Security Target lite for Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform

Version 1.51 Public
No. MAP01-ASEP01-E01-51

FeliCa Networks, Inc

Introduction

This document is the Security Target for CC evaluation of "Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform"

Contents

1. Introducing the Security Target

This document is the Security Target for CC evaluation of Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform.
This Security Target is provided in accordance with "Common Criteria for Information Technology Security Evaluation" [CC].
For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 7, "Glossary and references

1.1. ST and TOE identification

This section provides the information necessary to identify and control this Security Target and its TOE, Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform (hereinafter referred as to FeliCa Applet) in a mobile phone.

Table 1: ST identification

ST attribute	Value
Name	Security Target lite for Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform
Version	1.51 Public
Reference	MAP01-ASEP01-E01-51
Issue Date	September 2017

Table 2: TOE identification

TOE attribute	Value
Name	Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform
Version	5.0
Product type	Mobile FeliCa IC Chip
Form Factor	Embedded secure element

1.2. Conformance claims

This section describes the conformance claims.

1.2.1. CC Conformance Claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1 [CC CEM]

This Security Target claims the following conformances:

- [CC Part 2] extended
- [CC Part 3] conformant

1.2.2. Package claim

The chosen level of assurance is:

- Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2 and AVA_VAN.5

1.2.3. PP claim

This Security Target and the TOE do not claim any Protection Profile (PP):

1.3. TOE overview

The TOE is an integrated circuit with an embedded smartcard operating system with FeliCa Applet. The operating system is Sm@rtSIM CX Virgo and the integrated circuit is BCM_SPS02 [ST-PLATFORM].
The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has a file system consisting of Areas and FeliCa Services, which organise files in a tree structure (as shown in Figure 1). Multiple Service Providers can use an Area or a FeliCa Service. Access keys enable access to data, via the Areas and FeliCa Services. This prevents unauthorised access to the User Services of other Service Providers. By organising these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

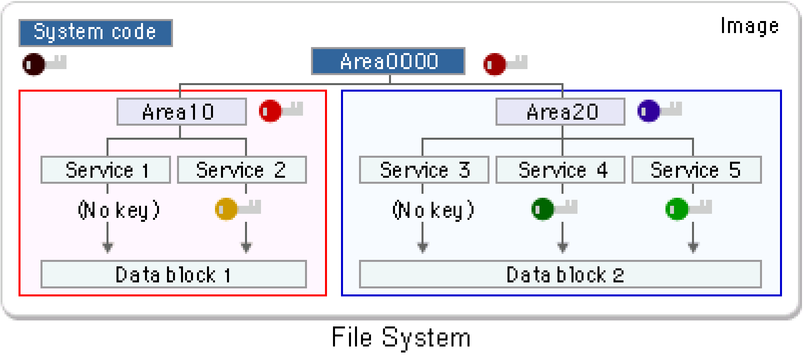


Figure 1: The FeliCa file system

The security measures of the TOE aim at protecting the access to the User Services (including associated user data), and to maintain the confidentiality and integrity of the user data. The User Services are defined by Service Providers. For example, a public transport Service Provider can incorporate the TOE into a ticketing system, to offer a ticket-payment User Service. A single TOE can be used by multiple Service Providers. A Service Provider can provide multiple User Services.

To set up the User Services and the access to those services, the Administrator (also known as a Personaliser) configures the TOE. This configuration work enables the TOE to offer various User Services, such as cash-purse and transport-payment solutions. After the TOE is personalised, the Users are allowed only to access the FeliCa Services defined by the Administrator.

The card reader and the TOE authenticate each other, and only then shall the TOE allow the card reader access, according to the access policy defined by the Administrator. After authentication the communication between the TOE and the card reader is encrypted.

The TOE has several self-protection mechanisms sufficient to satisfy all requirements for self-protection, non-bypassability, and domain separation as described by the CC supporting documents for the smartcard security evaluations [AAPS].

