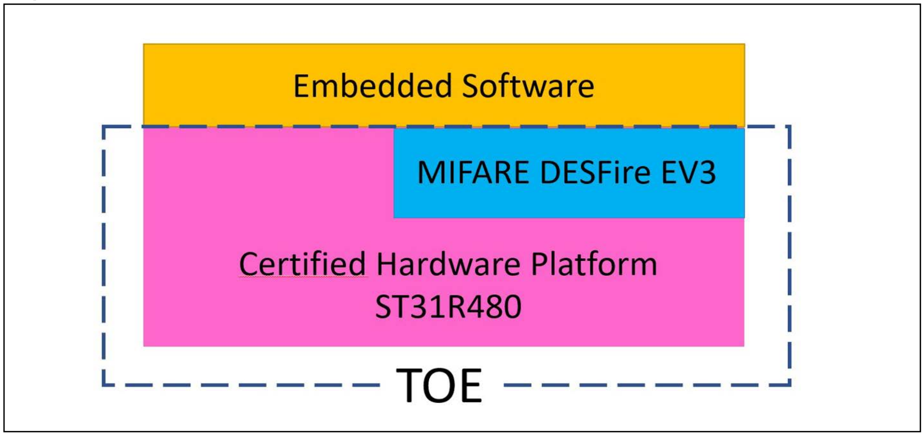
1.5 TOE overview

21 This TOE consists of a certified hardware platform and an applicative embedded software, MIFARE DESFire EV3, stored in the hardware User NVM of the Platform.

22 The hardware platform is the ST31R480 with its firmware. It is identified as ST31R480 A01 which means it includes the components listed in the “Platform identification” columns in*Table 1: TOE components*, and detailed in the Security IC Security Target *ST31R480 A01 Security Target for composition*, referenced *SMD_ST31R480_ST_23_002*.
The ST31R480 is designed to enable an effective usage of MIFARE DESFire EV3, and underly its security functionality.
The Platform Security Target references the guidance documentation directly related to the hardware platform.

23 *Figure 1* provides an overview of the TOE.

Figure 1. TOE overview



24 The TOE is primarily designed for secure contact-less transport applications, loyalty programs, access control management systems as well as closed loop payment systems. It

fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

25 The MIFARE technology library MIFARE DESFire EV3 features a mutual three pass authentication, a data encryption on RF channel, and a flexible self-securing file system.

26 MIFARE DESFire EV3 has its own guidance documentation, listed in*Table 16: Guidance documentation*.

27 The hardware platform is not fully described in the present Security Target, all useful information can be found in its dedicated Platform Security Target *[PF-ST]*. Nevertheless, the related assets, assumptions, threats, objectives and SFRs are reproduced in this document.

1.6 TOE description

1.6.1 TOE hardware description

28 The ST31R480 A01 is described in the Platform Security Target *ST31R480 A01 Security Target for composition*.

29 Note that the usage of the hardware platform and associated firmware is not limited or constrained when MIFARE DESFire EV3 is embedded. The functions provided by the Security IC platform remain normally accessible to the ES, as well as its life-cycle.

30 The only exception is the Library Protection Unit (LPU) of the hardware platform which is dedicated to the protection of MIFARE DESFire EV3, ensuring that no application can read, write, compare any piece of data or code belonging to MFDF. Thus, the LPU is not available for any other usage.

1.6.2 TOE software description

31 The ST31R480 A01 firmware, included in the platform evaluation is described in the *ST31R480 A01 Security Target for composition*.

32 The TOE comprises a secure applicative Embedded Software, a MIFARE technology library, which is embedded in the User NVM of the Platform by ST, and protected for confidentiality and integrity of code and data by the LPU. MFDF is used in the User configuration mode of the hardware platform.

33 MIFARE® DESFire® EV3, features:

- flexible file system that groups user data into applications and files within each application,
- support for different file types like values or data records,
- State-of-the-art mutual authentication and Secure Messaging as introduced in DESFire EV2,
- mutual three pass authentication according to ISO 7816-4,
- authentication on application level with fine-grained access conditions for files,
- multi-application support that allows distributed management of applications and ensures application segregation,
- delegated-application support that allows third party service providers to create their applications onto the issued TOE,
- multiple application selection that allows transaction over files in two applications,
- data encryption on the communication path,
- Message Authentication Codes (MAC) for replay attack protection,
- transaction system with rollback that ensures consistency for complex transactions,
- unique serial number for each device (UID) with optional random UID,
- key set rolling feature per application to switch to a predefined key set,
- transaction MAC feature to prevent fraudulent merchant attacks,
- originality functionality that allows verifying the authenticity of the TOE,
- Virtual Card architecture to allow multiple applications on one device,
- proximity check feature against replay attacks on the TOE,
- secure dynamic messaging which allows confidential and integrity protected data exchange without requiring a preceding authentication,
- MIFARE DESFire EV0 backward compatible mode for authentication and secure messaging

34 The recommended authentication and secure messaging is called EV2 secure messaging that is covered by the Security Functional Requirement mentioned in this Security Target.

35 The TOE supports a MIFARE DESFire EV1 backward compatible authentication, the certification scope is limited to the AES mode (both for authentication and secure messaging) and 3TDEA (only authentication) so 3-key Tripe-DES. Hence, 2-key Triple-DES authentication is not part of any Security Functional Requirement of this Security Target and is therefore not in the scope of the evaluation.

36 The MIFARE DESFire EV0 backward compatible mode is not part of any SFR and therefore not in the certification scope.

Note: The ES is not part of the TOE and is out of the scope of the evaluation, except MIFARE DESFire EV3. Proximity Check and Virtual Card Architecture are also out of scope.

37 Note that the notion of various different roles and privileges does not exist for the MFDF library. Only one role (the ES) is defined at the level of the MFDF library and there are no privileges, the ES having access to all the functions of the MFDF API.

38 If privacy is an issue, the TOE can be configured not to disclose any information to unauthorised users.

1.6.3 TOE documentation

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

- the platform user guidance documentation listed in the *ST31R480 A01 Security Target for composition*,
- The *MIFARE® DESFire® EV3 library v1.0 for the ST31R platform devices - User manual - 1*
- The *MIFARE DESFire EV3 interface specification - Technical note*
- The *MIFARE® DESFire® EV3 on ST31R: Guidance and operational manual*
- The *MIFARE® DESFire® EV3 library 1.0.3 on ST31R480 - Release note*

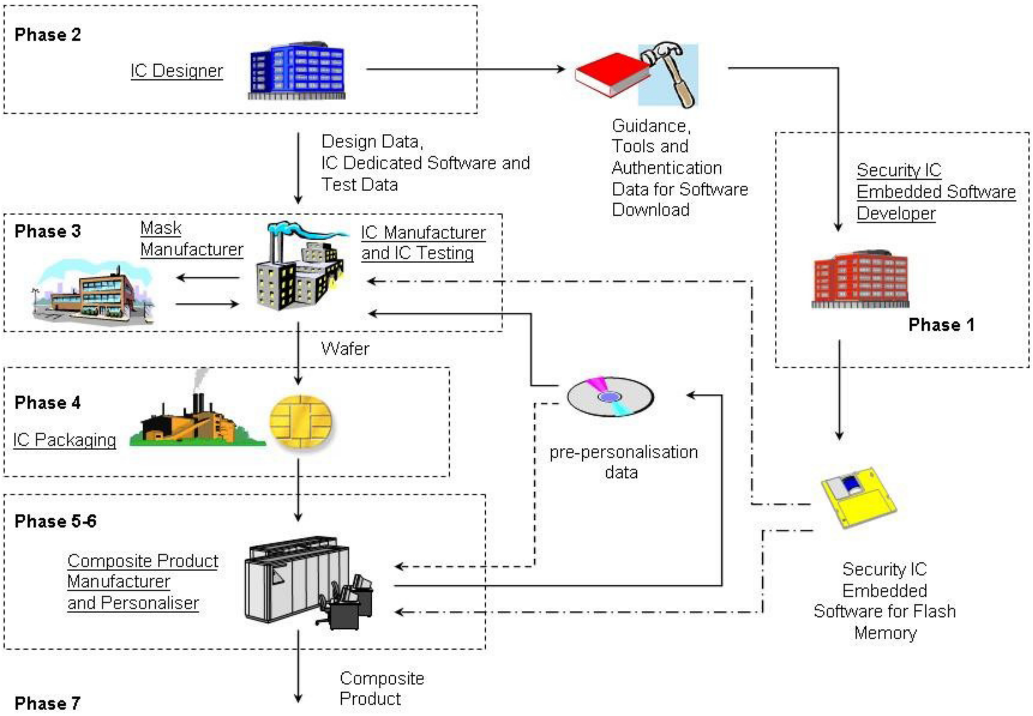
40 The complete list and details of guidance documents is provided in *Table 16*, except those of the platform, listed in the *ST31R480 A01 Security Target for composition*.

1.7 TOE life cycle

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

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

Figure 2. Security IC Life-Cycle



43 The life cycle phases are summarized in *Table 2*.

44 The security IC platform life cycle is described in the Platform Security Target, as well as its delivery format.

45 All the sites likely to be involved in the complete TOE life cycle are listed in *Table 17*, except those dedicated to the Security IC platform, already detailed in the Platform Security Target. In *Table 17*, the library development centers are denoted by the activity “ES-DEV”. The IT support centers are denoted by the activity "IT".

46 MFDF is developed as part of Phase 1, then embedded by ST in the User NVM of the platform, in Phase 3, in one of the sites denoted by the activity “EWS” in the Platform Security Target.

47 The TOE is then delivered as described in the Platform Security Target, i.e. after Phase 3 in form of wafers or after Phase 4 in packaged form, depending on the customer’s order.

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

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

49 The sites potentially involved in the complete TOE life cycle are listed in *Table 17*, except those dedicated to the Security IC platform, already detailed in the Platform Security Target.

Table 2. Composite product life cycle phases

Phase	Name	Description
1	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	integration and photomask fabrication IC production IC testing Initialisation pre-personalisation if necessary
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary
5	Composite product integration	composite product finishing process
6	Personalisation	composite product personalisation composite product testing
7	Operational usage	composite product usage by its issuers and consumers

1.7.1 TOE intended usage

50 In Phase 7, the TOE is in the end-user environments. Depending on the application, the composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are secure contact-less transport applications and related loyalty programs, access control systems, closed loop payment systems.

51 The end-user environment therefore covers a wide range of very different functions. The TOE is designed to be used in unsecured and unprotected environments.

1.7.2 Delivery format and method

52 MIFARE DESFire EV3 is delivered with the Security IC, already embedded by ST, in phase 3 or 4.

53 The Security IC platform can be delivered in form of wafers, micromodules or packages, as described in the *ST31R480 A01 Security Target for composition*.

54 All the possible forms of delivery are equivalent from a security point of view.

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

2 Conformance claims (ASE_CCL, ASE_ECD)

2.1 Common Criteria conformance claims

56 The MIFARE DESFire EV3 on ST31R480 A01 Security Target claims to be conformant to the Common Criteria 2022 revision 1.

More precisely the MIFARE DESFire EV3 on ST31R480 A01 Security Target is:

• CC Part 2 extended, where *CCMB-2022-11-002 R1* is extended with FAU_SAS.1 and FDP_ETC.3, and,

57 • CC Part 3 conformant, cf. *CCMB-2022-11-003 R1*.

58 The extended Security Functional Requirement FAU_SAS Audit data storage is defined in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*).

59 The extended Security Functional Requirement FDP_ETC.3 Export of user data in unauthenticated state is defined in *Section 5* of this Security Target.

60 The assurance level for the MIFARE DESFire EV3 on ST31R480 A01 Security Target is EAL5 augmented by ALC_DVS.2, ASE_TSS.2, AVA_VAN.5, ALC_FLR.2 and the composite package (COMP).

61 The composite product package is defined in *CCMB-2022-11-005 R1*.

62 The ST31R480 A01 platform has been evaluated according to the evaluation level EAL6 augmented with ASE_TSS.2 and ALC_FLR.2, thus ensuring compatibility between the assurance levels chosen for the platform and this composite evaluation.

2.2 PP Claims

2.2.1 PP Reference

63 The MIFARE DESFire EV3 on ST31R480 A01 Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), as required by this Protection Profile.

