SECURITY TARGET-LITE

FLY3bis

ISSUE: 2.1

Issue Date	Author	Status	Purpose
October 4/12	S. Mestiri	Version1	**Version 1 of Security Target Lite, created from full ST**
June 7/13	S. Mestiri	Version 2	**Updated version following complete validated ST**
August 9/13	JM. Esteban	Version 2.1	**Update TOE Name**

Table of contents

List of tables

List of figures

1 PREFACE

1.1 OBJECTIVES OF THE DOCUMENT

The objective of this document is to present the security target of the TOE. This Security target is an implementation of security needs for the use of DESFire on the (U)SIM Open Platform.

The basis for this evaluation is the composite evaluation of this security needs plus an already evaluated component (ie: the hardware plus the DESFire library provided by the component).

This Security Target aims to satisfy the requirements of Common Criteria level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.

1.2 SCOPE OF THE DOCUMENT

This document describes the Security Target for the NFC FLYBuy Platinum V3.0 with the DESFire services.
This card is consistent with the Java Card 3.01 Classic Edition specifications, as well as the GlobalPlatform 2.2 specification.

The objectives of this Security Target are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle.
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases.
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the platform active phases.
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment.
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements.
- To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

1.3 RELATED DOCUMENTS

[1] "Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", July 2009, Version 3.1 revision 3.

[2] "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", July 2009, Version 3.1 revision 3.

[3] "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", July 2009, Version 3.1 revision 3.

[4] “Composite product evaluation for Smart Cards and similar devices”, September 2007, Version 1.0, CCDB-2007-09-001.

[5] PP SUN Java Card™ System Protection Profile Open Configuration V2.6, April 19, 2010.

[6] "Java Card - API" Application Programming Interfaces, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[7] "Java Card – JCRE” Runtime Environment Specification, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[8] "Java Card - Virtual Machine Specifications" Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[9] GlobalPlatform Card Specification – Version 2.2.1 – January 2011.

[10] GlobalPlatform Card Mapping Guidelines of existing GP v2.1.1 implementations on v2.2.1 – Version 1.0.1 – January 2011.

[11] GlobalPlatform Card Confidential Card Content Management – Card Specification v 2.2 – Amendment A – Version 1.0.1 – January 2011.

[12] GlobalPlatform Card UICC Configuration – Version 1.0.1 – January 2011.

[13] GlobalPlatform Card Contactless Services Card Specification v 2.2 – Amendment C Version 1.0– February 2010.

[14] Visa GlobalPlatform 2.1.1 Card Implementation Requirements – Version 2.0 – July 2007.

[15] "Identification cards - Integrated Circuit(s) Cards with contacts, Part 6: Inter industry data elements for interchange", ISO / IEC 7816-6 (2004).

[16] FIPS PUB 46-3 “Data Encryption Standard”, October 25, 1999, National Institute of Standards and Technology

[17] FIPS PUB 81 “DES Modes of Operation”, December, 1980, National Institute of Standards and Technology

[18] FIPS PUB 140-2 “Security requirements for cryptographic modules”, May 2001, National Institute of Standards and Technology

[19] FIPS PUB 180-3 “Secure Hash Standard”, March 2012 , National Institute of Standards and Technology

[20] FIPS PUB 186-3 “Digital Signature Standard (DSS)”, June 2009, National Institute of Standards and Technology

[21] FIPS PUB 197, “The Advanced Encryption Standard (AES)”, November 26, 2001, National Institute of Standards and Technology

[22] SP800_90 “Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)”, March 2007, National Institute of Standards and Technology

[23] ANSI X9.31 “Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)”, 1998, American National Standards Institute

[24] ISO/IEC 9796-1, Public Key Cryptography using RSA for the financial services industry", annex A, section A.4 and A.5, and annex C (1995)

[25] ISO/IEC 9797-1, “Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher”, 1999, International Organization for Standardization

[26] PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993

[27] IEEE Std 1363a-2004, “Standard Specification of Public Key Cryptography – Amendment 1: Additional techniques”, 2004, IEEE Computer Society

[28] IC Platform Protection Profile, Version 1.0, reference BSI-PP-0035 (15.06.2007).

[29] ST33F1M/1M0/896/768/640/512E,SC33F1M0/896/768/640/512/384E, SM33F1M/1M0/896/768/640/512E,E33F1M/1M0/896/768/640/512E, SL33F1M/1M0/896/768/640/512E, SP33F1ME, with dedicated software revision D, optional cryptographic library NESLIB3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 Security Target - Public Version Common Criteria for IT security Evaluation SMD_SM33Fxxx_ST_12_001 Rev 01.02.