2. TOE description

This chapter describes the following aspects of the TOE:

- physical scope
- delivery
- logical scope
- lifecycle

2.1. Physical scope

The TOE is an integrated circuit with the Security IC Embedded Software with FeliCa Applet. The Security IC Embedded Software is the Sm@rtSIM CX Virgo and the integrated circuit is BCM_SPS02 .
The following figure illustrates the physical scope of the TOE, which is indicated in yellow, and the product, which is indicated in blue:

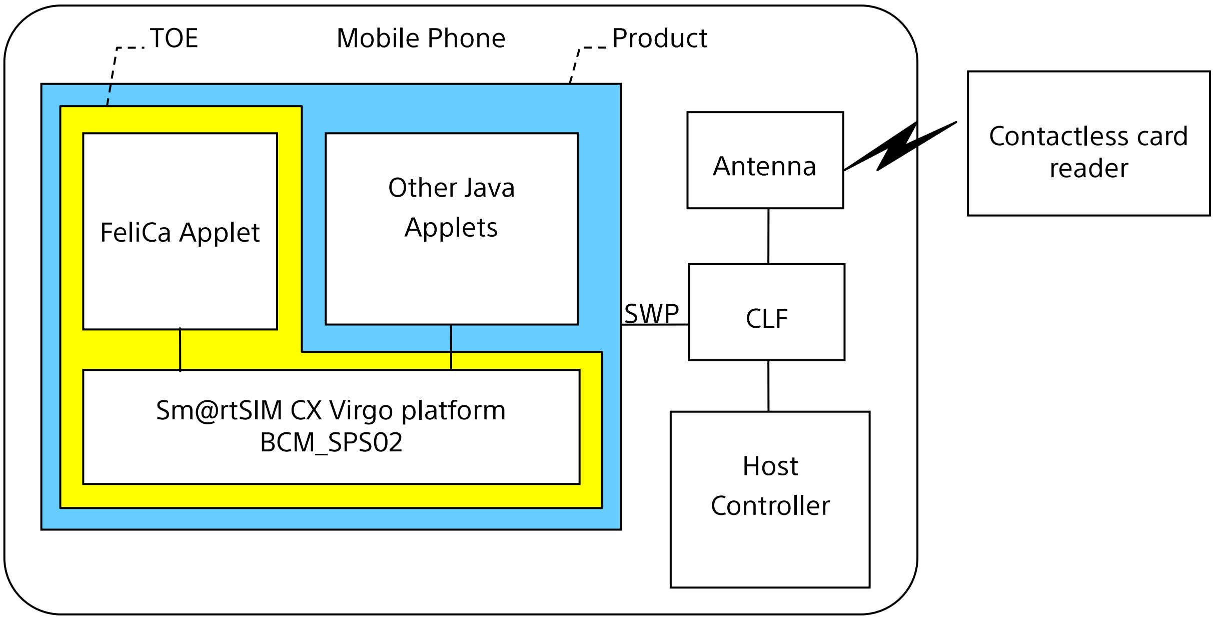


Figure 2: TOE physical scope

The components of the TOE are explained as follows:

- "FeliCa Applet" constitutes the part of the TOE that is responsible for managing and providing access to the Areas and FeliCa Services.
- Sm@rtSIM CX Virgo has a Java Card System which manages and executes applets. It provides APIs for developing applets in accordance with the Java Card specification. Sm@rtSIM CX Virgo has GlobalPlatform packages providing a common interface to communicate with a smart card and manage applications in a secure way according to the GP specifications.

- "BCM_SPS02" is the hardware platform of the TOE. The hardware platform provides the following security functionality, DES[1], AES, RNG and CRC. The hardware platform also includes security detectors, sensors and circuitry to protect the TOE.

The SWP interface enables the exchange of FeliCa commands, which are processed by the FeliCa Applet. The CLF chip, the Host controller and the antenna are out of scope of the TOE. The CLF chip provides contact and contactless communication among the TOE, the contactless card reader and the host controller.

All components of the TOE including guidance manuals are listed in the following section.