64 The following packages have been selected from the *BSI-CC-PP-0084-2014*, and completely addressed by the Security IC platform:

- 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 authorised users only.

2.2.2 PP Additions

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

- Those described in the *ST31R480 A01 Security Target for composition*,
- Specific additions for MFDF.

66 These additions are used to address additional functionality provided by the TOE, and not covered by the *Eurosmart - Security IC Platform Protection Profile with Augmentation*

Packages, nor by the Platform Security Target *ST31R480 A01 Security Target for composition*. They address the additional security functionality provided by MFDF.

67 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 *[JILSR]* is typeset as indicated here.

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

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

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

71 The additional SARs relative to the PP are summarized in *Table 8*.

2.2.3 PP Claims rationale

72 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 6*. They have been introduced in the previous section.

73 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*.

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

75 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*.

76 Similarly, the security requirements rationale presented in *Section 6.4* has been updated with respect to the Protection Profile.

77 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.

2.2.4 Rationale regarding CC:2022

78 The SFRs defined in *BSI-CC-PP-0084-2014*, including the functional packages, are conformant to the CC version 3.1. Since this Security Target conforms to the CC:2022, the SFRs have been updated to both comply with CC:2022 and meet *BSI-CC-PP-0084-2014*.

The *Table 3* provides the rationale of the changes.

Table 3. CC:2022 rationale

SFR	*BSI-CC-PP-0084-2014* and *CCMB-2017-04-002 R5* definition	*CCMB-2022-11-002 R1* definition	Change
FMT_LIM.1	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 [assignment: Limited capability policy].	The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: Limited capability and availability policy].	The CC:2022 definition modifies the wording of the SFR to emphasize that the TSF shall limit its capabilities. The new SFR modifies the assignment to limit availability. The CC:2022 version explicitly links the limited capability and limited availability policies, not only at the level of the dependencies. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.
FMT_LIM.2	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited availability policy].	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].	The new SFR modifies the assignment to limit capability. The CC:2022 version explicitly links the limited capability and limited availability policies, not only at the level of the dependencies. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.
FDP_SDC.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*].	The TSF shall ensure the confidentiality of [selection: *all user data, the following user data* [assignment: *list of user data*]] while it is stored in the [selection: *temporary memory, persistent memory, any memory*].	The new SFR provides the option to select the type of data and memory type. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.

Table 3. CC:2022 rationale (continued)

SFR	***BSI-CC-PP-0084-2014*** **and** ***CCMB-2017-04-002 R5*** **definition**	***CCMB-2022-11-002 R1*** **definition**	**Change**
FIA_API.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [selection: *TOE*, [assignment: *object, authorized user or role*]] to an external entity.	The TSF shall provide an [assignment: *authentication mechanism*] to prove the identity of [assignment: *entity*] by including the following properties [assignment: *list of properties*] to an external entity.	A selection is replaced by an assignment: the SFR in CC:2022 is more flexible than in CC 3.1. Nevertheless, the instantiation made in this Security Target meets the SFR defined in the PP.
FAU_SAR.1	The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.	The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit data.	The new definition changes the term "record" with the term "data". The change does not have any impact.
	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.	The TSF shall provide the audit data in a manner suitable for the user to interpret the information.	
FCS_RNG.1	The TSF shall provide a [selection: *physical, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].	The TSF shall provide a [selection: *physical, nonphysical* true, deterministic, hybrid physical, hybrid *deterministic*] random number generator that implements: [assignment: *list of security capabilities*].	The first selection add the terms “non physical true” and “deterministic”. The change does not have any impact.
	The TSF shall provide [selection: *bits, octets of bits,* numbers [assignment: format *of the numbers]*] that meet [assignment: *a defined quality metric*].	The TSF shall provide [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]] that meet [assignment: *a defined quality metric*].	

Table 3. CC:2022 rationale (continued)

SFR	*BSI-CC-PP-0084-2014* and *CCMB-2017-04-002 R5* definition	*CCMB-2022-11-002 R1* definition	Change
FCS_CKM.4	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction *method*] that meets the following: [assignment: *list of standards*].	Removed SFR.	FCS_CKM.6 is replacing FCS_CKM.4. FCS_COP.1 has a dependency on FCS_CKM.6. FCS_CKM.6 in CC:2022 is more flexible than FCS_CKM.4 in CC 3.1. Nevertheless, although no instantiation is made in this Security Target, the dependency is discussed later and this change has no impact.
FCS_CKM.6	Not present.	The TSF shall destroy [assignment: *list of* cryptographic keys (including *keying material)*] when [selection: *no longer* needed, [assignment: other circumstances for key or keying material destruction]].	
		The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction *method*] that meets the following: [assignment: *list of standards*].	

3 Security problem definition (ASE_SPD)

79 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.

80 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security aspects defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security aspects have been introduced in the Platform Security Target and in this one.

81 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3.

82 A summary of all these security aspects with their respective origin and status of inclusion in the *ST31R480 A01 Security Target for composition* is provided in *Table 4*.
All the security aspects defined in the *ST31R480 A01 Security Target for composition* are valid for the present Security Target.

83 Only the ones introduced in this Security Target, are detailed in the following sections (column “In *[PF-ST]* ” = No).

Table 4. **Summary of security aspects**

	Label	Title	Origin	In *[PF-ST]*
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage	*[PP0084]*	Yes
	BSI.T.Phys-Probing	Physical Probing	*[PP0084]*	Yes
	BSI.T.Malfunction	Malfunction due to Environmental Stress	*[PP0084]*	Yes
	BSI.T.Phys-Manipulation	Physical Manipulation	*[PP0084]*	Yes
	BSI.T.Leak-Forced	Forced Information Leakage	*[PP0084]*	Yes
	BSI.T.Abuse-Func	Abuse of Functionality	*[PP0084]*	Yes
	BSI.T.RND	Deficiency of Random Numbers	*[PP0084]*	Yes
	BSI.T.Masquerade-TOE	Masquerade the TOE	*[PP0084]*	Yes
	AUG4.T.Mem-Access	Memory Access Violation	*[AUG]*	Yes
	JIL.T.Open-Samples-Diffusion	Diffusion of open samples	*[JILSR]*	Yes
	MFDF.T.Data-Modification	Unauthorised data modification		No
	MFDF.T.Impersonate	Impersonating authorised users during authentication		No
	MFDF.T.Cloning	Cloning		No
	T.Confid-Appli-Code	Specific application code confidentiality		Yes
	T.Confid-Appli-Data	Specific application data confidentiality		Yes
	T.Integ-Appli-Code	Specific application code integrity		Yes
	T.Integ-Appli-Data	Specific application data integrity		Yes
	MFDF.T.Resource	Resource availability		No
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production	*[PP0084]*	Yes
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality	*[PP0084]*	Yes
	BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality	*[PP0084]*	Yes
	AUG1.P.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	MFDF.P.Encryption	Confidentiality during communication		No
	MFDF.P.MAC	Integrity during communication		No
	MFDF.P.No-Trace	Untraceability of end-users		No
	MFDF.P.Transaction	Transaction mechanism		No
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	*[PP0084]*	Yes
	BSI.A.Resp-Appl	Treatment of User Data	*[PP0084]*	Yes
	MFDF.A.Secure-Values	Usage of secure values		No
	MFDF.A.Terminal-Support	Terminal support		No
	MFDF.A.KeyFunction	Usage of Key-dependent Functions		No

3.1 Description of assets

84 This Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*). The high-level concerns and the assets to be protected are described in section 3.1 of this Protection Profile and also in the *ST31R480 A01 Security Target for composition*.

85 The list of assets is given below:

- The user data of the composite TOE.
- The Security IC Embedded Software, stored and in operation.
- The Security Services provided by the TOE for the Security IC Embedded Software.

86 These assets are related to the following high level security concerns:

- The user data of the composite TOE
- Integrity of user data of the Composite TOE.
- Confidentiality of user data of the Composite TOE being stored in the TOE’s protected memory areas.
- Correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- Deficiency of random numbers.

87 To be able to protect the assets the TOE shall self-protect its security functionality. Critical information about the security functionality shall be protected by the development environment and the operational environment. Critical information may includes:

- Logical design data, physical design data, IC Dedicated Software, Security IC Embedded Software and configuration data.
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photomasks.

88 Note that the keys for the cryptographic co-processors are seen as User Data.

3.2 Threats

89 The threats related to the platform are described in the Platform Security Target *[PF-ST]*, and just recalled here:

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

JIL.T.Open-Samples-Diffusion	Diffusion of open samples

90 The following additional threats related to MFDF are added to the Security Problem Definition of this security target:

MFDF.T.Data-Modification
: Unauthorised data modification:

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

MFDF.T.Impersonate
: Impersonating authorised users during authentication:

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.

MFDF.T.Cloning
: Cloning:

User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.

MFDF.T.Resource
: Resource availability:

The availability of the TOE resources for the MIFARE DESFire EV3 Licensed product shall be controlled to prevent denial of service or malfunction.
An attacker prevents correct execution of MIFARE DESFire EV3 Licensed product through consumption of some resources of the card: e.g. RAM or non-volatile RAM.

3.3 Organisational security policies

91 These security policies are described in the Platform Security Target *[PF-ST]*, and just recalled here:

BSI.P.Process-TOE	Identification 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

92 The TOE provides specific security functionality that can be used by MIFARE DESFire EV3. 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 MFDF will use the specific security functionality.

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

94 MFDF.P.Confidentiality, MFDF.P.MAC, MFDF.P.Transaction and MFDF.P.No-Trace are related to MFDF.

MFDF.P.Encryption Confidentiality during communication:

The TOE shall provide the possibility to protect selected data elements from eavesdropping during contact-less communication.

MFDF.P.MAC Integrity during communication:

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.

MFDF.P.Transaction Transaction mechanism:

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

MFDF.P.No-Trace Un-traceability of end-users:

The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised subjects without consent. Tracing of end-users may happen by performing a contact-less communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element.

3.4 Assumptions

95 The following assumptions are described in the Platform Security Target *[PF-ST]* and 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

96 The next assumptions are added for MFDF. They are required for the correct functioning of MFDF security functionality.
They do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, since they are only related to assets which are out of the scope of this PP.

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

MFDF.A.Secure-Values Usage of secure values:

Only confidential and secure cryptographically strong keys shall be used to set up the authentication. These values are generated outside the TOE and they are downloaded to the TOE.

MFDF.A.Terminal-Support Terminal support:

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]* for the authentication

MFDF.A.KeyFunction Usage of Key-dependent Functions:

Key-dependent Functions (if any) shall be implemented in the Security IC Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

Note that here the routines which may compromise keys when being executed are part of the Security IC Embedded Software. In contrast to this, the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE (ii) the processing of User Data including cryptographic keys.

4 Security objectives (ASE_OBJ)

98 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 access control functionality,
- provide cryptographic support.

99 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security objectives defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security objectives have been introduced in the Platform Security Target and in this one.

100 Note that the origin of each security objective 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.

101 A summary of all the TOE security objectives with their respective origin and status of inclusion in the *ST31R480 A01 Security Target for composition* is provided in *Table 5*.
All the security objectives defined in the *ST31R480 A01 Security Target for composition* are valid for the present Security Target.