[30] 3GPP TS 21.111 (v6.3.0, Rel-6): USIM and IC card requirements

[31] 3GPP TS 22.038 (v6.5.0, Rel-6): USIM Application Toolkit (USAT) - Stage 1

[32] 3GPP TS 23.040 (v6.9.0, Rel-6): Technical realization of the Short Message Service (SMS)

[33] 3GPP TS 23.041 (v6.2.0, Rel-6): Technical realization of Cell Broadcast Service (CBS)

[34] 3GPP TS 23.048 (v5.9.0, Rel-5): Security Mechanisms for the (U)SIM application toolkit; Stage 2

[35] 3GPP TS 31.048 (v5.1.0, Rel-5): Test of (U)SAT security

[36] 3GPP TS 31.101 (v6.5.1, Rel-6): UICC-Terminal interface; Physical and Logical Characteristics

[37] 3GPP TS 31.102 (v6.21.0, Rel-6): Characteristics of the USIM Application

[38] 3GPP TS 31.103 (v6.11.0, Rel-6): Characteristics of the ISIM Application

[39] 3GPP TS 31.111 (v6.14.0, Rel-6): USIM Application Toolkit (USAT)

[40] 3GPP TS 31.115 (v6.5.0, Rel-6): Secured packet structure for (U)SIM Toolkit applications

[41] 3GPP TS 31.116 (v6.8.0, Rel-6): Remote APDU Structure for (U)SIM Toolkit applications

[42] 3GPP TS 31.122 (v6.3.0, Rel-6): USIM conformance test (card side)

[43] 3GPP TS 31.130 (v6.5.0, Rel-6): (U)SIM Application Programming Interface; (U)SIM API for Java™ Card

[44] 3GPP TR 31.900 (v7.1.0, Rel-7): SIM/USIM Internal and External Inter-working Aspects

[45] 3GPP TS 31.919 (v6.1.0, Rel-6): 2G/3G Java Card™ API based applet interworking

[46] 3GPP TS 33.102 (v6.5.0, Rel-6): 3G Security; Security architecture

[47] 3GPP TS 33.105 (v6.0.0, Rel-6): Cryptographic algorithm requirements

[48] 3GPP TS 35.205 (v6.0.0, Rel-6): Specification of the MILENAGE Algorithm Set

[49] 3GPP TS 42.017 (v4.0.0, Rel-4): SIM functional characteristics

[50] 3GPP TS 42.019 (v5.6.0, Rel-5): SIM API for Java Card™ - Stage 1 -

[51] 3GPP TS 43.019 (v5.6.0, Rel-5): Subscriber Identity Module Application Programming Interface; (SIM API) for Java Card™; Stage 2

[52] 3GPP TS 51.011 (v4.15.0, Rel-4): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

[53] 3GPP TS 51.014 (v4.5.0, Rel-4): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

[54] 3GPP TS 51.017 (v4.2.0, Rel-4): Test of SIM-ME interface (card side)

[55] ETSI TS 101 220 (v6.7.0, Rel-6): Application Identifiers for telecommunications

[56] ETSI TS 102 124 (v6.1.0, Rel-6): Transport Protocol for CAT Applications - Stage 1

[57] ETSI TS 102 127 (v6.13.0, Rel-6): Transport Protocol for CAT applications; Stage 2

[58] ETSI TS 102 151 (v6.0.0, Rel-6): Measurement of Electromagnetic Emission of SIM cards

[59] ETSI TS 102 221 (v6.12.0, Rel-6): UICC-Terminal interface; Physical and logical characteristics

[60] ETSI TS 102 222 (v6.11.0, Rel-6): Administrative Commands for telecommunications applications

[61] ETSI TS 102 223 (v6.13.0, Rel-6): Card Application Toolkit

[62] ETSI TS 102 224 (v6.1.0, Rel-6): CAT security – Stage 1

[63] ETSI TS 102 225 (v6.8.0, Rel-6): Secured packet structure for UICC applications

[64] ETSI TS 102 226 (v6.18.0, Rel-6): Remote APDU Structure for UICC based Applications

[65] ETSI TS 102 240 (v6.2.0, Rel-6): UICC Java Card™ API - Stage 1

[66] ETSI TS 102 241 (v6.12.0, Rel-6): UICC Java Card™ API - Stage 2

[67] ETSI TS 102 613 (v7.9.0, Rel-7): UICC – Contactless Front-end (CLF) Interface – Part 1: Physical and data link layer characteristics

[68] ETSI TS 102 622 (v7.9.0, Rel-7): UICC – Contactless Front-end (CLF) Interface – Host Controller Interface (HCI)

[69] ETSI TS 102 705 (v9.2.0, Rel-9): UICC Application Programming Interface for Java Card™ for Contactless Applications

[70] ETSI TS 131.111, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 6)

[71] ETSI TS 131.130, Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS); (U)SIM Application Programming Interface (API);(U)SIM API for Java Card (3GPP TS 31.130 version 6.6.0 Release 6)

[72] Mifare Classic references Mifare Classic 1KB and 4KB, Interface Specification rev. 1.3 -2009-10-30

[73] ST, User manuel, MIFARE Classic Sofware library revision 1.0

[74] Mifare Desfire ST Library ST, User manuel, MIFARE DESFire EV1 library revision 1.0

[75] Mifare DESFire EV1, Interface Specification rev. 1.0 -2008-11-21

1.4 ABREVIATIONS

AES	Advanced Encryption Standard
AID	Applet Identifier
APDU	Application Protocol Data Unit
API	Application Programmer Interface
APSD	Application Provider Security Domain
BIOS	Basic Input/Output System
CASD	Controlling Authority Security Domain
CC	Common Criteria
CM	Card Manager
CPLC	Card Production Life Cycle
DAP	Data Authentication Pattern
DES	Cryptographic module "Data Encryption Standard"
EAL	Evaluation Assurance Level
EC	Elliptic Curves
EEPROM	Electrically Erasable and Programmable Read Only Memory
ES	Embedded Software
FAT	File Allocation Table
GP	Global Platform
IC	Integrated Circuit
ISD	Issuer Security Domain
IT	Information Technology
JCP	Java Card Platform
JCRE	Java Card Runtime Environment
OSP	Organizational Security Policy
PP	Protection Profile
RNG	Random Number Generation
ROM	Read Only Memory
RSA	Cryptographic module "Rivest, Shamir, Adleman"
SF	Security Function
SFP	Security Function Policy
SHA-1	Cryptographic module "Secure hash standard"
ST	Security Target
TOE	Target of Evaluation.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VASD	Validation Authority Security Domain
VM	Virtual Machine

2 Security Target Introduction

This Security Target takes place in the context of the explosion of services provided by MNOs which intends to open (U)SIM card to new applications using the DESFire.