2.2. Delivery

The TOE delivery items are listed in the following table:

Table 3: TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	Broadcom BCM_SPS02	0x1C404230	Smartcard integrated circuit
Software	BCM_SPS02 Secure Firmware	002.030	Embedded in hardware
	G+D Mobile Security Sm@rtSIM CX Virgo V5.0	0.31.0	Embedded in hardware
	Mobile FeliCa Applet	615100	An application on Java card platform.
Manuals	Mobile FeliCa Applet User's Manual	1.40	Document
	FeliCa Card User's Maual	1.02	Document
	Mobile FeliCa Appet Personalization Specification	1.20	Document
	Individual data for Issuer	1.20	Document
	Product Acceptance Procedure	1.10	Document
	Security Reference Manual – Group Key Generation (AES 128bit)	1.21	Document
	Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)	1.21	Document
	Security Reference Manual – Package Generation (AES 128bit)	1.21	Document

[1] Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform does not implement any Security Functional Requirement using DES operation. Therefore, the functionality implemented from using DES is part of the evaluation but the security in this functionality is not claimed.

Delivery item type	Identifier	Version	Medium
	Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21	Document
	Security Reference Manual – Group Service Key & User Service Key Generation	1.00	Document
	Security Reference Manual – Mutual Authentication & Packet Cryptography	1.00	Document
	Security Reference Manual – Issuing Package Generation Type2	1.00	Document
	Security Reference Manual – Changing Key Package Generation	1.00	Document
	Security Reference Manual – Changing Key Package Generation Type2	1.00	Document

2.3. Logical scope

The TOE offers the following features:

- it can receive FeliCa commands from the CLF.
- it enables the set-up and maintenance of FeliCa Services by Service Providers
- it enables the use of FeliCa Services (e.g., decrement, cash-back)

The TOE offers the following security features:

- authentication of users (AES or DES[1])
- controlled access to data stored internally in the TOE
- secure communication with the smartcard Reader/Writer (AES and DES[1])
- protection of integrity of data stored internally in the TOE
- anti-tearing and rollback
- protection against excess environment conditions
- protection against information leakage and manipulation
- protection against probing and alteration

The security features are provided partly by the underlying hardware and partly by the Security IC Embedded Software and FeliCa Applet.

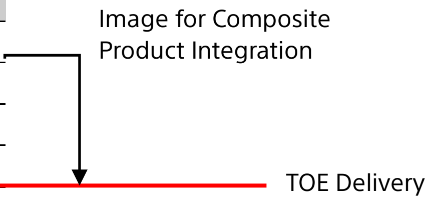
[1] Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform does not implement any Security Functional Requirement using DES operation. Therefore, the functionality implemented from using DES is part of the evaluation but the security in this functionality is not claimed.

2.4. Lifecycle

The lifecycle of the TOE is explained using the smartcard lifecycle as defined in “Security IC Platform Protection Profile with Augmentation Packages” [BSI-PP-0084], which includes the phases listed in the following table:

Table 4: Phases of the TOE lifecycle

Phase	Description
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage



The TOE is delivered at the end of **Phase 4**.

An explanation of each phase of the TOE lifecycle follows:

Phase 1 and Phase 2 compose the product development: Embedded Software (IC Dedicated Software, OS, Java Card System, other platform components such as Card Manager, Applets) and IC development.

Phase 3 and Phase 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 personalisation prior final use.

Phase 7 is the product operational phase.

2.5. Evaluated configurations

The TOE provides a very flexible access control configuration system that allows the system administrator to choose from several options when creating the services. The administrator may create (i) unprotected files (i.e., public access files), (ii) files that are protected by advanced high-grade encryption and (iii) files that are protected by both advanced high-grade encryption and low-grade encryption. In the above case (iii), the files are practically regarded as being protected by low-grade encryption.

The TOE provides two distinct modes of operation – Advanced and Backward-Compatible – to ensure that the TOE can provide the required level of protection.

In the Advanced operation mode, the TOE is accessed via a channel using advanced high-grade encryption for the protected data, or no encryption for public data.

In the Backward-Compatible operation mode the TOE is accessed via a channel using low-grade encryption for the protected data, or no encryption for public data.