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

Table 5. Summary of security objectives

	Label	Title	Origin	In *[PF-ST]*
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage	*[PP0084]*	Yes
	BSI.O.Phys-Probing	Protection against Physical Probing	*[PP0084]*	Yes
	BSI.O.Malfunction	Protection against Malfunctions	*[PP0084]*	Yes
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation	*[PP0084]*	Yes
	BSI.O.Leak-Forced	Protection against Forced Information Leakage	*[PP0084]*	Yes
	BSI.O.Abuse-Func	Protection against Abuse of Functionality	*[PP0084]*	Yes
	BSI.O.Identification	TOE Identification	*[PP0084]*	Yes
	BSI.O.RND	Random Numbers	*[PP0084]*	Yes
	BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader	*[PP0084]*	Yes
	BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader	*[PP0084]*	Yes

Table 5. Summary of security objectives (continued)

	Label	Title	Origin	In *[PF-ST]*
TOE	JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF	*[JILSR]*	Yes
	JIL.O.Secure-Load-ACode	Secure loading of the Additional Code	*[JILSR]*	Yes
	JIL.O.Secure-AC-Activation	Secure activation of the Additional Code	*[JILSR]*	Yes
	JIL.O.TOE-Identification	Secure identification of the TOE	*[JILSR]*	Yes
	O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image	*[PF-ST]*	Yes
	O.MemImage-Identification	Secure identification of the Memory Image	*[PF-ST]*	Yes
	BSI.O.Authentication	Authentication to external entities	*[PP0084]*	Yes
	AUG1.O.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control	*[AUG]*	Yes
	MFDF.O.Access-Control	Access Control for MFDF		No
	MFDF.O.Authentication	Authentication for MFDF		No
	MFDF.O.Encryption	MFDF Confidential Communication		No
	MFDF.O.MAC	MFDF Integrity-protected Communication		No
	MFDF.O.Type-Consistency	MFDF Data type consistency		No
	MFDF.O.Transaction	MFDF Transaction mechanism		No
	MFDF.O.No-Trace	Preventing Traceability for MFDF		No
	MFDF.O.Resource	Resource availability for MFDF		No
	O. Firewall	Specific application firewall		Yes
	MFDF.O.Shr-Res	MFDF data cleaning for resource sharing		No
	MFDF.O.Verification	MFDF code integrity check		No

Table 5. Summary of security objectives (continued)

	Label	Title	Origin	In [PF-ST]
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE	[PP0084]	Yes
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	[PP0084]	Yes
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	[PP0084]	Yes
	BSI.OE.Loader-Usage	Secure communication and usage of the Loader	[PP0084]	Yes
	BSI.OE.TOE-Auth	External entities authenticating of the TOE	[PP0084]	Yes
	OE.Composite-TOE-Id	Composite TOE identification	[PF-ST]	Yes
	OE.TOE-Id	TOE identification	[PF-ST]	Yes
	OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	[PF-ST]	Yes
	OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	[PF-ST]	Yes
	MFDF.OE.Secure-Values	Generation of secure values for MFDF		No
	MFDF.OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers MFDF		No

4.1 Security objectives for the TOE

103 These security objectives are described in the Platform Security Target *[PF-ST]*

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

JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF
JIL.O.Secure-Load-ACode	Secure loading of the Additional Code
JIL.O.Secure-AC-Activation	Secure activation of the Additional Code
JIL.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
AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
AUG1.O.Add-Functions	Additional Specific Security Functionality
O.Firewall	Specific application firewall

104 The following objectives are added for MFDF:

MFDF.O.Access-Control

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

MFDF.O.Authentication

Authentication for MFDF:
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.

MFDF.O.Encryption

MFDF 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.

MFDF.O.MAC

MFDF Integrity-protected Communication:
The TOE must be able to protect the communication by adding a MAC. This shall be implemented by security attributes that enforce integrity protected communication for the respective data elements. Usage of the protected communication shall also support the detection of injected and bogus commands within the communication session before the protected data transfer.

MFDF.O.Type-Consistency

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

MFDF.O.Transaction

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

MFDF.O.No-Trace	Preventing Traceability for MFDF: The TOE must be able to prevent that the TOE end-user can be traced. This shall be done by providing an option that disables the transfer of any information that is suitable for tracing an end-user by an unauthorised subject.
MFDF.O.Resource	Resource availability for MFDF: The TOE shall control the availability of resources for MIFARE DESFire EV3 Licensed product.
MFDF.O.Shr-Res	MFDF data cleaning for resource sharing: It shall be ensured that any hardware resource, that is shared by MIFARE DESFire EV3 and other applications or by any application which has access to such hardware resource, is always cleaned (using code that is part of the MIFARE DESFire EV3 system and its certification) whenever MIFARE DESFire EV3 is interrupted by the operation of another application. The only exception is buffers as long as these buffers do not contain other information than what is communicated over the contactless interface or has a form that is no different than what is normally communicated over the contacless interface. For example, no data shall remain in a hardware crytographic coprocessor (e.g. DES or AES coprocessor) when MIFARE DESFire EV3 is interrupted by another application.
MFDF.O.Verification	MFDF code integrity check: The TOE shall ensure that MIFARE DESFire EV3 code is verified prior being executed.

4.2 Security objectives for the environment

105 The following security objectives for the environment are detailed in the *ST31R480 A01 Security Target for composition* and still valid in the same terms for this Security Target. The clarifications made there also apply.

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

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

107 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	Up to phase 6

BSI.OE.Loader-Usage	Secure communication and usage of the Loader	Up to phase 7
BSI.OE.TOE-Auth	External entities authenticating of the TOE	Up to phase 7
OE.Composite-TOE-Id	Composite TOE identification	Up to phase 7
OE.TOE-Id	TOE identification	Up to phase 7
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	Up to phase 7
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	Up to phase 7

108 The following security objectives for the operational environment (phase 5 up to 7) are added for MFDF:

MFDF.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 to 7.

MFDF.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

109 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* Protection Profile, those already introduced in the *ST31R480 A01 Security Target for composition* 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.

110 Thus, it is necessary to show that:

- security environment aspects from this ST, are addressed by security objectives stated in this chapter,
- security objectives from this ST, are suitable (i.e. they address security environment aspects),
- security objectives from this ST, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).

111 All security aspects are already justified in the Platform Security Target *[PF-ST]*, except the ones denoted by "New" in *Table 6*.

112 The augmentations made in this ST introduces the following security environment aspects related to MIFARE DESFire EV3:

- TOE threats "Unauthorised data modification for MFDF, (*MFDF.T.Data-Modification*)", "Impersonating authorised users during authentication for MFDF, (*MFDF.T.Impersonate*)", "Cloning for MFDF, (*MFDF.T.Cloning*)", and "MFDF resource availability, (*MFDF.T.Resource*)".
- organisational security policies "Confidentiality during communication, (*MFDF.P.Encryption*)", "Integrity during communication, (*MFDF.P.MAC*)", "Un-traceability of end-users, (*MFDF.P.No-Trace*)", and "Transaction mechanism, (*MFDF.P.Transaction*)".
- assumptions "Usage of secure values, (*MFDF.A.Secure-Values*)", "Terminal support, (*MFDF.A.Terminal-Support*)", and "Usage of Key-dependent Functions, (*MFDF.A.KeyFunction*)".

113 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* and *ST31R480 A01 Security Target for composition* for the assumptions, policy and threats defined there.

114 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 MFDF, which is out of the scope of this Protection Profile.

115 Only the security aspects denoted by "New" in *Table 6* will be detailed in the following.

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
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*	

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
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*	
JIL.T.Open-Samples-Diffusion	*JIL.O.Prot-TSF-Confidentiality* *BSI.O.Leak-Inherent* *BSI.O.Leak-Forced*	
MFDF.T.Data-Modification	*MFDF.O.Access-Control* *MFDF.O.Type-Consistency* *MFDF.OE.Terminal-Support*	New
MFDF.T.Impersonate	*MFDF.O.Authentication*	New
MFDF.T.Cloning	*MFDF.O.Access-Control* *MFDF.O.Authentication*	New
T.Confid-Appli-Code	*O. Firewall*	
T.Confid-Appli-Data	*O. Firewall*	
T.Integ-Appli-Code	*MFDF.O.Verification* *O. Firewall*	
T.Integ-Appli-Data	*MFDF.O.Shr-Res* *O. Firewall*	
MFDF.T.Resource	*MFDF.O.Resource*	New
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	
BSI.P.Ctrl-Loader	*BSI.O.Ctrl-Auth-Loader* *JIL.O.Secure-Load-ACode* *JIL.O.Secure-AC-Activation* *JIL.O.TOE-Identification* *O.Secure-Load-AMemImage* *O.MemImage-Identification* *BSI.OE.Loader-Usage* *OE.TOE-Id* *OE.Composite-TOE-Id*	
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
MFDF.P.Encryption	*MFDF.O.Encryption*	New

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
MFDF.P.MAC	*MFDF.O.MAC*	New
MFDF.P.No-Trace	*MFDF.O.No-Trace* *MFDF.O.Access-Control* *MFDF.O.Authentication*	New
MFDF.P.Transaction	*MFDF.O.Transaction*	New
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
MFDF.A.KeyFunction	*BSI.OE.Resp-Appl*	Phase 1
MFDF.A.Secure-Values	*MFDF.OE.Secure-Values*	New Phases 5-7
MFDF.A.Terminal-Support	*MFDF.OE.Terminal-Support*	New Phase 7

4.3.1 Assumption "Usage of secure values"

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

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

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

4.3.2 Assumption "Terminal support"

119 The justification related to the assumption “Terminal support, (*MFDF.A.Terminal-Support*)” is as follows:

120 The objective *MFDF.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.

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

4.3.3 Assumption "Usage of Key-dependent Functions"

122 The justification related to the assumption “Usage of Key-dependent Functions, (*MFDF.A.KeyFunction*)” is as follows:

123 *BSI.OE.Resp-Appl* requires the Security IC Embedded Software to implement measures to manage the cryptographic keys appropriately to ensure the strength of the cryptographic operation, therefore it covers the assumption.

124 *MFDF.A.KeyFunction* does not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, because it is only related to MFDF, which is out of the scope of this Protection Profile.

4.3.4 TOE threat "Unauthorised data modification for MFDF"

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

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

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

4.3.5 TOE threat "Impersonating authorised users during authentication for MFDF"

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

129 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. *MFDF.O.Authentication* requires that the authentication mechanism provided by the TOE shall be resistant against attack scenarios targeting the impersonation of authorised users. Therefore the threat is covered by *MFDF.O.Authentication*.

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

4.3.6 TOE threat "Cloning for MFDF"

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

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

users are authenticated before they can read any information that is restricted to authorised users. Therefore the two objectives cover *MFDF.T.Cloning*.

4.3.7 TOE threat "MFDF resource availability"

133 The justification related to the threat “MFDF resource availability, (*MFDF.T.Resource*)” is as follows:

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

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

4.3.8 TOE threat "Specific application code integrity"

136 Additional justification for MFDF related to the threat “Specific application code integrity, *T.Integ-Appli-Code*” is as follows:

137 The threat is related to the alteration of MFDF code by an attacker. *MFDF.O.Verification* requires that the TOE verifies the code integrity before its execution.

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

4.3.9 TOE threat "Specific application data integrity"

139 Additional justification for MFDF related to the threat “Specific application data integrity, *T.Integ-Appli-Data”* is as follows:

140 The threat is related to the alteration of MFDF data by an attacker. Since *MFDF.O.Shr-Res* require that the TOE ensures isolation of data between MFDF and the other applications, the data of MFDF is protected against unauthorised modification, therefore MFDF.T.Integ-Applic-data is also covered by *MFDF.O.Shr-Res*.

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

4.3.10 Organisational security policy "Confidentiality during communication"

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

143 *MFDF.O.Encryption* is an immediate transformation of the security policy, therefore it covers the Security Policy.

144 The added objective for the TOE *MFDF.O.Encryption* does not introduce any contradiction in the security objectives.

4.3.11 Organisational security policy "Integrity during communication"

145 The justification related to the organisational security policy "Integrity during communication, (*MFDF.P.MAC*)” is as follows:

146 *MFDF.O.MAC* is an immediate transformation of the security policy, therefore it covers the Security Policy.

147 The added objective for the TOE *MFDF.O.MAC* does not introduce any contradiction in the security objectives.

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

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

149 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.

150 *MFDF.O.Access-Control* provides means to implement access control to data elements on the TOE and *MFDF.O.Authentication* provides means to implement authentication on the TOE, in order to prevent tracing based on freely accessible data elements. *MFDF.O.No-Trace* requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorised subject, which includes the UID. Therefore the policy is covered by these three objectives.

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

4.3.13 Organisational security policy "Transaction mechanism"

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

153 *MFDF.O.Transaction* is an immediate transformation of the security policy, therefore it covers the Security Policy.

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

5 Extended Component Definition (ASE_ECD)

155 To define the Secure Dynamic Messaging functionality of the TOE, an additional component FDP_ETC.3 of the family FDP_ETC (export from the TOE) of the class FDP (user data protection) is defined.