In addition to services provided by the IC, the TOE offers to applications a security services in order to protect application data and code of DESFire.

The TOE offers two physical interfaces: ISO7816 and SWP interfaces.

2.1 ST REFERENCE

Title: Security Target FLY3bis

Name: DESFire services of NFC FLYBuy Platinum V3.0 on SM33F1M

Oberthur Technologies registration: FQR 110 6469

Version: Issue 2.2

Authors: Oberthur Technologies

Date: June 2013

2.2 ST-Lite REFERENCE

Title: Security Target-Lite FLY3bis

Name: DESFire services of NFC FLYBuy Platinum V3.0 on SM33F1M

Oberthur Technologies registration: FQR 110 6326

Version: Issue 2.1

Authors: Oberthur Technologies

Date: June 2013

2.3 TOE REFERENCE

TOE Name	DESFire services of NFC FLYBuy Platinum V3.0 on SM33F1ME
Internal reference	**USIM V3.1 NFC FLYBuy Platinum V3.0 EAL4+ 768K on DCN9**
Code / Hardware Identification	079424
Card Manager Identification	GOP Ref V11.3
Label PVCS CODE	USIM_V31_NFC_ FLYBUY_PLATINUM_079424

IC reference	SM33F1ME
Identication of IC ST lite	ST33F1M/1M0/896/768/640/512E, SC33F1M0/896/768/640/512/384E, SM33F1M/1M0/896/768/640/512E, SE33F1M/1M0/896/768/640/512E, SL33F1M/1M0/896/768/640/512E, SP33F1ME, with dedicated software revision D, optional cryptographic library NESLIB 3.0 or 3.2, and optional technology MIFARE DESFire™ EV1 Security Target - Public Version SMD_SM33Fxxx_ST_12_001 Rev 01.02 December 2012
IC Certificate	ANSSI-CC-2013/13

Table 1: TOE References

2.3.1 TOE Identification

In order to assure the authenticity of the card, the product identification shall be verified by analysing:

- The ATR:
  3B 9F 96 80 3F C7 00 80 31 E0 73 FE 21 1B 64 **07 94 24** 00 82 90 00

  Where **07 94 24** is the SAAAAR code.

- The response of the command GET DATA:

```
Command      : 80 CA 9F 7F 2D
Output Data  : 9F 7F2A 47 50 00 2B 82 31 30 35 33 38 00 00 00
             : 00 00 00 00 00 00 00 00 00 00 00 00 00 14 34 12
             : 80 00 00 00 00 14 34 03 36 00 00 00 00
Status       : 90 00
```

The meaning of the following bytes in the response of the command is:

- ⇨ FAB_ID : **47 50**
- ⇨ IC_ID : **00 2B**
- ⇨ OS_ID : **82 31**
- ⇨ OS_Release_Date : **30 35**
- ⇨ OS_Release_Level : **33 38**

2.4 TOE Overview

Embedded Software comprises the MIFARE technology library. This library is a secure library called MIFARE DESFire™ EV1, which is in the scope of this evaluation.

This section presents the TOE, it consists on the evaluated IC with DESFire function plus the complement of the DESFire specified within this security target.

This section presents also the architecture of the product containing the TOE. The TSF is implemented in the yellow part.