The TOE claims the security functionality in the Advanced operation mode only.

3. Security problem definition

The statement of the security problem describes the assets that the TOE is expected to protect and the security measures that are to be enforced by the TOE or its operational environment.
To this end, the security problem definition (this chapter) identifies and lists the following:

- primary and secondary assets
- the assumptions about the TOE environment
- the organisational security policies with which the TOE is designed to comply.

3.1. Assets

The assets that the TOE is expected to protect are as follows:

- the primary asset of the TOE is the sensitive user data (i.e., data from Users and Service Providers) loaded into the volatile and non-volatile memory
- all assets employed to protect the primary assets are secondary assets (such as cryptographic keys, the applet code, data, and so on).

3.2. Assumptions

A.Process **The TOE is administered in a secure manner after the TOE delivery.**

The customer is responsible for the secure administration of both the TOE and the protected storage. It is assumed that security procedures are used between delivery of the TOE by the TOE manufacturer and delivery to the customer, to maintain the confidentiality and integrity of the TOE and its manufacturing and test data (to prevent any possible copying, modification, retention, theft for unauthorised use). This means that assets after TOE delivery are assumed to be protected appropriately.

3.3. Organisational security policies

To record the security problem definition in terms of policies, we state what protection the TOE shall afford to the user, as follows:

P.Confidentiality **The TOE shall provide the means to protect the confidentiality of the stored assets.**

The TOE shall have security measures that can protect the stored user data from unauthorised disclosure. We do not expect the TOE to enforce these security measures on any or all user data, but those measures shall be available when the user decides that they shall be used to protect the user data.

P.Integrity **The TOE shall provide the means to protect the integrity of the stored assets.**

The integrity of the stored assets shall be protected during operation in a hostile environment. The possibility of attacks trying to alter specific data cannot be discounted but, for a contactless smart card, there are other considerations that already make the integrity a prime concern, such as the very real possibility of power cut-off at any point during processing. To ensure the integrity, the TOE shall have security measures that can protect the stored user data from unauthorised modification and destruction.

P.TransferSecret **The TOE shall provide the means to protect the confidentiality of assets during transfer from outside of the TOE.**

At the user's discretion, user data that is sent or received through the communication channel needs protection from unauthorised disclosure. The TOE shall provide the capabilities to provide such measures.

P.TransferIntegrity **The TOE shall provide the means to protect the integrity of assets during transfer from outside of the TOE.**

The integrity of the messages on the communication channel shall take into account both the possibility of benign interference and malicious interference in various forms, such as: RF noise, spikes in the field, short removals of the field, ghost transmissions, replay, and injection of data into the channel. The TOE shall provide the means to ensure the integrity of user data transferred.

P.Configure **The TOE shall provide the means to configure the level of protection for each of the assets.**

The TOE is a tool to be used by the user in a system that shall implement specific business rules. The TOE may not assume the level of protection required for any asset. The TOE shall provide the means for the level of protection to be specified explicitly by the user for each asset.

P.Keys **The keys generated for TOE use shall be secure. The keys for use by the TOE shall be generated and handled in a secure manner.**

Some keys for TOE use are generated outside of the TOE, by the supporting system in a controlled environment. This system shall check that all such keys are suitably secure by, for example, weeding out weak keys. The secure keys are then loaded into the TOE. The process of key generation and management shall be suitably protected and shall occur in a controlled environment.

P.NoDebugIF **The TOE shall not implement the means to export any information for debugging purposes to outside of the TOE.**

The TOE shall be built to provide only the capabilities for its genuine purpose. No test or debug features shall remain in the TOE. Such test or debug features shall be completely disabled, i,e,, not even enabled with restricted privileges.

4. Security objectives

This chapter describes the security objectives for the TOE and the TOE environment in response to the security needs identified in Chapter 3, "Security problem definition".
Security objectives for the TOE are to be satisfied by technical countermeasures implemented by the TOE.
Security objectives for the environment are to be satisfied either by technical measures implemented by the IT environment, or by non-IT measures.