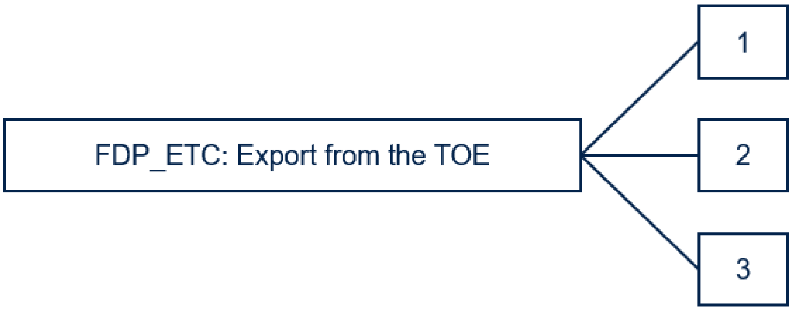
156 As defined in CC Part 2, the FDP class addresses user data protection. The FDP_ETC family defines functions for TSF-mediated exporting of user data from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. The extended component FDP_ETC.3 (Export of user data in unauthenticated state) addresses a similar concern but does not require a TOE enforcement of an access control SFP(s) and/or information flow control SFP(s) as the already defined component of the FDP_ETC family.

157 Note that the *BSI-CC-PP-0084-2014* Protection Profile defines extended security functional requirements FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1 and FDP_SDC.1 in chapter 5 which are included in this security target.

5.1 Export of user data in unauthenticated state (FDP_ETC.3)

158 The class and family behaviour of FDP_ETC are already defined in CC Part 2.

Figure 3. Component leveling of Extended Component FDP_ETC



FDP_ETC Export from the TOE

Management: FDP_ETC.3
There are no management activities foreseen.

Audit: FDP_ETC.3
There are no actions defined to be auditable.

FDP_ETC.3 **Export of user data in unauthenticated state**

Hierarchical to: No other components.

Dependencies No dependencies.

FDP_ETC.3.1 **The TSF shall export the following pieces of user data: [assignment: pieces of user data] with the following user data's associated security attributes: [assignment: list of security attributes].**

FDP_ETC.3.2 **The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.**

FDP_ETC.3.3 **The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: additional exportation control rules]**

159 The extended component is defined to capture the Secure Dynamic Messaging feature provided by the TOE, which allows for the encrypted and authenticated extraction of user data without the need of establishing a trusted channel beforehand. Due to this specific property, the existing data export SFRs FDP_ETC.1 and FDP_ETC.2 did not apply well.

6 Security requirements (ASE_REQ)

160 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 6.1*), a section on security assurance requirements (SARs) for the TOE (*Section 6.2*), a section on the refinements of these SARs (*Section 6.3*) as required by the "*BSI-CC-PP-0084-2014*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 6.4*).

6.1 Security functional requirements for the TOE

161 The selected security functional requirements (SFRs) for this TOE (MIFARE DESFire EV3 on ST31R480 A01) are summarized in *Table 7*.
This table also specifies:

- Their type i.e. drawn from *CCMB-2022-11-002 R1* or extended,
- Their origin i.e. defined in the *BSI-CC-PP-0084-2014* Protection Profile, in *[AUG]*, or in the Platform Security Target *[PF-ST]*. All SFRs are inherited from *[PF-ST]*, except those identified by “This ST”.

162 The extended SFRs are defined in the "*BSI-CC-PP-0084-2014*" Protection Profile and in *Section 5* of this Security Target.

163 All iterations, assignments, selections, or refinements on SFRs have been performed according to section 8.2 of *CCMB-2022-11-001 R1*. They are easily identified in the following text since they appear ***as indicated here***.

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-2022-11-002 R1*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality		
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-CC-PP-0084-2014* Operated	Extended

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

Label	Title	Addressing	Origin	Type
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing	BSI-CC-PP-0084-2014 Operated	CCMB-2022-11-002 R1
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 / PTG.2	Random number generation - PTG.2	Weak cryptographic quality of random numbers	BSI-CC-PP-0084-2014 Operated	
FCS_RNG.1 / PG	Random number generation			
FCS_RNG.1 / DRG.3	Random number generation - DRG.3			
FCS_COP.1	Cryptographic operation	TDES and AES Cipher scheme support	[AUG] #1 Operated / [PF-ST]	
FDP_ACC.2 / Memories	Complete access control	Memory access violation	[PF-ST]	
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		[PF-ST]	
FIA_API.1	Authentication Proof of Identity	Masquerade	BSI-CC-PP-0084-2014 Operated	
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality		
FMT_LIM.2 / Loader	Limited availability			

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

Label	Title	Addressing	Origin	Type
FTP_ITC.1 / Loader	Inter-TSF trusted channel - Loader	Loader violation	BSI-CC-PP-0084-2014 Operated	CCMB-2022-11-002 R1
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	[PF-ST]	
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
FTP_ITC.1 / Sdiag	Inter-TSF trusted channel - Secure Diagnostic	Abuse of Secure Diagnostic functionality	*[PF-ST]*	*CCMB-2022-11-002 R1*
FAU_SAR.1 / Sdiag	Audit review - Secure Diagnostic			
FMT_LIM.1 / Sdiag	Limited capabilities - Secure Diagnostic			
FMT_LIM.2 / Sdiag	Limited availability - Secure Diagnostic			
FMT_SMR.1 / MFDF	Security roles	MFDF access control	This ST	
FDP_ACC.1 / MFDF	Subset access control			
FDP_ACF.1 / MFDF	Security attribute based access control			
FMT_MSA.3 / MFDF	Static attribute initialisation			
FMT_MSA.1 / MFDF	Management of security attribute			
FMT_SMF.1 / MFDF	Specification of management functions			
FDP_ITC.2 / MFDF	Import of user data with security attributes			
FMT_MTD.1 / MFDF	Management of TSF data			

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

Label	Title	Addressing	Origin	Type
FIA_UID.2 / MFDF	User identification before any action	MFDF confidentiality, authentication and integrity	This ST	CCMB-2022-11-002 R1
FIA_UAU.2 / MFDF	User authentication before any action			
FIA_UAU.3 / MFDF	Unforgeable authentication			
FIA_UAU.5 / MFDF	Multiple authentication mechanisms			
FPT_TDC.1 / MFDF	Inter-TSF basic TSF data consistency			
FTP_TRP.1 / MFDF	Trusted path			
FCS_COP.1 / MFDF-DES	Cryptographic operation - MFDF-DES			
FCS_COP.1 / MFDF-AES	Cryptographic operation - MFDF-AES			
FCS_CKM.1 / MFDF	Cryptographic key generation			
FCS_CKM.6 / MFDF	Cryptographic key destruction			
FDP_ROL.1 / MFDF	Basic rollback	MFDF robustness		
FPT_RPL.1 / MFDF	Replay detection			
FPR_UNL.1 / MFDF	Unlinkability			
FRU_RSA.2 / MFDF	Minimum and maximum quotas	MFDF correct operation		
FDP_RIP.1 / MFDF	Subset residual information protection	MFDF intrinsic confidentiality and integrity		
FDP_ETC.3 / MFDF	Export of user data in unauthenticated state	MFDF Secure Dynamic Messaging		Extended

164 All these SFRs have already been stated in the *ST31R480 A01 Security Target for composition*, and are satisfied by the *ST31R480* platform, except the following ones, dedicated to MFDF: *FCS_RNG.1 / DRG.3*, *FMT_SMR.1 / MFDF*, *FDP_ACC.1 / MFDF*, *FDP_ACF.1 / MFDF*, *FMT_MSA.3 / MFDF*, *FMT_MSA.1 / MFDF*, *FMT_SMF.1 / MFDF*, *FDP_ITC.2 / MFDF*, *FMT_MTD.1 / MFDF*, *FIA_UID.2 / MFDF*, *FIA_UAU.2 / MFDF*, *FIA_UAU.3 / MFDF*, *FIA_UAU.5 / MFDF*, *FPT_TDC.1 / MFDF*, *FTP_TRP.1 / MFDF*, *FCS_COP.1 / MFDF-DES*, *FCS_COP.1 / MFDF-AES*, *FCS_CKM.1 / MFDF*, *FCS_CKM.6 /*

MFDF, *FDP_ROL.1 / MFDF*, *FPT_RPL.1 / MFDF*, *FPR_UNL.1 / MFDF*, *FRU_RSA.2 / MFDF*, *FDP_RIP.1 / MFDF*, *FDP_ETC.3 / MFDF*.

165 The SFRs from the Platform Security Target are detailed in the *ST31R480 A01 Security Target for composition [PF-ST]*.

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

6.1.1 Additional Security Functional Requirements regarding random number generation

Random number generation - Class DRG.3 (FCS_RNG.1 / DRG.3)

167 The TSF shall provide a ***deterministic*** random number generator that implements:

- ***(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 256 bit*s *of entropy.***
- ***(DRG.3.2) The RNG provides forward secrecy.***
- ***(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.***

168 The TSF shall provide ***random numbers*** that meet:

- ***(DRG.3.4) The RNG initialized with a random seed using a PTRNG of class PTG.2, generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least $1\text{-}2\text{-}^{24}$.***
- ***(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequence of an ideal RNG. The random numbers must pass test procedure A and no additional test suites.***

6.1.2 Additional Security Functional Requirements regarding access control

Security roles (FMT_SMR.1 / MFDF)

169 The TSF shall maintain the roles ***Admin, AppMgr, DelAppMgr, AppUser, AppChangeUser, AppRollUser, OrigKeyUser and Anybody***.

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

Subset access control (FDP_ACC.1 / MFDF)

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

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

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

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

- ***The Admin is allowed to perform Application.Create and Application.Delete.***
- ***The Admin is allowed to perform DelApplication.Delete.***
- ***The AppMgr is allowed to perform File.Create and File.Delete.***
- ***The DelAppMgr is allowed to perform DelApplication.Create with valid DAMMAC and valid DAMENC.***

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

- ***The AppMgr is allowed to perform Application.Delete if the attribute PICCLevelData.PICCKeySettings grants this right.***
- ***The AppUser is allowed to perform File.Read or File.Write or File.ReadWrite or File.Change on File if the File.AccessRights grant these rights.***
- ***The Anybody is allowed to perform Application.Create if the attribute PICCLevelData.PICCKeySettings grant this right.***
- ***The Anybody is allowed to perform File.Create and File.Delete if the Application.AppKeySettings grant these rights.***
- ***The Anybody is allowed to perform File.Read or File.Write or File.ReadWrite or File.Change on File if the File.AccessRights grant these rights.***

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

- ***No one but Nobody is allowed to perform File.Read or File.Write or File.ReadWrite or File.Change on File if the File.AccessRights do not grant this right.***
- ***OrigKeyUser is not allowed to perform any operation on objects.***
- ***No one but Nobody is allowed to perform any operation on OriginalityKey.***

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

177 *SFP_1: DESFire Access Control Policy*

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

The subjects are:

- *Admin: Administrator*
  The Admin is the subject that owns or has access to the PICCMasterKey.
  The Admin is the subject that distributes the PICCDAMAuthKey, DAMMACs, and DAMENCs containing the AppDAMDefaultKey, to the DelAppMgr.
- *AppMgr: Application Manager*
  The AppMgr is the subject that owns or has access to an AppMasterKey. Note that the TOE supports multiple Applications and therefore multiple AppMgr, however for one Application there is only one AppMgr.
- *DelAppMgr: Delegated Application Manager*
  The DelAppMgr is the subject that has access to a valid DAMMAC, the PICCDAMAuthKey, and a DAMENC containing the AppDAMDefaultKey. Note that the TOE supports multiple DelApplications and therefore multiple DelAppMgr.
- *AppUser: Application User*
  The AppUser is the subject that owns or has access to an AppKey. Note that the TOE

supports multiple AppUser within each Application and the assigned rights to the AppUser can be different, which allows to have more or less powerful AppUser.

- *AppChangeUser: Application Change User*
  The AppChangeUser is the subject that owns or has access to an AppChangeKey.
- *AppRollUser: Application Roll Key Set User*
  The AppRollUser is the subject that owns or has access to an AppRollKey.
- *OrigKeyUser: Originality Key User*
  The OrigKeyUser is the subject that owns or has access to an OriginalityKey. The OrigKeyUser can authenticate with the TOE to prove the authenticity of the Security IC.
- *Anybody: Anybody*
  Any subject that does not belong to one of the roles Admin, AppMgr, DelAppMgr, AppUser, AppChangeUser, AppRollUser or OrigKeyUser 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 Admin, AppMgr, DelAppMgr, AppUser, AppChangeUser, AppRollUser, OrigKeyUser 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.