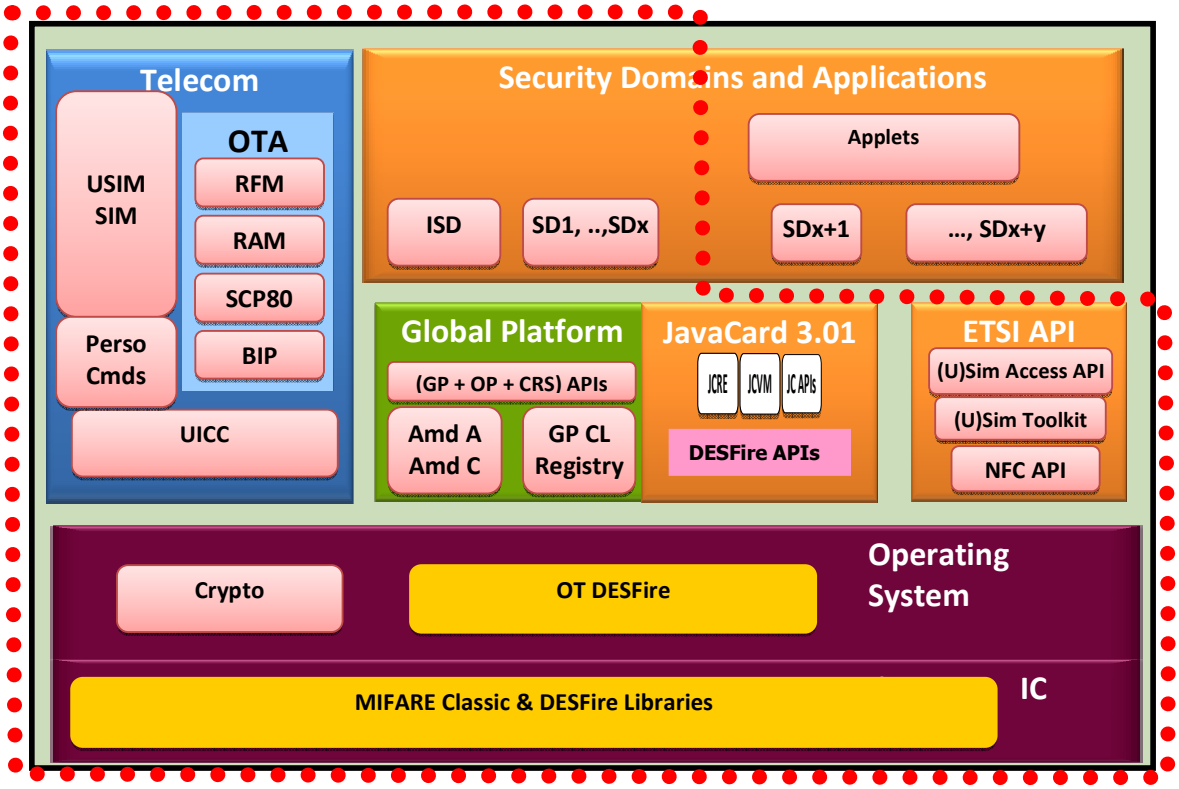

Figure 1: Product Architecture

The (U)SIM card is intended to be plugged in a mobile phone or other mobile devices to provide services to an end user.

The Target of Evaluation (TOE) is composed of all the blocks except applets. The security functions are implemented in the yellow parts:

- DESFire specific Security Functions to allow integrity and confidentiality of the Desfire application Data and confidentiality of the DesFire application Code.
- An already evaluated Chip with DESFire librairies.

The ISD and some SDs (SD1, .. SDx) are included in the scope as they are part of the TOE. The others (SDx+1….SDx+y) are not included and will be created during the life cycle of the product (as they are associated to new loaded applets).

2.5 TOE Description

The generic architecture of the **product** is presented in Figure 1 and each TSF block (in yellow) is detailed in the following paragraphs. There is disctinction between DESFire Libraries and DESFire OT.

The DESFire libraries are developped by ST and the OT DESFire is developped by OT.

This Security IC with the DESFire library includes:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- Hardware Security Enhanced DES accelerator,
- AIS-31 class P2 compliant True Random Number Generator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- NExt Step CRYPTography accelerator (NESCRYPT),
- and secure MIFARE DESFire EV1 library.

This library contains also MIFARE Classic™, which is not in the scope of this evaluation.

For security function IC details, please refer to [29]. General Characteristics are presented in the Table 1 below:

Different Chip ID	**SM ST33F1ME**
Flash size	1,2 Mbytes
ROM	280 Kbytes
General RAM	30 Kbytes
Crypto RAM	2 Kbytes
SWP RAM	512 bytes
OTP	256 bytes
ContactLess interface	SWP
Mifare Libraries	Classic DESFire

Table 2: IC General Characteristics

This OT DESFire consits on:

- Access control to DESFire code and date.
- Clearing ressources used by the DESfire.

2.5.1 TOE Life Cycle

The TOE life cycle follows the description of the [5] and is part of the product life cycle, i.e. the (U)SIM card, which goes from product development to its usage by the final user. The product life cycle phases are those detailed in Figure 2. We refer to [PP0035] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software with DESFire Libraries, OS, Java Card System, DESFire OT

(U)SIM applet, other platform components such as Card Manager, Applets) and IC development.

- Phase 3 and 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalisation steps may occur in Phase 3.
- Phase 5 concerns the embedding of software components within the IC.
- Phase 6 is dedicated to the product personalization prior final use.
- Phase 7 is the product operational phase.

The TOE life cycle is composed of four stages:

- Development,
- Storage, pre-personalization and test,
- Personalization and test,
- Final usage.

These 4 stages map to the typical smart card life cycle phases as shown in Figure 2.