4.1. TOE security objectives

The following TOE Security Objectives have been identified for the TOE, as a result of the discussion of the Security Problem Definition. Each objective is stated in **bold type** font. It is followed by an application note, in regular font, which provides additional information and interpretation.

O.AC **The TOE shall provide a configurable access control system to prevent unauthorised access to stored user data.**

The TOE shall provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for in a configurable and deterministic manner. This objective combines all aspects of authentication and access control.

O.SC **The TOE shall provide configurable secure channel mechanisms for the protection of user data when transferred between the TOE and an outside entity.**

The TOE receives and sends user data over a wireless interface, which is considered easy to tap and alter. Therefore, the TOE shall provide mechanisms that allow the TOE and an external entity to communicate with each other in a secure manner. The secure channel mechanisms shall include protection of the confidentiality and integrity of the transferred user data.

O.NoDebugIF **The TOE shall provide a protection mechanism against abuse of the debugging interface.**

The TOE shall protect from leakage and manipulation of information through any debugging interfaces, such as abuse of test commands. All components of the TOE, i.e., FeliCa Applet, the underlying platform (including the Java Card OS and the hardware) shall prevent the debugging interfaces from being enabled.

4.2. TOE operational environment security objectives

This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in Chapter 3, "Security problem definition". Each objective is stated in bold type font; it is followed by an application note, in regular font, which supplies additional information and interpretation.

OE.Keys **The handling of the keys outside of the TOE shall be performed in accordance to the specified policies.**

Specific keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and control of the keys shall be performed in strict compliance to the specific policies set for such operations.

OE.Process **The handling of the TOE after the TOE delivery shall be performed in a secure manner**

In the TOE environment, confidentiality and integrity of the TOE and its manufacturing and test data shall be maintained by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the customer.

4.3. Security objectives rationale

This section demonstrates the suitability of the choice of security objectives and that the stated security objectives counter all identified, policies, or assumptions.

The following table maps the security objectives to the security problem, which is defined by the relevant, policies, and assumptions. This illustrates that each policy or assumption is covered by at least one security objective.

Table 5: Assumptions or Policies Security Objectives

Policy	Policy text	Objective	Objective text
A.Process	The TOE is administered in a secure manner after the TOE delivery.	OE.Process	The handling of the TOE after the TOE delivery shall be performed in a secure manner.
P.Confidentiality	The TOE shall provide the means to protect the confidentiality of the stored assets.	O.AC	The TOE shall provide a configurable access control mechanism to prevent unauthorised access to stored user data.
P.Integrity	The TOE shall provide the means to protect the integrity of the stored assets.	O.AC	The TOE shall provide an access control mechanism to protect integrity of the stored user data from unauthorised access.

Policy	Policy text	Objective	Objective text
P.TransferSecret	The TOE shall provide the means to protect the confidentiality of assets during transfer to and from the TOE.	O.SC	The TOE shall provide configurable secure channel mechanisms for the protection of user data transferred between the TOE and an external entity.
P.TransferIntegrity	The TOE shall provide the means to protect the integrity of assets during transfer to and from the TOE.	O.SC	The TOE shall provide a configurable secure channel mechanism for the protection of user data transferred between the TOE and an external entity.
P.Configure	The TOE shall provide the means to configure the level of protection for each of the assets.	O.AC	The TOE shall provide a configurable access control mechanism to prevent unauthorised access to stored user data.
P.Keys	The keys generated for the use of the TOE shall be secure. The keys for the use of the TOE shall be generated and handled in a secure manner.	OE.Keys	The handling of the keys outside of the TOE shall be performed in accordance with the specified policies.
P.NoDebugIF	The TOE shall not implement the means to export any information for debugging purposes to outside of the TOE.	O.NoDebugIF	The TOE shall provide a protection mechanism against abuse of the debugging interface.

The following explanation shows that the chosen security objectives are sufficient and suitable to address the identified, assumptions, and policies.