The objects are:

- *PICCLevelData: PICC Level Data*
  The PICC level is the lowest level of the MFDF Software (PICC level, Application level, File level). On the PICC level Application and DelApplication can be created or deleted. Hence to the PICCLevelData belong Application and DelApplication.
- *Application: Application*
  The card can store a number of Application. An Application can store a number of File.
- *DelApplication: Delegated Application*
  The card can store a number of DelApplication. After creation the DelApplication has the same attributes as an Application.
- *File: File*
  An Application can store a number of File of different types.
- *PICCMasterKey: PICC Master Key*
  The Card Master Key.

- *PICCAppDefaultKey: PICC Application Default Key*
  The Default Application Master Key and Application Keys that are used when an Application is created and when a KeySet is initialized.
- *PICCDAMAuthKey: PICC DAM Authentication Key*
  Delegated Application Management Authentication Key
- *PICCDAMENCKey: PICC DAM Encryption Key*
  Delegated Application Management Encryption Key to generate DAMENC.
- *PICCDAMMACKey: PICC DAM MAC Key*
  Delegated Application Management MAC Key to generate DAMMAC.
- *OriginalityKey: Originality Key*
  Key to check the originality of the card.
- *AppMasterKey: Application Master Key*
  Application Master Key.
- *AppChangeKey: Application Change Key*
  Application Change Key.
- *AppKey: Application Key*
  Application Key.
- *AppTransactionMACKey: Application Transaction MAC Key*
  Application Transaction MAC Key.
- *AppRollKey: Application Roll Keyset Key*
  Application Roll Key Set Key.
- *AppDAMDefaultKey: Application DAM Default Key*
  Delegated Application Management Default Authentication Key.
- *KeySet: Key Set*
  AppKeys are grouped into KeySets.

The security attributes are:

- *PICCLevelData.PICCKeySettings: Generic PICC key settings.*
- *Application.AppKeySettings: Generic Application key settings.*
- *File.AccessRights:Generic access rights for File.*

The operations that can be performed with the objects are:

- *PICCLevelData.Modify: Modify attribute PICCLevelData.PICCKeySettings.*
- *PICCLevelData.Freeze: Freeze attribute PICCLevelData.PICCKeySettings.*
- *Application.Modify: Modify attribute Application.AppKeySettings.*
- *Application.Freeze: Freeze attribute Application.AppKeySettings.*
- *Application.Create: Create an Application.*
- *Application.Delete: Delete an Application.*
- *Application.Select: Select an Application.*
- *DelApplication.Create: Create a DelApplication.*
- *DelApplication.Delete: Delete a DelApplication.*
- *File.Create: Create a File.*
- *File.Delete: Delete a File.*
- *File.Freeze: Freeze attributes of File.*
- *File.Read: Read operations accessing the content of a File.*
- *File.Write: Write operations accessing the content of a File.*
- *File.ReadWrite: ReadWrite operations accessing the content of a File.*
- *File.Change: Change operation to change the attribute File.AccessRights.*
- *PICCMasterKey.Change: Change the PICCMasterKey.*
- *PICCMasterKey.Freeze: Freeze the PICCMasterKey.*
- *PICCAppDefaultKey.Change: Change the PICCAppDefaultKey.*
- *PICCDAMAuthKey.Change: Change the PICCDAMAuthKey.*
- *PICCDAMENCKey.Change: Change the PICCDAMENCKey.*
- *PICCDAMMACKey.Change: Change the PICCDAMMACKey.*
- *AppMasterKey.Change: Change the AppMasterKey.*
- *AppMasterKey.Freeze: Freeze the AppMasterKey.*
- *AppChangeKey.Change: Change the AppChangeKey.*
- *AppKey.Change: Change the AppKey.*
- *AppTransactionMACKey.Create: Create the AppTransactionMACKey.*
- *AppTransactionMACKey.Delete: Delete the AppTransactionMACKey.*
- *AppRollKey.Change: Change the AppRollKey.*
- *KeySet.Roll: Roll the KeySet.*

Note that subjects are authorised by cryptographic keys. These keys are considered as authentication data and not as security attributes of the subjects. The card has a card master key PICCMasterKey. Every application has an AppMasterKey and a variable number of AppKeys organized in KeySet used for operations on Files (all these keys are called Application Keys). The Application Keys and Key Sets within an application are numbered.

Implications of the DESFire Access Control Policy:

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

- *The TOE end-user does normally not belong to the group of authorised users (Admin, AppMgr, DelAppMgr, AppUser), but 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 Admin can have the exclusive right to create and delete Applications on the Card, however he can also grant this privilege to Anybody. In the case of DelApplications the Admin can grant this privilege to the AppMgr. Additionally, changing the PICCLevelData is reserved for the Admin. AppKeys, at delivery time should be personalized to a preliminary, temporary key only known to the Admin and the AppMgr.*
- *At Application personalization time, the AppMgr uses the preliminary AppKey in order to personalize the AppKeys, whereas all keys, except the AppMasterKey, can be personalized to a preliminary, temporary key only known to the AppMgr and the AppUser. Furthermore, the AppMgr has the right to create Files within his Application scope.*

Static attribute initialisation (FMT_MSA.3 / MFDF)

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

179 The TSF shall allow the ***no one but Nobody*** to specify alternative initial values to override the default values when an object or information is created.

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

Management of security attributes (FMT_MSA.1 / MFDF)

181 The TSF shall enforce the ***DESFire Access Control Policy*** to restrict the ability to ***modify or freeze and change*** the security attributes ***of the objects PICCLevelData, Application and the security attribute File.AccessRights*** to the ***Admin, AppMgr and AppChangeUser respectively***.

182 ***Refinement:***

The detailed management abilities are:

- ***Only the Admin is allowed to perform PICCLevelData.Modify or PICCLevelData.Freeze on PICCLevelData.PICCKeySettings.***
- ***Only the AppMgr is allowed to perform Application.Modify or Application.Freeze on Application.AppKeySettings.***
- ***The AppChangeUser is allowed to perform File.Freeze on File.AccessRights.***

Specification of Management Functions (FMT_SMF.1 / MFDF)

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

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

Starting a new authentication, Rolling key set, Failed Proximity Check, Deleting an Application as AppMgr, Reset,

- ***Changing a security attribute,***
- ***Rolling the key set,***
- ***Creating or deleting an application, a delegated application or a file,***
- ***Selection of the Virtual Card.***

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

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

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

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

187 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.

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

Management of TSF data (FMT_MTD.1 / MFDF)

189 The TSF shall restrict the ability to ***perform the operations PICCMasterKey.Change, PICCMasterKey.Freeze, PICCAppDefaultKey.Change, AppMasterKey.Change, AppMasterKey.Freeze, AppChangeKey.Change*** to ***the Admin, AppMgr and AppUser***.

190 ***Refinement:***

The detailed management abilities are:

- ***Only the Admin is allowed to perform PICCMasterKey.Change or PICCMasterKey.Freeze.***
- ***The Admin is allowed to perform PICCAppDefaultKey.Change.***
- ***The Admin is allowed to perform PICCDAMAuthKey.Change.***
- ***The Admin is allowed to perform PICCDAMENCKey.Change.***
- ***The Admin is allowed to perform PICCDAMMACKey.Change.***
- ***The AppMgr is allowed to perform AppMasterKey.Change and AppMasterKey.Freeze.***
- ***The AppMgr is allowed to perform AppChangeKey.Change.***
- ***The AppMgr is allowed to perform AppKey.Change.***
- ***The AppMgr is allowed to perform AppRollKey.Change.***
- ***The AppMgr is allowed to perform AppTransactionMACKey.Create and AppTransactionMACKey.Delete.***
- ***The AppChangeUser is allowed to perform AppChangeKey.Change.***
- ***The AppChangeUser is allowed to perform AppKey.Change.***
- ***The AppUser is allowed to perform AppKey.Change on AppKey if Application.AppKeySettings grant this right.***
- ***The AppUser is allowed to perform AppTransactionMACKey.Create and AppTransactionMACKey.Delete on AppTransactionMACKey if Application.AppKeySettings grant this right.***
- ***The AppRollUser is allowed to perform KeySet.Roll.***

6.1.3 Additional Security Functional Requirements regarding confidentiality, authentication and integrity

Cryptographic operation (FCS_COP.1 / MFDF-DES)

191 The TSF shall perform ***encryption and decryption used for authentication*** in accordance with the specified algorithm ***Triple-DES in one of the following modes of operation: CBC and 3-key Triple-DES*** and cryptographic key sizes ***168 bit***s that meet the following standards: *NIST SP 800-67* ***(TDES),*** *NIST SP 800-38A* ***(CBC mode)***.

Cryptographic operation (FCS_COP.1 / MFDF-AES)

The TSF shall perform ***encryption and decryption and cipher based MAC for authentication and communication*** in accordance with the specified algorithm ***Advanced Encryption Standard (AES) in one of the following modes of operation: CBC, CMAC*** and cryptographic key sizes ***128 bits*** that meet the following standards: *FIPS 197* ***(AES),*** *NIST SP 800-38A* ***(CBC mode),*** *NIST SP 800-38B* ***(CMAC mode)***.

192 ***Refinement:***

For the MIFARE DESFire EV1 secure messaging, the TOE uses the cryptographic algorithm for CMAC according to *NIST SP 800-38B* ***(CMAC mode) with the following modification: the TOE does not use the standard zero byte IV, instead it uses an IV defined by the previous cryptographic operation (chaining mode).***

Cryptographic key generation (FCS_CKM.1 / MFDF)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***EV1 Session Key Generation (for AES) and EV2 Session Key Generation and specified cryptographic key sizes 128 bits*** that meets the following: *MIFARE DESFire EV3 interface specification - Technical note*, Section 4.9.5 (EV1) and Section 4.10.7 (EV2).

Timing and event of cryptographic key destruction (FCS_CKM.6 / MFDF)

193 The TSF shall destroy:

- (FCS_CKM.6.1 / MFDF) Cryptographic keys used in MFDF in volatile RAM when no longer needed or under any attack detected by the TOE.
- (FCS_CKM.6.2 / MFDF) Cryptographic keys and keying material specified by FCS_CKM.6.1 / MFDF in accordance with a specified cryptographic key destruction method ***overwriting*** that meets the following: ***none***.

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

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

Application note:
Identification of a user is performed upon an authentication request based on the currently selected context and the key number. For example, if an authentication request for key number 0 is issued after selecting a specific application, the user is identified as the Application Manager of the respective application. Before any authentication request is issued, the user is identified as “Everybody”.

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

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

Unforgeable authentication (FIA_UAU.3 / MFDF)

196 The TSF shall ***detect and prevent*** use of authentication data that has been forged by any user of the TSF.

197 The TSF shall ***detect and prevent*** use of authentication data that has been copied from any other user of the TSF.

Multiple authentication mechanisms (FIA_UAU.5 / MFDF)

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

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

- ***The ‘none’ authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The ‘none’ authentication implicitly and solely authorises the “Everybody” subject.***
- ***The cryptographic authentication is used to authorise the Administrator, Application Manager, Delegated Application Manager and Application User.***

Trusted path (FTP_TRP.1 / MFDF)

200 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, disclosure or only modification***.

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

202 The TSF shall require the use of the trusted path for ***authentication requests with 3-key Triple-DES or AES, confidentiality and/or integrity verification for data transfers protected with AES based on a setting in the file attributes***.

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

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

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

6.1.4 Additional Security Functional Requirements regarding the robustness and correct operation

Basic rollback (FDP_ROL.1/ MFDF)

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

206 The TSF shall permit operations to be rolled back within the ***scope of the current transaction, which is defined by the following limitative events: chip reset, select command, deselect command, explicit commit, explicit abort, command failure***.

Replay detection (FPT_RPL.1 / MFDF)

207 The TSF shall detect replay for the following entities: ***authentication requests with 3-key Tripe-DES or AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes***.

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

Unlinkability (FPR_UNL.1 / MFDF)

209 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 / MFDF)

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

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

Subset residual information protection (FDP_RIP.1 / MFDF)

212 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: ***MFDF***.