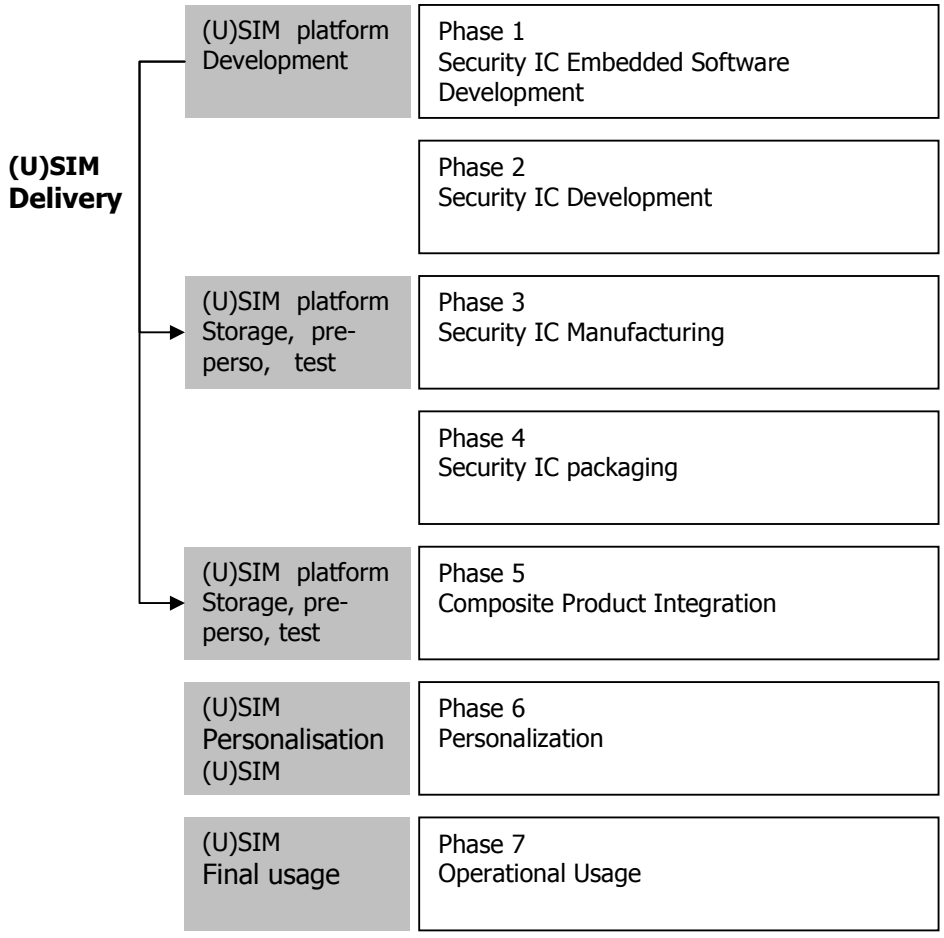

Figure 2: (U)SIM platform (TOE) Life Cycle within Product Life Cycle

The TOE Development is performed during Phase 1. This includes OT DESFire (all security functions added to the libraries are included here), Java Card System (JCS) and (U)SIM conception, design, implementation, testing and documentation. The development fulfilled requirements of the final product, including conformance to Java Card Specifications, and recommendations of the SCP user guidance. The development is made in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The evaluation of the TOE includes the platform development environment.

The delivery of the product occurs end of phase 4 (5 and 6 are done in the same environment) at Oberthur manufacturing sites. In this phase, IC is also delivered by the IC manufacturer to Oberthur manufacturing sites.

Delivery and acceptance procedures guaranty the authenticity, the confidentiality and integrity of the exchanged pieces. (U)SIM platform delivery involves encrypted signed sending and it supposes the previous exchange of public keys. The evaluation of the TOE includes the delivery process.

Phases 4, 5 and 6 are done in the Oberthur manufacturing sites. They represent the code loading and personalisation of the (U)SIM Platforms. The phases take place in a controlled environment (secure locations, secure procedures and trusted personnel).

The product is tested and all critical materials including personalization data, test suites and documentation are protected from disclosure and modification.

During these phases, MNO (ISD keys and other initial data), Controlling Authority and Verification Authority data are loaded on the (U)SIM. After this phase, the (U)SIM card reaches the INITIALIZED state.

In phase 7, the (U)SIM platform provides the full set of security functionalities of the DESFire.

Card management (including applications loading and personalization) can occur during production in a secure area in phases 4, 5 and 6 or during the product usage in phase 7 using an OTA bearer.

All processes until the end of phase 6 are part of the assurance component ALC. (U)SIM Platform personalisation and applet loading are performed in Oberthur's industrial sites.

At the end of phase 6, the (U)SIM product is ready for use, it is sent to the customer.