The policies for the TOE call for protection of user data when stored in the TOE and when in transit between the TOE and an external security product. Also, the policies require that the system used for protection of the assets when stored within the TOE be flexible and configurable. These policies are upheld by defining the following two objectives for the TOE: O.AC and O.SC. The O.AC objective makes sure that the TOE implements an access control system that protects the stored user data from illegal access (as required by the P.Confidentiality policy), while providing the capability to configure the access rules and operations for the authorised users (as required by the P.Configure policy). The O.SC objective provides a secure channel that shall be established between the TOE and an external entity; this secure channel shall protect all transmitted user data from disclosure (as required by P.TransferSecret) and from integrity errors, whether as a result of an attack or environmental conditions (such as loss of power), as required by P.TransferIntegrity.

The policy P.Integrity requires that user data shall be protected from integrity errors when stored in the

TOE. It is upheld by two objectives for the TOE: O. AC. The O.AC objective provides the access control system, which allows only authorised users to access stored user data and protects the integrity of stored user data from illegal access.

The policy P.NoDebugIF requires that all debug features are completely disabled, and the O.NoDebugIF objective provides protection against abuse of debug features.

The policy for the environment that requires secure generation and handling of keys, P.Keys, is similarly directly translated into the objective for the environment OE.Keys for the secure handling of keys and generation of secure keys.

The security problem defined for the TOE calls for the protection of assets by the TOE. There are several security measures implemented by the TOE itself, but the proper administration of the TOE's security measures and proper handling of the TOE are essential, as stated in the A.Process assumption. That assumption is upheld by defining the objective for the environment OE.Process, which ensures that secure procedures are used by the TOE environment to ensure both the security of the assets and the proper administration of the TOE security measures.

The following table maps all security objectives defined in this Security Target to the relevant, policies, and assumptions. This illustrates that each security objective covers at least one policy or assumption

Table 6: Security objectives versus Assumptions or Policies

Policy	Objective
O.AC	P.Confidentiality
	P.Integrity
	P.Configure
O.SC	P.TransferSecret
	P.TransferIntegrity
O.NoDebugIF	P.NoDebugIF
OE.Keys	P.Keys
OE.Process	A.Process

5. Security requirements

IT security requirements include the following:

- TOE security functional requirements (SFRs)
  That is, requirements for security functions such as information flow control, identification and authentication.
- TOE security assurance requirements (SARs)
  Provide grounds for confidence that the TOE meets its security objectives (such as configuration management, testing, vulnerability assessment.)
- This chapter discusses these requirements in detail. It also explains the rationales behind them, as follows:
- Security functional requirements rationale
- Security assurance requirements rationale

5.1. TOE security functional requirements

The TOE Security Objectives result in a set of Security Functional Requirements (SFRs).
About the notation used for Security Functional Requirements (SFRs):

- The refinement operation is used in many cases, to make the requirements easier to read and understand. All these cases are indicated and explained in footnotes.
- Selections appear in ***Italic bold*** font.
- Assignments appear in **Tahoma bold** font.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **User and Administrator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **Polling, Requests, Public_read, Public_write, Echo Back, Reset Mode** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **Polling, Requests, Public_read, Public_write, Echo Back, Reset Mode** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **all authentication mechanisms**.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Service Access Policy** on **the following:**

- **Subjects:**
  - **User**
  - **Administrator**
- **Objects: Files**
- **Operations:**
  - **Authentication**
  - **Read**
  - **Write**
  - **Reset Mode**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Service Access Policy** to objects based on the following:

- **Subjects:**
  - **User with security attribute authentication**
  - **Administrator with security attribute authentication**
- **Objects: Files with security attributes ACL**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **A Subject can do this operation on an Object when: the Subject is successfully authenticated, and the operation is listed in the Object's ACL.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **no additional explicit rules.**

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy** to restrict the ability to ***perform any operation*** on the security attributes **authentication and ACL** to **Administrator**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

management of security attributes.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***another trusted IT product*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **no functions**.

The following two SFRs are CC Part 2 extended and defined in the Protection Profile [BSI-PP-0084]. Definitions of these SFRs are described in [BSI-PP-0084].