Additional Security Functional Requirements regarding the secure dynamic messaging

Export of user data in unauthenticated state (FDP_ETC.3 / MFDF)

213 The TSF shall export the following pieces of user data: ***a configurable subset of file data*** with the following user data's associated security attributes: ***confidentiality, authenticity and replay protection for the configurable subset of the file data.***

214 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

215 The TSF shall enforce the following rules when user data is exported from the TOE: ***plain export of file data in case that SDM is not activated for the file.***

6.2 TOE security assurance requirements

216 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level ***5*** (EAL5) and augmented by taking the following components:

- ALC_DVS.2,
- AVA_VAN.5,
- ***ASE_TSS.2,***
- ***ALC_FLR.2,***
- ***the composite product package (COMP)***

217 Regarding application note 22 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.

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

219 The component ALC_FLR.2 is chosen as an augmentation in this ST because a solid flaw management is key for the continuous improvement of the security IC platforms, especially on markets which need highly resistant and long lasting products.

220 The composite product package (COMP) is chosen as an augmentation in this ST to provide assurance that the MIFARE DESFire EV3 on ST31R480 A01 has been assembled and evaluated according to the relevant criteria defined in *CCMB-2022-11-005 R1*.

221 The set of security assurance requirements (SARs) is presented in *Table 8*, indicating the origin of the requirement.

Table 8. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
ADV_COMP.1	Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority	*CCMB-2022-11-005 R1*
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_COMP.1	Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures	*CCMB-2022-11-005 R1*
ALC_DEL.1	Delivery procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	*BSI-CC-PP-0084-2014*
ALC_FLR.2	Flaw reporting procedures	Security Target
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
ASE_COMP.1	Consistency of Security Target	*CCMB-2022-11-005 R1*
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*

Table 8. TOE security assurance requirements (continued)

Label	Title	Origin
ATE_COMP.1	Composite product functional testing	*CCMB-2022-11-005 R1*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-CC-PP-0084-2014*
AVA_COMP.1	Composite product vulnerability assessment	*CCMB-2022-11-005 R1*

6.3 Refinement of the security assurance requirements

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

223 Regarding application note 23 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.

224 An impact summary is provided in *Table 9*.

Table 9. 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_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	None, presentation style changes
ADV_IMP	1	1	None
ATE_COV	2	2	None
AGD_OPE	1	1	None
AVA_VAN	5	5	None

6.4 Security Requirements rationale

6.4.1 Rationale for the Security Functional Requirements

225 Just as for the security objectives rationale of *Section* , 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 introduced in the Platform Security Target *[PF-ST]*, and 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 10. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Inherent	*Basic internal transfer protection FDP_ITT.1* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.Phys-Probing	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*
BSI.O.Malfunction	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.Phys-Manipulation	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* *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 - PTG.2 FCS_RNG.1 / PTG.2* *Random number generation FCS_RNG.1 / PG* *Random number generation - DRG.3 FCS_RNG.1 / DRG.3* 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

Table 10. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
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*
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*
JIL.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*

Table 10. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
JIL.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*
JIL.O.Secure-AC-Activation	*"Failure with preservation of secure state - Loader" FPT_FLS.1 / Loader*
JIL.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*

Table 10. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
AUG4.O.Mem-Access	“*Complete access control FDP_ACC.2 / Memories* “*Security attribute based access control*” *FDP_ACF.1 / Memories* “*Static attribute initialisation*” *FMT_MSA.3 / Memories* “*Management of security attribute*” *FMT_MSA.1 / Memories* “*Specification of management functions*” *FMT_SMF.1 / Memories*
MFDF.O.Access-Control	“*Cryptographic key destruction*” *FCS_CKM.6 / MFDF* “*Subset access control*” *FDP_ACC.1 / MFDF* “*Security attribute based access control*” *FDP_ACF.1 / MFDF* “*Import of user data with security attributes*” *FDP_ITC.2 / MFDF* “*Management of security attribute*” *FMT_MSA.1 / MFDF* “*Static attribute initialisation*” *FMT_MSA.3 / MFDF* “*Inter-TSF basic TSF data consistency*“ *FMT_MTD.1 / MFDF* “*Specification of management functions*” *FMT_SMF.1 / MFDF* “*Security roles*” *FMT_SMR.1 / MFDF*
MFDF.O.Authentication	“*Cryptographic operation - MFDF-DES*” *FCS_COP.1 / MFDF-DES* “*Cryptographic operation - MFDF-AES*” *FCS_COP.1 / MFDF-AES* “*Cryptographic key generation*” *FCS_CKM.1 / MFDF* “*User identification before any action*” *FIA_UID.2 / MFDF* “*User authentication before any action*” *FIA_UAU.2 / MFDF* “*Unforgeable authentication*” *FIA_UAU.3 / MFDF* “*Multiple authentication mechanisms*” *FIA_UAU.5 / MFDF* “*Specification of management functions*” *FMT_SMF.1 / MFDF* “*Replay detection*” *FPT_RPL.1 / MFDF* “*Trusted path*” *FTP_TRP.1 / MFDF*
MFDF.O.Encryption	“*Cryptographic key generation*” *FCS_CKM.1 / MFDF* “*Cryptographic key destruction*” *FCS_CKM.6 / MFDF* “*Cryptographic operation - MFDF-AES*” *FCS_COP.1 / MFDF-AES* “*Trusted path*” *FTP_TRP.1 / MFDF* “*Export of user data in unauthenticated state*” *FDP_ETC.3 / MFDF*
MFDF.O.MAC	“*Cryptographic key generation*” *FCS_CKM.1 / MFDF* “*Cryptographic key destruction*” *FCS_CKM.6 / MFDF* “*Cryptographic operation - MFDF-AES*” *FCS_COP.1 / MFDF-AES* “*Replay detection*” *FPT_RPL.1 / MFDF* “*Trusted path*” *FTP_TRP.1 / MFDF* “*Export of user data in unauthenticated state*” *FDP_ETC.3 / MFDF*
MFDF.O.Type-Consistency	“*Inter-TSF basic TSF data consistency*” *FPT_TDC.1 / MFDF*
MFDF.O.Transaction	“*Basic rollback*” *FDP_ROL.1 / MFDF*
MFDF.O.No-Trace	“*Unlinkability*” *FPR_UNL.1 / MFDF*
MFDF.O.Resource	“*Export of user data in unauthenticated state*” *FRU_RSA.2 / MFDF*

Table 10. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
MFDF.O.Verification	“*Failure with preservation of secure state*” *FPT_FLS.1* “*Complete access control*” *FDP_ACC.2 / Memories* “*Security attribute based access control*” *FDP_ACF.1 / Memories* “*Static attribute initialisation*” *FMT_MSA.3 / Memories*
O. Firewall	“*Complete access control FDP_ACC.2 / Memories* “*Security attribute based access control*” *FDP_ACF.1 / Memories* “*Static attribute initialisation*” *FMT_MSA.3 / Memories* “*Management of security attribute*” *FMT_MSA.1 / Memories* “*Specification of management functions*” *FMT_SMF.1 / Memories*
MFDF.O.Shr-Res	“*Subset residual information protection*” *FDP_RIP.1 / MFDF*
MFDF.OE.Secure-Values	Not applicable
MFDF.OE.Terminal-Support	Not applicable

226 All justifications for Security Objectives and SFRs have been already provided in the Platform Security Target *[PF-ST]*, except for *MFDF.O.Access-Control*, *MFDF.O.Authentication*, *MFDF.O.Encryption*, *MFDF.O.MAC*, *MFDF.O.Type-Consistency*, *MFDF.O.Transaction*, *MFDF.O.No-Trace*, *MFDF.O.Resource*, *MFDF.O.Verification*, and *MFDF.O.Shr-Res* and their associated SFRs.

227 This rationale must show that security requirements suitably address these objectives.

228 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* and in *[PF-ST]*, they form an internally consistent whole, is provided in the next subsections.

6.4.2 Additional security objectives are suitably addressed

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

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

230 The security functional requirement "*Security roles (FMT_SMR.1 / MFDF)*" defines the roles of the DESFire Access Control Policy.
The security functional requirements "*Subset access control (FDP_ACC.1 / MFDF)*" and "*Security attribute based access control (FDP_ACF.1 / MFDF)*" define the rules and "*Static attribute initialisation (FMT_MSA.3 / MFDF)*" and "*Management of security attributes (FMT_MSA.1 / MFDF)*" the attributes that the access control is based on.
The security functional requirement "*Management of TSF data (FMT_MTD.1 / MFDF)*" provides the rules for the management of the authentication data.
The management functions are defined by "*Specification of Management Functions (FMT_SMF.1 / MFDF)*".
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 / MFDF)*".
Since cryptographic keys are used for authentication (refer to *MFDF.O.Authentication*), these keys have to be removed if they are no longer needed for the access control (i.e. an

application is deleted). This is required by "*Timing and event of cryptographic key destruction (FCS_CKM.6 / MFDF)*".
These nine SFRs together provide an access control mechanism as required by the objective *MFDF.O.Access-Control*.

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

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

232 The two security functional requirements "*Cryptographic operation - MFDF-DES*" and "*Cryptographic operation - MFDF-AES*" require that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication.
The security functional requirements "*User identification before any action (FIA_UID.2 / MFDF)*", "*User authentication before any action (FIA_UAU.2 / MFDF)*" and "*Multiple authentication mechanisms (FIA_UAU.5 / MFDF)*" together define that users must be identified and authenticated before any action. The SFR "*Unforgeable authentication (FIA_UAU.3 / MFDF)*" prevents that forged authentication data can be used. The ‘none’ authentication of "*Multiple authentication mechanisms (FIA_UAU.5 / MFDF)*" also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE.
"*Specification of Management Functions (FMT_SMF.1 / MFDF)*" defines security management functions the TSF shall be capable to perform.
"*Trusted path (FTP_TRP.1 / MFDF)*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 / MFDF especially requires “authentication requests”. Together with "*Replay detection (FPT_RPL.1 / MFDF)*" which requires a replay detection for these authentication requests, the eight security functional requirements fulfil the objective *MFDF.O.Authentication*.

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

233 The justification related to the security objective “MFDF Confidential communication (*MFDF.O.Encryption*)” is as follows:

234 The security functional requirement "*Cryptographic operation - MFDF-AES*" requires that the TOE provides the basic cryptographic algorithm AES that can be used to protect the communication by encryption.
"*Trusted path (FTP_TRP.1 / MFDF)*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 / MFDF especially requires “confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes”.
"*Cryptographic key generation (FCS_CKM.1 / MFDF)*" generates the session key used for encryption.
"*Timing and event of cryptographic key destruction (FCS_CKM.6 / MFDF)*" requires that cryptographic keys used for encryption have to be removed after usage.
The TOE also provides Secure Dynamic Messaging service which allows encrypted and MACed data read without being in the authenticated state.”*Export of user data in unauthenticated state (FDP_ETC.3 / MFDF)*" requires user data export in unauthenticated state, and hence models the requirements to reach the objective *MFDF.O.Encryption.*

Security objective “MFDF Integrity-protected Communication (*MFDF.O.MAC*)”

235 The justification related to the security objective “MFDF Integrity-protected Communication (*MFDF.O.MAC*)” is as follows:

236 The security functional requirement "*Cryptographic operation - MFDF-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 / MFDF)*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 / MFDF especially requires “confidentiality and/or data integrity verification for data transfers on request of the file owner”.
"*Cryptographic key generation (FCS_CKM.1 / MFDF)*" generates the session key used for encryption.
"*Timing and event of cryptographic key destruction (FCS_CKM.6 / MFDF)*" requires that cryptographic keys used for MAC operations have to be removed after usage.
"*Replay detection (FPT_RPL.1 / MFDF)*" requires a replay detection for these data transfers.
The TOE also provides Secure Dynamic Messaging service which allows encrypted and MACed data read without being in the authenticated state.”*Export of user data in unauthenticated state (FDP_ETC.3 / MFDF)*" requires user data export in unauthenticated state, and hence models the requirements to reach the objective *MFDF.O.MAC*.