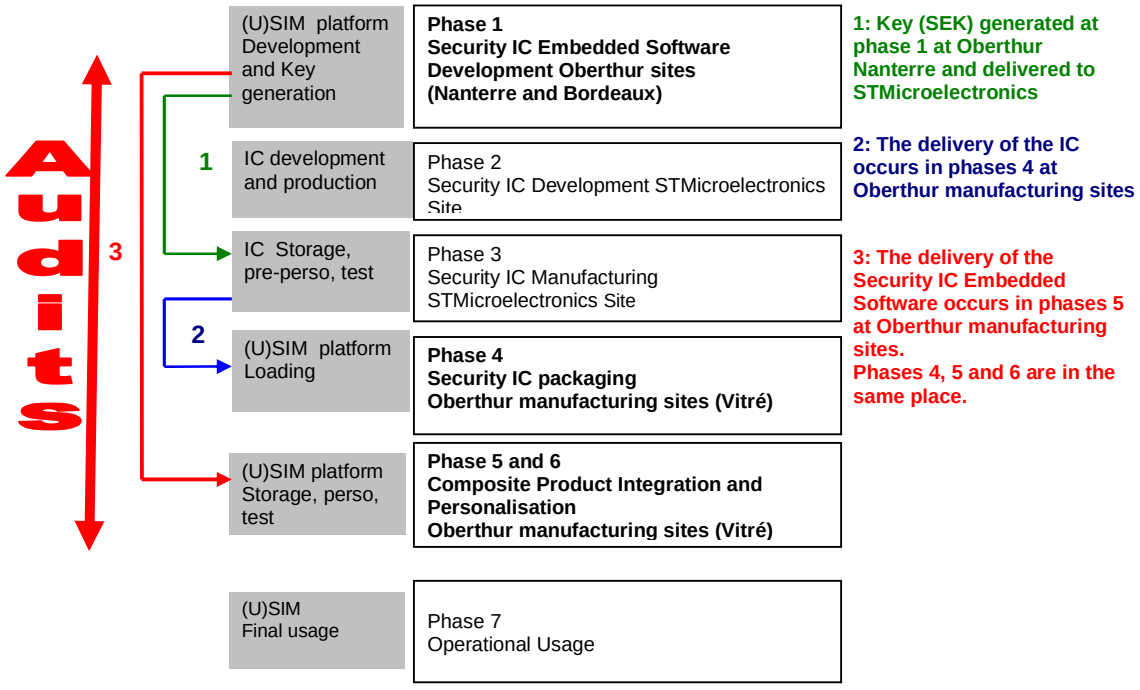

Figure 3: DESFire services of NFC FLYBuy Platinum V3.0 Life Cycle within Product Life Cycle

The following steps of the life cycle are covered as specified in the table below:

Life cycle phase	Environment	Covered by
Phase 1	DESFire services of NFC FLYBuy Platinum V3.0 on SM33F1M	ALC [FLY] Oberthur Sites : *Nanterre and Bordeaux in France Covered by an audit*
Phase 2	IC Development	ALC [IC] STMicroelectronics Site And [IC] EAL4+ Evaluation
Phase 3	Security IC Manufacturing	ALC [IC] STMicroelectronics Site And [IC] EAL4+ Evaluation
Phase 4	Security IC packaging TOE	ALC [FLY] Oberthur Site: Vitré Site *Covered by an audit*
Phase 5 and 6	Construction of the TOE	ALC [FLY] Oberthur Site: Vitré Site *Covered by an audit*
Phase 7	Operational Phase of the TOE	AGD_OPE [FLY]

[FLY] means that the audit is under the scope of FLY3bis at Oberthur promises.

[IC] is under the responsibility of STMicroelectronics. It's under the scope of IC certificate.

2.5.1.1 TOE Guidance

The table below lists the guidance for the users of the TOE.

1-Guidance document for Platform production	- FQR 110 6560 Issue1 NFC FlyBuy Platinum v3.0 AGD_PRE - FQR 110 6561 Issue1 NFC FlyBuy Platinum v3.0 Production Life Cycle
2-Guidance document for development of application on Platform	- SRS 079421 11 SRS AA APIs - FQR 110 6576 Issue1 NFC FlyBuy Platinum v3.0, DESFireST APIs User Guide - Standard documentation for Java Card API [6] and UICC API [65][66]. - NFC FlyBuy platinum - Application Development guide FQR 110 5885 V1.1 - NFC FlyBuy - Application Security Recommandations FQR 110 5886 Issue2
3-Guidance document for Product Issuer	- NFC Flybuy Platinum V3.0 - Application Management Guide FQR 110 6443 Ed 1
4-Guidance for ticketing systems terminals	- Mifare DESFire EV1 Initialization Specification Rev.01.12 - 22. Dec 2010 NXP - Mifare DESFire EV1, Interface Specification rev. 1.0 -2008-11-21,NXP

Table 3: TOE Guidance references

2.5.2 Non-TOE available to the TOE

2.5.2.1 Mobile Terminals

The (U)SIM as a smart card is intended to be plugged in a mobile handset. This equipment can be a mobile phone or a PDA or any other connecting device.

2.5.2.2 Terminals, Remote Servers and Trusted IT Products

Using its NFC (contactless) interface, the TOE can communicate with a card reader such as POS (Point of Sale) equipments or ticketing systems terminals. These terminals are responsible for the protection of their own assets.

The Platform NFC with DESFire can communicate with the ticketing systems terminals (Contactless). This ticketing systems terminals shall be conformant to:

-Mifare DESFire EV1 Initialization Specification Rev.01.12 - 22. Dec 2010 NXP,

-and Mifare DESFire EV1, Interface Specification rev. 1.0 -2008-11-21,NXP.

Using the BIP interface or SMS, the TOE can also communicate with remote servers, for instance for remote administration or transfer of applicative data. For sensitive operations, such as remote administration, the TOE may require mutual authentication or the use of secure channels. In that case, the keys and/or certificates required for these operations on the TOE will also have to be available from the remote server and protected. The remote server and, if any, the device (such a HSM) from which the keys are obtained are referred as a Trusted IT product.

3 Conformance Claims

3.1 CC Conformance Claims

This Security Target claims conformance to **CC version 3.1** with the following documents:

[1] "Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4.

[2] "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4.

[3] "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4.

Conformance is claimed as follows:

Part 1:conformant
Part 2: conformant
Part 3: conformant EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

4 Security Problem Definition

4.1 DESFire Assets

Since this Security Target is a composition with a component already evaluated with Profile (BSI-PP-0035) with DESFire embedded in the component. This ST has 2 assets: DESFire application data and DESFire Code.

DESFire application Data

This asset concerns DESFire Data. These data need to be protected from disclosure and unauthorized modification.

DESFire application Code

This asset concerns DESFire code. This code requires protection form unauthorized disclosure.

4.2 Threats

4.2.1 Threats on DESFIRE

This ST faces to the 3 threats related to DESFire code and Data. The 3 threats are Assumptions in IC ST of the component [29] as precised: A.Confid-Applic-Code is in this ST T.confid-appli-code, A.Confid-Applic-Data is in this ST T.Confid-Applic-Data and A.Integ-Applic-Data is in this ST T.Integ-Applic-Data.