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 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 **No debug features shall be available**.

FMT_LIM.2 Limited availability

FMT_LIM.1.1 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 **No debug features shall be available**.

5.2. TOE security assurance requirements

The TOE Security Assurance Requirements (SARs) consist of the requirements defined by EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

5.3. Security functional requirements rationale

The following table presents both the rationale for choosing specific Security Functional Requirements (SFRs) and how those requirements correspond to the specific Security Objectives:

Table 7: TOE Security Functional Requirements versus Security Objectives

Objective	TOE Security Functional Requirements
O.AC	- FMT_SMR.1 “Security roles” - FIA_UID.1 “Timing of identification” - FIA_UAU.1 “Timing of authentication” - FIA_UAU.4 “Single-use authentication mechanisms” - FDP_ACC.1 “Subset access control - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.1 “Management of security attributes” - FMT_SMF.1 “Specification of Management Functions”
O.SC	- FTP_ITC.1 “Inter-TSF trusted channel”
O.NoDebugIF	- FMT_LIM.1 ” Limited capabilities - FMT_LIM.2 “Limited availability”

The objective O.AC is achieved through inclusion of the SFRs FDP_ACC.1 and FDP_ACF.1, which together specify the access control policy. The operation of the access control system is supported by the SFR FIA_UAU.4 to make sure that unique authentication sessions shall be used every time. The SFRs FIA_UID.1 and FIA_UAU.1 complement the access control system operation by allowing very specific functions to be used without mutual authentication. The SFRs FMT_SMR.1 and FMT_MSA.1 in conjunction with the SFR FMT_SMF.1 allow for the implementation of a flexible, configurable access control system and specify the roles that shall be allowed to utilise the access control system configuration capabilities. The presented combination of the SFRs provides an access control system that, as required by the O.AC objective, is precisely specified, allows for very specific exceptions, and supports very flexible configuration.

The objective O.SC is directly realised through the requirement for the secure channel SFR FTP_ITC.1 between the TOE and the external device. The objective O.NoDebugIF is directly realised through the SFRs FMT_LIM.1 and FMT_LIM.2, which together limit the capability and availability of all debug features.

The following table presents the list of the SFRs with the associated dependencies:

Table 8: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
FMT_SMR.1	Security roles	FIA_UID.1	Included
FIA_UID.1	Timing of identification	None	
FIA_UAU.1	Timing of authentication	FIA_UID.1	Included
FIA_UAU.4	Single-use authentication mechanisms	None	
FDP_ACC.1	Subset access control	FDP_ACF.1	Included
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	Included Not satisfied
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Included (FDP_ACC.1) Included Included

ID	SFR	Dependencies	Notes
FMT_SMF.1	Specification of Management Functions	None	
FTP_ITC.1	Inter-TSF trusted channel	None	
FMT_LIM.1	Limited capabilities	FMT_LIM.2	Included
FMT_LIM.2	Limited availability	FMT_LIM.1	Included

The SFR “FMT_MSA.3 Static attribute initialisation” is a dependency for the SFR FDP_ACF.1. In the TOE, however, the security attributes are always explicitly set and the notion of “default value” for a security attribute simply does not exist. The security attributes are always set explicitly by the Administrator to a value appropriate for each asset without exception, so it is our opinion that the system is no less secure in the absence of the SFR FMT_MSA.3. Therefore, there is no need to include the SFR FMT_MSA.3 in the ST.

5.4. Security assurance requirements rationale

- To meet the assurance expectations of customers, the assurance level EAL4 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 are chosen. The assurance level of EAL4 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to protect high value assets. Explanation of the security assurance component ALC_DVS.2 and AVA_VAN.5 follows:
- ALC_DVS.2 Sufficiency of security measures:
  This Security Target selects ALC_DVS.2 instead of ALC_DVS.1 because it verifies the security measures that provide the necessary level of protection to maintain the confidentiality and integrity of the TOE and its user data.
- AVA_VAN.5 Highly resistant:
  The TOE might be in danger of high-level attacks such as those it might encounter in a university laboratory. Therefore, AVA_VAN.5 is augmented to confirm that TOE has a high level of resistance against such attacks.