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

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

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

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

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

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

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

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

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

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

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

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

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

245 The justification related to the security objective “MFDF code integrity check *MFDF.O.Verification*)” is as follows:

246 The security functional requirements "*Complete access control FDP_ACC.2 / Memories* " and "*Security attribute based access control FDP_ACF.1 / Memories*", supported by "*Static attribute initialisation FMT_MSA.3 / Memories*", ensure that MFDF code integrity is protected. In addition, the security functional requirement "*Failure with preservation of secure state FPT_FLS.1*" ensures that in case of error on NVM, MFDF execution is stopped. This meets the objective *MFDF.O.Verification*.

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

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

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

6.4.3 Additional security requirements are consistent

"Security roles (*FMT_SMR.1 / MFDF*),
Subset access control (*FDP_ACC.1 / MFDF*),
Security attribute based access control (*FDP_ACF.1 / MFDF*),
Static attribute initialisation (*FMT_MSA.3 / MFDF*),
Management of security attributes (*FMT_MSA.1 / MFDF*),
Specification of TSF data (*FMT_MTD.1 / MFDF*)
Specification of management function (*FMT_SMF.1 / MFDF*)
Import of user data with security attributes (*FDP_ITC.2 / MFDF*)”

249 These security requirements have already been argued in *Section : Security objective “Access control for MFDF (MFDF.O.Access-Control)”* above.

"Cryptographic operation - MDF-DES (*FCS_COP.1 / MFDF-DES*),
Cryptographic operation - MDF-AES (*FCS_COP.1 / MFDF-AES*)
User identification before any action (*FIA_UID.2 / MFDF*),
User authentication before any action (*FIA_UAU.2 / MFDF*),
Unforgeable authentication (*FIA_UAU.3 / MFDF*),
Multiple authentication mechanisms (*FIA_UAU.5 / MFDF*);

250 These security requirements have already been argued in *Section : Security objective “Authentication for MFDF (MFDF.O.Authentication)”* above.

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

251 These security requirements have already been argued in *Section : Security objective “MFDF Integrity-protected Communication (MFDF.O.MAC)”* above.

"Inter-TSF basic TSF data consistency (*FPT_TDC.1 / MFDF*)
Cryptographic key generation (*FCS_CKM.1 / MFDF*)
Timing and event of cryptographic key destruction (*FCS_CKM.6 / MFDF*)
Export of user data in unauthenticated state(*FDP_ETC.3 / MFDF*)"

252 This security requirement has already been argued in *Section : Security objective "MFDF Confidential Communication (MFDF.O.Encryption)"* above.

"Basic rollback (*FDP_ROL.1 / MFDF*)"

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

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

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

"Minimum and maximum quotas (*FRU_RSA.2 / MFDF*)"

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

"Subset residual information protection (*FDP_RIP.1 / MFDF*)"

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

6.4.4 Dependencies of Security Functional Requirements

257 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 justified in the *ST31R480 A01 Security Target for composition [PF-ST]* security requirements rationale,
- those justified in *[AUG]* security requirements rationale.

258 Details are provided in *Table 11* below.

259 Note that in order to avoid repetitions of the SFRs iterated in this Security Target, and improve readability, some are mentioned in a generic form in this table.

Table 11. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* 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*

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
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, by FDP_ACC.1 / Memories and FDP_IFC.1	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 / PTG.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PG	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / DRG.3	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, or FCS_CKM.5]	No, see *[PF-ST]*	***No,*** *CCMB-2022-11-002 R1*
	FCS_CKM.6	No, see *[PF-ST]*	
FDP_ACC.2 / Memories	FDP_ACF.1 / Memories	Yes	Yes, *[PF-ST]*
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes, by FDP_ACC.1 / Memories	Yes, *[PF-ST]*
	FMT_MSA.3 / Memories	Yes	
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No, see *[AUG]* ***#4***	

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FMT_MSA.1 / Memories	[FDP_ACC.1 / Memories or FDP_IFC.1]	Yes, by FDP_ACC.1 / Memories and FDP_IFC.1	Yes, *[PF-ST]*
	FMT_SMF.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No	Yes, *[PF-ST]*
FMT_SMF.1 / Memories	None	No dependency	Yes, *[PF-ST]*
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	
FDP_UIT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Loader	Yes	

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	Yes, *[PF-ST]*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FIA_UID.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FIA_UAU.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_SMF.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FPT_FLS.1 / Loader	None	No dependency	Yes, *[PF-ST]*
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 *[PF-ST]*	Yes, *[PF-ST]*
FTP_ITC.1 / Sdiag	None	No dependency	Yes, *[PF-ST]*
FAU_SAR.1 / Sdiag	FAU_GEN.1	No, see *[PF-ST]*	Yes, *[PF-ST]*
FMT_SMR.1 / MFDF	FIA_UID.1 / MFDF	Yes, by FIA_UID.2 / MFDF	***No,*** *CCMB-2022-11-002 R1*
FDP_ACC.1 / MFDF	FDP_ACF.1 / MFDF	Yes	***No,*** *CCMB-2022-11-002 R1*
FDP_ACF.1 / MFDF	FDP_ACC.1 / MFDF	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_MSA.3 / MFDF	Yes	
FMT_MSA.3 / MFDF	FMT_MSA.1 / MFDF	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_SMR.1 / MFDF	Yes	
FMT_MSA.1 / MFDF	[FDP_ACC.1 / MFDF or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFDF	***No,*** *CCMB-2022-11-002 R1*
	FMT_SMF.1 / MFDF	Yes	
	FMT_SMR.1 / MFDF	Yes	
FMT_SMF.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FDP_ITC.2 / MFDF	[FDP_ACC.1 / MFDF or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFDF	***No,*** *CCMB-2022-11-002 R1*
	[FTP_ITC.1 or FTP_TRP.1 / MFDF]	Yes, by FTP_TRP.1 / MFDF	
	FPT_TDC.1 / MFDF	Yes	
FMT_MTD.1 / MFDF	FMT_SMR.1 / MFDF	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_SMF.1 / MFDF	Yes	
FIA_UID.2 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FIA_UAU.2 / MFDF	FIA_UID.1	Yes, by FIA_UID.2 / MFDF	***No,*** *CCMB-2022-11-002 R1*
FIA_UAU.3 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FIA_UAU.5 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FPT_TDC.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FTP_TRP.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FCS_COP.1/MFDF-DES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, or FCS_CKM.5]	Yes, by FCS_ITC.2 / MFDF, FCS_CKM.1 / MFDF	***No,*** *CCMB-2022-11-002 R1*
	FCS_CKM.6	Yes, by FCS_CKM.6 / MFDF	
FCS_COP.1/MFDF-AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, or FCS_CKM.5]	Yes, by FCS_ITC.2 / MFDF, FCS_CKM.1 / MFDF	***No,*** *CCMB-2022-11-002 R1*
	FCS_CKM.6	Yes, by FCS_CKM.6 / MFDF	
FCS_CKM.1 / MFDF	[FCS_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.1 / MFDF-DES, FCS_COP.1 / MFDF-AES	***No,*** *CCMB-2022-11-002 R1*
	FCS_CKM.6	Yes, by FCS_CKM.6 / MFDF	
FCS_CKM.6 / MFDF	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FDP_ITC.2 / MFDF	***No,*** *CCMB-2022-11-002 R1*

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FDP_ROL.1 / MFDF	[FDP_ACC.1 / or FDP_IFC.1]	Yes, by FDP_ACC.1 / MFDF	***No,*** *CCMB-2022-11-002 R1*
FPT_RPL.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FPR_UNL.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FRU_RSA.2 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FDP_RIP.1 / MFDF	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FDP_ETC.3 / MFDF	None	No dependency	No, extended component defined in this ST

6.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5

260 Regarding application note 22 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

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

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

263 Note that detailed and updated refinements for assurance requirements are given in *Section 6.3*.

264 The MIFARE DESFire EV3 on ST31R480 Security Target for composition claims conformance to Common Criteria 2022 revision 1 and strict conformance to the *BSI-CC-PP-0084-2014* Protection Profile. As the *BSI-CC-PP-0084-2014* claims conformance to Common Criteria version 3.1 it does not contain “Evaluation Methods / Evaluation Activities”. It explains there is no rationale in this Security Target for the disposition of such “Evaluation Methods / Evaluation Activities” for the extended security assurance requirements.

Dependencies of assurance requirements

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

266 The augmentation to this package identified in *Section 6.2* 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*,
- ALC_FLR.2 has no dependency.
- ASE_COMP.1 has no dependency,
- ALC_COMP.1 has no dependency,
- ADV_COMP.1 has no dependency,
- ATE_COMP.1 has no dependency,
- AVA_COMP.1 has no dependency.

7 TOE summary specification (ASE_TSS)

267 This section demonstrates how the TOE meets each Security Functional Requirement, and includes a statement of compatibility vs. the Platform Security Target *[PF-ST]*. More detail can be found in the ADV_FSP and ADV_ARC documents.

7.1 TOE Security Functional Requirements realisation

268 This section argues how the TOE meets each SFR.

269 The TOE is evaluated as a composite TOE, made of the underlying hardware platform and the MIFARE DESFire EV3 library on top of it.

270 Consequently, the *ST31R480 A01 Security Target for composition* details how all the platform SFRs are met, and in the following only the SFRs related to MFDF are addressed.

7.1.1 Random number generation - Class DRG.3 (FCS_RNG.1 / DRG.3)

The TSF provides deterministic random numbers that can be qualified with the test metrics required by the AIS20/31 standard for a DRG.3 class device.

7.1.2 Security roles (FMT_SMR.1 / MFDF)

271 MFDF supports the assignment of roles to users through the assignment of different keys for the different roles and through the structure and configuration of the access rights. This allows to distinguish between the roles of Admin, AppMgr, DelAppMgr, AppUser, AppChangeUser, AppRollUser and OrigKeyUser.

7.1.3 Subset access control (FDP_ACC.1 / MFDF)

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

7.1.4 Security attribute based access control (FDP_ACF.1 / MFDF)

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

7.1.5 Static attribute initialisation (FMT_MSA.3 / MFDF)

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

7.1.6 Management of security attributes (FMT_MSA.1 / MFDF)

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

7.1.7 Specification of Management Functions (FMT_SMF.1 / MFDF)

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

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

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

7.1.9 Management of TSF data (FMT_MTD.1 / MFDF)

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

7.1.10 Cryptographic operation (FCS_COP.1 / MFDF-DES)

279 The MFDF library uses Triple DES as cryptographic operation (EDES+ accelerator), to perform encryption and decryption used for authentication in accordance with *NIST SP 800-67* and *NIST SP 800-38A*, in one of the following modes of operation: CBC and 3-key Triple-DES with a cryptographic key size of 168 bits.

7.1.11 Cryptographic operation (FCS_COP.1 / MFDF-AES)

280 The MFDF library uses AES as cryptographic operation (AES accelerator), to perform encryption and decryption and cipher based MAC for authentication and communication in accordance with *FIPS 197, NIST SP 800-38A* and *NIST SP 800-38B*, in one of the following modes of operation: CBC, CMAC with a cryptographic key size of 128 bits.

281 Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

7.1.12 Cryptographic key generation (FCS_CKM.1 / MFDF)

282 The MFDF library generates cryptographic keys with the generation algorithm EV1 Session Key Generation (for AES) and EV2 Session Key Generation and specified cryptographic key sizes 128 bits that meets the following: *MIFARE DESFire EV3 interface specification - Technical note*, Section 4.9.5 (EV1) and Section 4.10.7 (EV2).

7.1.13 Timing and event of cryptographic key destruction (FCS_CKM.6 / MFDF)

283 The MFDF library erases key values from memory after their context becomes obsolete.

7.1.14 User identification before any action (FIA_UID.2 / MFDF)

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

7.1.15 User authentication before any action (FIA_UAU.2 / MFDF)

285 During the authentication, the MFDF library verifies that the user knows the selected key.

286 bAfter this authentication, both parties share a session key.

7.1.16 Unforgeable authentication (FIA_UAU.3 / MFDF)

287 The MFDF authentication commands (AuthenticateISO, AuthenticateEV2First, AuthenticateEV2NonFirst or the combination of ISOGetChallenge, ISOExternalAuthenticate and ISOInternalAuthenticate) make sure that the session authentication data cannot be reused or forged by using freshly generated session keys and random challenges.