T.confid-appli-code

DESFire code confidentiality:

MIFARE DESFire EV1 Licensed product code must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the MIFARE DESFire EV1 licensed product executable code is stored. The attacker executes an application to disclose code belonging to MIFARE DESFire EV1 Licensed product.

T.confid-appli-Data

DESFire data confidentiality:

MIFARE DESFire EV1 Licensed product data must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the MIFARE DESFire EV1 licensed product data by another application. For example, the attacker executes an application that tries to read data belonging to MIFARE DESFire EV1 Licensed product.

T.Integ-Appli-Data

DESFire data integrity:

MIFARE DESFire EV1 Licensed product data must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the MIFARE DESFire EV1 Licensed product data by another application. The attacker executes an application that tries to alter (part of) the DESFire EV1 Licensed product data.

4.3 Organizational Security Policies

This ST doesn't provide any additional OSP to the certified IC, see IC ST [29].

4.4 Assumptions

The following paragraphs present the assumptions on the product operational environment from phase 5 to phase 7. The Assumptions are from certified IC ST [29]. Then there is no contradiction with each other.

A.Secure _Value

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

A.Terminal_Support

Terminal support to ensure integrity and confidentiality:

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

5 Security Objectives

5.1 Security Objectives for the TOE

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.

The 2 following objectives for the TOE are taken from the ST [29] were they are security objective for the environment.

O.Firewall

DESFire firewall:

The TOE shall ensure isolation of data and code between MIFARE DESFire EV1 and the other applications. An application shall not read, write, compare any piece of data or code belonging to the MIFARE DESFire EV1 Licensed product.

O.Shr-Res

DESFire data cleaning for resource sharing:

It shall be ensured that any hardware resource, that is shared by MIFARE DESFire EV1 and other applications or by any application which has access to such hardware resource, is always cleaned (using code that is part of the MIFARE DESFire EV1 system and its certification) whenever MIFARE DESFire EV1 is interrupted by the operation of another application. The only exception is buffers as long as these buffers do not contain other information than what is communicated over the contactless interface or has a form that is no different than what is normally communicated over the contactless interface. For example, no data shall remain in a hardware cryptographic coprocessor when MIFARE DESFire EV1 is interrupted by another application.

5.2 Security Objectives for the Operational Environment

The 2 following objectives for the operational Environment are taken from the ST [29] were they are also security objective for the environment.

OE.Secure_Values

Generation of secure values:

The environment shall generate confidential and secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalization or usage in phase 5 to 7.

OE.Terminal_Support

Terminal support to ensure integrity and confidentiality:

The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session in phase 7.

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 Threats on DESFIRE

T.confid-appli-code The justification related to the threat DESFire code confidentiality, (T.Confid-Applic-Code) is as follows: Since O.Firewall requires that the TOE ensures isolation of code between DESFire and the other applications, the code of DESFire is protected against unauthorized disclosure, therefore T.Confid-Applic-Code is covered by O.Firewall.

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

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

T.Integ-Appli-Data The justification related to the threat DESFire data integrity, (T.Integ-Applic-Data) is as follows: The threat is related to the alteration of DESFire data by an attacker. Since O.Firewall and O.Shr-Res require that the TOE ensures complete isolation of data between DESFire and the other applications, the data of DESFire is protected against unauthorized modification; therefore T.Integ-Applic-Data is covered by O.Firewall together with O.Shr-Res.

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

5.3.2 Assumptions

A.Secure _Value This assumption is directly upheld by OE.Secure_Values

A.Terminal_Support This assumption is directly upheld by OE.Terminal_Support.

5.3.3 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.confid-appli-code	O.Firewall	Section 2.3.1
T.confid-appli-Data	O.Firewall	Section 2.3.1
T.Integ-Appli-Data	O.Shr-Res, O.Firewall	Section 2.3.1

Table 4 Threats and Security Objectives - Coverage

Security Objectives	Threats
O.Firewall	T.confid-appli-code, T.confid-appli-Data, T.Integ-Appli-Data
O.Shr-Res	T.Integ-Appli-Data
OE.Secure_Values	
OE.Terminal_Support	

Table 5 Security Objectives and Threats - Coverage

Security Objectives
O.Firewall
O.Shr-Res
OE.Secure_Values
OE.Terminal_Support

Table 6 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Secure_Value	OE.Secure_Values	Section 2.3.2
A.Terminal_Support	OE.Terminal_Support	Section 2.3.2

Table 7 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.Secure_Values	A.Secure_Value
OE.Terminal_Support	A.Terminal_Support

Table 8 Security Objectives for the Operational Environment and Assumptions - Coverage

6 Security Requirements

6.1 Security Functional Requirements

FDP_ACC.1/DSF/OT Subset access control

FDP_ACC.1.1/DSF/OT The TSF shall enforce the ***Access Control Policy*** on ***DESFire Code and Data***.

FDP_RIP.1/DSF/OT Subset residual information protection

FDP_RIP.1.1/DSF/OT 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: ***DES***.

FDP_ACF.1/DSF/OT Security attribute based access control

FDP_ACF.1.1/DSF/OT The TSF shall enforce the ***Access Control Policy*** to objects based on the following: ***DESFire code and data***.

FDP_ACF.1.2/DSF/OT The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***An application cannot read, write, and compare any piece of data or code belonging to DESFire***.

FDP_ACF.1.3/DSF/OT The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***None***.

FDP_ACF.1.4/DSF/OT The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***An application cannot read, write, and compare any piece of data or code belonging to DESFire.***

FMT_MSA.3/DSF/OT Static attribute initialisation

FMT_MSA.3.1/DSF/OT The TSF shall enforce the ***Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/DSF/OT The TSF shall allow the ***no subject*** to specify alternative initial values to override the default values when an object or information is created.

6.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Objectives

6.3.1.1 Security Objectives for the TOE

Objectives for the TOE/DESFire

O.Firewall The justification related to the security objective DESFire firewall (O.Firewall) is as follows: The security functional requirements "Subset access control FDP_ACC.1/DSF/OT" and "Security attribute based access control (FDP_ACF.1/DSF/OT", supported by "Static attribute initialisation FMT_MSA.3/DSF/OT", require that no application can read, write, compare any piece of data or code belonging to DESFire. This meets the objective O.Firewall.

O.Shr-Res The justification related to the security objective DESFire data cleaning for resource sharing O.Shr-Res is as follows: The security functional requirement "Subset residual information protection FDP_RIP.1/DSF/OT requires that the information content of a resource is made unavailable upon its deallocation from DESFire. This meets the objective O.Shr-Res.

6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.Firewall	FDP_ACF.1/DSF/OT, FDP_ACC.1/DSF/OT, FMT_MSA.3/DSF/OT	Section 3.3.1
O.Shr-Res	FDP_RIP.1/DSF/OT	Section 3.3.1

Table 9 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FDP_ACC.1/DSF/OT	O.Firewall
FDP_RIP.1/DSF/OT	O.Shr-Res
FDP_ACF.1/DSF/OT	O.Firewall
FMT_MSA.3/DSF/OT	O.Firewall

Table 10 SFRs and Security Objectives

6.3.3 Dependencies

6.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/DSF/OT	(FDP_ACF.1)	FDP_ACF.1/DSF/OT
FDP_RIP.1/DSF/OT	No Dependencies	
FDP_ACF.1/DSF/OT	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/DSF/OT, FMT_MSA.3/DSF/OT
FMT_MSA.3/DSF/OT	(FMT_MSA.1) and (FMT_SMR.1)	

Table 11 SFRs Dependencies

Rationale for the exclusion of Dependencies

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

The dependency FMT_SMR.1 of FMT_MSA.3/DSF/OT is discarded. See justification for FMT_MSA.1/DSF/OT.

6.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 12 SARs Dependencies

6.3.4 Rationale for the Security Assurance Requirements

The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

6.3.5 ALC_DVS.2 Sufficiency of security measures

DESFire development and manufacturing processes, especially for the secure handling of the embedded software and data. Those requirements appear as the most adequate ones for a manufacturing process in which several actors exchange and store highly sensitive information. This assurance requirement will be evaluated for development and the personalization environment. The personalizer is in charge of the TOE personalization process before card issuance. He ensures the security of the keys he loads on the cards. The security of all the keys must be ensured by a well defined security policy that covers generation, storage, distribution, destruction and recovery. This policy is audited.

6.3.6 AVA_VAN.5 Advanced methodical vulnerability analysis

This component is added to EAL 4 package in order to provide sufficient robustness to counter an attacker with high attack potential without the support of a protecting environment. Moreover, the (U)SIM card with DESFire is a generic platform that could be used for a wide range of applications and specifically transport card. Potential attackers for such kind of applications include international organizations, or even a state, disposing of important means and resources.

7 TOE Summary Specification

7.1 TOE Summary Specification

SF_Firewall_Access_Control_OT_DSF

Firewall Access Control Policy

An application cannot read, write, and compare any piece of data or code belonging to DESFire.

SF_Clearing_Hardware_Ressource

SF_Clearing_Hardware_Ressource:

The TSF clears the DES that can be shared by MIFARE DESFire EV1 and other applications or by any application which has access to such hardware resource. The MIFARE DESFire EV1 is never interrupted by the operation of another application.

7.2 Compatibility of OSP

This ST doesn't add any OSP. All OSP are taken from [29].

7.3 Compatibility of assumptions

This ST doesn't add any assumption. All assumptions are taken from [29]. Some assumptions are removed:

A.Confid-Applic-Code

A.Confid-Applic-Data

A.Integ-Applic-Data

7.4 Compatibility of security objectives for the TOE and for the environment

This ST doesn't add any objective. All are issued from [29]. With the same scope, some objectives from the environment are now objectives for the TOE.

7.5 Compatibility of security functional requirements

All security functions of the IC [29] are included in this ST, all are relevant. This composite ST adds the following one. These SFRs are added to protect DESFire code and DATA to answer to Security Objectives added (initially security objectives for the Environment).

FDP_ACC.1/DSF/OT FDP_ACF.1/DSF/OT FMT_MSA.3/DSF/OT	The three SFRs ensure access control to DESFire data and code. They add additional control to already implemented SFRs in the IC and are then compatible with IC SFRs.
FDP_RIP.1/DSF/OT	This SFR contributes to data and code protection, It clears DESFire used resources and then doesn't contradict the IC SFRs

7.6 Compatibility of assurance requirements

The IC is EAL5+ augmented by ALC_DVS.2 and AVA_VAN.5. The composite TOE claims a subset of the IC assurance requirement EAL4+ with ALC_DVS.2 and AVA_VAN.5.