7.1.17 Multiple authentication mechanisms (FIA_UAU.5 / MFDF)

288 The MFDF library implements the MFDF Interface Specification, that has a mechanism to authenticate Admin, AppMgr, DelAppMgr, AppUser, AppChangeUser, AppRollUser and OrigKeyUser, while Anybody is assumed when there is no valid authentication state.

289 Two types of authentication are supported: the native MFDF 3-pass authentication and the ISO authentication.

7.1.18 Inter-TSF basic TSF data consistency (FPT_TDC.1 / MFDF)

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

7.1.19 Trusted path (FTP_TRP.1 / MFDF)

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

7.1.20 Basic rollback (FDP_ROL.1 / MFDF)

292 The MFDF library implements the MFDF transaction mechanism ensuring that either all or none of the (modifying) file commands within a transaction are performed. If not, they are rolled back.

7.1.21 Replay detection (FPT_RPL.1 / MFDF)

293 The MFDF library implements the MFDF authentication command, and authenticated commands, that allow replay detection.

7.1.22 Unlinkability (FPR_UNL.1 / MFDF)

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

7.1.23 Minimum and maximum quotas (FRU_RSA.2 / MFDF)

295 The MFDF library ensures the memory required for its operation is available.

7.1.24 Subset residual information protection (FDP_RIP.1 / MFDF)

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

7.1.25 Export of user data in unauthenticated state (FDP_ETC.3 / MFDF)

297 The MFDF library implements Secure Dynamic Messaging as specified in *MIFARE DESFire EV3 interface specification - Technical note*.

7.2 Statement of compatibility

298 This section details the statement of compatibility between this Security Target and the Platform Security Target *[PF-ST]*.

299 The following mappings regarding SFRs, objectives and assurance requirements demonstrate that there is no inconsistency between this composite Security Target and the *ST31R480 A01 Security Target for composition*.

7.2.1 Compatibility of security objectives

300 There is no conflict between the security objectives of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 12. Platform Security Objectives vs. TOE Security Objectives

Platform Security Objectives	TOE Security Objectives
BSI.O.Leak-Inherent	*BSI.O.Leak-Inherent*
BSI.O.Phys-Probing	*BSI.O.Phys-Probing*
BSI.O.Malfunction	*BSI.O.Malfunction*
BSI.O.Phys-Manipulation	*BSI.O.Phys-Manipulation*
BSI.O.Leak-Forced	*BSI.O.Leak-Forced*
BSI.O.Abuse-Func	*BSI.O.Abuse-Func*
BSI.O.Identification	*BSI.O.Identification*
BSI.O.RND	*BSI.O.RND*
BSI.O.Authentication	*BSI.O.Authentication*
BSI.O.Cap-Avail-Loader	*BSI.O.Cap-Avail-Loader*
BSI.O.Ctrl-Auth-Loader	*BSI.O.Ctrl-Auth-Loader*
JIL.O.Prot-TSF-Confidentiality	*JIL.O.Prot-TSF-Confidentiality*
JIL.O.Secure-Load-ACode	*JIL.O.Secure-Load-ACode*
JIL.O.Secure-AC-Activation	*JIL.O.Secure-AC-Activation*
JIL.O.TOE-Identification	*JIL.O.TOE-Identification*
O.Secure-Load-AMemImage	*O.Secure-Load-AMemImage*
O.MemImage-Identification	*O.MemImage-Identification*

Table 12. Platform Security Objectives vs. TOE Security Objectives

Platform Security Objectives	TOE Security Objectives
AUG1.O.Add-Functions	*AUG1.O.Add-Functions* *MFDF.O.Authentication* *MFDF.O.Encryption* *MFDF.O.MAC*
AUG4.O.Mem-Access	*AUG4.O.Mem-Access* *O. Firewall* *MFDF.O.Verification*
O. Firewall	*O. Firewall*
	Additional objectives:
	MFDF.O.Access-Control
	MFDF.O.Type-Consistency
	MFDF.O.Transaction
	MFDF.O.No-Trace
	MFDF.O.Resource
	MFDF.O.Shr-Res

301 There is no conflict between the security objectives for the environment of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 13. Platform Security Objectives for the Environment vs. TOE Security Objectives for the Environment

Platform Security Objectives for the Environment	TOE Security Objectives for the Environment
BSI.OE.Resp-Appl	*BSI.OE.Resp-Appl*
BSI.OE.Process-Sec-IC	*BSI.OE.Process-Sec-IC*
BSI.OE.Lim-Block-Loader	*BSI.OE.Lim-Block-Loader*
BSI.OE.Loader-Usage	*BSI.OE.Loader-Usage*
BSI.OE.TOE-Auth	*BSI.OE.TOE-Auth*
OE.Enable-Disable-Secure-Diag	*OE.Enable-Disable-Secure-Diag*
OE.Secure-Diag-Usage	*OE.Secure-Diag-Usage*
OE.Composite-TOE-Id	*OE.Composite-TOE-Id*
OE.TOE-Id	*OE.TOE-Id*
	Additional objectives for the environment:
	MFDF.OE.Secure-Values
	MFDF.OE.Terminal-Support

7.2.2 Compatibility of Security Functional Requirements

302 All platform SFRs are relevant for this Composite ST.

303 The Composite ST SFRs do not show any conflict with the platform SFRs.

304 The following platform SFRs are used by this Composite ST because of their security properties providing protection against attacks to the TOE as a whole:

- FRU_FLT.2,
- FDP_SDC.1,
- FDP_SDI.2,
- FPT_PHP.3,
- FDP_ITT.1,
- FPT_ITT.1,
- FDP_IFC.1,

FPT_FLS.1 in order to generate a software reset,

FCS_RNG.1 for the provision of random numbers,

FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 for side-channel protection.

305 Complementary, the *Table 14* below shows the mapping between the Platform SFRs specifically used to implement a security service by SFRs of this Composite ST.

Table 14. Platform Security Functional Requirements vs. TOE Security Functional Requirements

Platform SFR	Composite ST SFRs
FRU_FLT.2	FRU_FLT.2
FPT_FLS.1	FPT_FLS.1
FMT_LIM.1 / Test	FMT_LIM.1 / Test
FMT_LIM.2 / Test	FMT_LIM.2 / Test
FAU_SAS.1	FAU_SAS.1
FDP_SDC.1	FDP_SDC.1
FDP_SDI.2	FDP_SDI.2
FPT_PHP.3	FPT_PHP.3
FDP_ITT.1	FDP_ITT.1
FPT_ITT.1	FPT_ITT.1
FDP_IFC.1	FDP_IFC.1
FCS_RNG.1 / PTG.2	FCS_RNG.1 / PTG.2 FCS_RNG.1 / DRG.3
FCS_RNG.1 / PG	FCS_RNG.1 / PG
FCS_COP.1 / TDES	FCS_COP.1 / TDES FCS_COP.1 / MFDF-DES
FCS_COP.1 / AES	FCS_COP.1 / AES FCS_COP.1 / MFDF-AES

Table 14. Platform Security Functional Requirements vs. TOE Security Functional Requirements (continued)

Platform SFR	Composite ST SFRs
FDP_ACC.2 / Memories	FDP_ACC.2 / Memories
FDP_ACF.1 / Memories	FDP_ACF.1 / Memories
FMT_MSA.3 / Memories	FMT_MSA.3 / Memories
FMT_MSA.1 / Memories	FMT_MSA.1 / Memories
FMT_SMF.1 / Memories	FMT_SMF.1 / Memories
FIA_API.1	FIA_API.1
FMT_LIM.1 / Loader	FMT_LIM.1 / Loader
FMT_LIM.2 / Loader	FMT_LIM.2 / Loader
FTP_ITC.1 / Loader	FTP_ITC.1 / Loader
FDP_UCT.1 / Loader	FDP_UCT.1 / Loader
FDP_UIT.1 / Loader	FDP_UIT.1 / Loader
FDP_ACC.1 / Loader	FDP_ACC.1 / Loader
FDP_ACF.1 / Loader	FDP_ACF.1 / Loader
FMT_MSA.3 / Loader	FMT_MSA.3 / Loader
FMT_MSA.1 / Loader	FMT_MSA.1 / Loader
FMT_SMR.1 / Loader	FMT_SMR.1 / Loader
FIA_UID.1 / Loader	FIA_UID.1 / Loader
FIA_UAU.1 / Loader	FIA_UAU.1 / Loader
FMT_SMF.1 / Loader	FMT_SMF.1 / Loader
FPT_FLS.1 / Loader	FPT_FLS.1 / Loader
FAU_SAR.1 / Loader	FAU_SAR.1 / Loader
FAU_SAS.1 / Loader	FAU_SAS.1 / Loader
FTP_ITC.1 / Sdiag	FTP_ITC.1 / Sdiag
FAU_SAR.1 / Sdiag	FAU_SAR.1 / Sdiag
FMT_LIM.1 / Sdiag	FMT_LIM.1 / Sdiag
FMT_LIM.2 / Sdiag	FMT_LIM.2 / Sdiag

7.2.3 Compatibility of Security Assurance Requirements

306 The level of assurance of the TOE is EAL5 augmented with ASE_TSS.2, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and the composite product package (COMP), while the level of assurance of the Platform is EAL6 augmented with ASE_TSS.2 and ALC_FLR.2.

307 Therefore, the set of Security Assurance Requirements of this composite evaluation is a subset of the he Security Assurance Requirements of the underlying platform, except the composite package (COMP) which is specific to the Security Target.

308 There is no conflict regarding the Security Assurance Requirements.

8 Identification

Table 15. TOE components

Platform identification				Library identification
IC Maskset name	IC version	Master identification number	Firmware version	MIFARE DESFire EV3 version
K4H0A	B	0x0299	3.0.6	1.0.3

Table 16. Guidance documentation

Component description	Reference	Version
MIFARE® DESFire® EV3 library v1.0 for the ST31R platform devices - User manual - 1	UM_ST31R_MFD_EV3_1.0	3
MIFARE DESFire EV3 interface specification - Technical note	TN_MIFARE_DESFire_EV3	3
MIFARE® DESFire® EV3 on ST31R: Guidance and operational manual	UM_ST31R_GOM_MFD_EV3	4
MIFARE® DESFire® EV3 library 1.0.3 on ST31R480 - Release note	RN_ST31R_MFD_EV3_1.0.3	1

Table 17. Sites list

Site	Address	Activities[(1)]	Phase
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	ES_DEV	1
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, ZI. 13106 Rousset Cedex France	ES_DEV	1
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l’Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT	1
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B 3d floor 1831 Diegem/Machelen Belgium	ES_DEV	1

1. ES-DEV = development, IT = Network infrastructure

9 References

Table 18. Common Criteria

Component description	Reference	Version
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 1: Introduction and general model, November 2022	CCMB-2022-11-001 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, November 2022	CCMB-2022-11-002 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, November 2022	CCMB-2022-11-003 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 5: Pre-defined packages of security requirements, November 2022.	CCMB-2022-11-005 R1	2022 Rev 1

Table 19. Platform Security Target

Ref	Component description	Reference	Version
[PF-ST]	ST31R480 A01 Security Target for composition	SMD_ST31R480_ST_23_002	A01.4

Table 20. Protection Profile and other related standards

Ref	Component description	Reference	Version
[PP0084]	Eurosmart - Security IC Platform Protection Profile with Augmentation Packages	BSI-CC-PP-0084-2014	1.0
[AUG]	Smartcard Integrated Circuit Platform Augmentations, March 2002.		1.0
[JILSR]	Security requirements for post-delivery code loading, Joint Interpretation Library, February 2016		1.0

Table 21. 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 Rev.2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology

Table 21. Other standards

Ref	Identifier	Description
[3]	FIPS 197	FIPS 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 2001
[4]	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
[5]	NIST SP 800-38B	NIST special publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), June 2016
[6]	ANSSI-PP0084.03	PP0084: Interpretations, ANSSI, June 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 authorised 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 authorised 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 1 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 22. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI).
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1. R5.
CMAC	Cipher-based Message Authentication Code
DES	Data Encryption Standard.
EAL	Evaluation Assurance Level.
ES	Security IC Embedded Software.
ES-DEV	Embedded Software Development.
FIPS	Federal Information Processing Standard.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
MFDF	MIFARE DESFire EV3
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
ST	Context dependent : STMicroelectronics or Security Target.
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.

IMPORTANT NOTICE – PLEASE READ CAREFULLY