6. TOE Summary Specification

This chapter describes the TOE summary specification by summarising the architectural design.
The TOE summary specification includes the following:

- TOE summary specification rationale
  Describe how the TOE meets each SFR.

6.1. TOE summary specification rationale

This section describes how the TOE is intended to comply with the Security Functional Requirements. The TOE must satisfy the requirements for secure storage, transfer and management of user data. Therefore, the TOE is implemented as a software platform on a secure chip.

The TOE includes the functions for creating secure containers (Area and FeliCa Service, also referred to as Files in section 5.1) and management of the security attributes of those containers. The TOE provides functions for populating the containers with user data in various ways that are functionally required by the customers, retrieval of the data or updating the data in situ.

The transfer of data during the operations on secure containers performed in a secure way, where the external security product and the TOE are mutually authenticated before the operation and then connected with each other via an encrypted session. The session allows the bilateral transfer of data in a manner protected from eavesdropping and alteration.

In compliance with the requirements, the TOE also provides a capability for the unsecured storage and retrieval of user data. The security attributes can be set up in such a manner that data can be made read only by any unauthenticated user, but can only be updated by an authenticated user/administrator, allowing for a flexible and fully-configurable access-control system.

- “FMT_SMR.1 Security roles” is met by providing an ability to distinguish between the roles of “Administrator” and “User”, where the different roles allow the subject to execute different kinds of operations. The TOE has built-in rules for distinguishing between the operations and required security attributes for various TOE and TSF data. The Administrator of the TOE specifies the security attributes for the TOE data and the TSF data. The role of the authenticated entity is assigned after the authentication has succeeded (in accordance with the requirements of FDP_ACC.1).
- “FIA_UID.1 Timing of identification” and “FIA_UAU.1 Timing of authentication” are intended to provide a possibility to configure a publically-accessible container. The TOE provides access to such specifically-configured containers based on the security attributes of the container. The container must be configured, by the Administrator, with special attributes that allow the specified mode of access before authentication.
- The TOE uses random numbers in the authentication mechanism to comply with the “FIA_UAU.4 Single-use authentication mechanisms” requirement; these numbers are generated by the Security IC Embedded Software. The random numbers are generated anew each time the authentication is started, according to the requirements of FDP_ACC.1, and are discarded each time the TOE exits the

authenticated state.

- “FDP_ACC.1 Subset access control” and “FDP_ACF.1 Security attribute based access control” are satisfied by providing an access-control mechanism based on the attributes of security containers. The TOE grants access to the TOE data stored in the containers, based on the security attributes during the authentication phase. If the correct security attributes are used during the authentication for the requested mode of access to the specified container, the requested mode of access is granted. The granularity of access control is based on a single mode of access and a single container. A request for access may combine attributes for several containers and several modes of access in a single request. The security attributes are assigned to the containers by the Administrator. The TOE allows the Administrator to access the security attributes for configuration purposes, based on the security attributes (in accordance with FMT_MSA.1 and FMT_SMR.1).
- “FMT_MSA.1 Management of security attributes” and “FMT_SMF.1 Specification of Management Functions“ are met by providing configuration capabilities accessible to the Administrator. The configuration capabilities are granted based on the security attributes and allow the changing of these security attributes to new values after successful authentication and privilege verification (in accordance with FDP_ACC.1 and FMT_SMR.1).
- “FTP_ITC.1 Inter-TSF trusted channel” requires the secure channel – this is provided by the TOE using the AES algorithm, which is calculated by the hardware, for encrypting and authenticating data that is sent or received through the link.
- “FMT_LIM.1 Limited capabilities“ and “FMT_LIM.2 Limited availability” are satisfied by not implementing any test commands that prevent abuse of test functionality. The test functionality provided by the hardware is not available to the user after Phase 3 IC manufacturing as defined in the Protection Profile [BSI-PP-0084]. The test functionality provided by the Java Card OS and the FeliCa Applet is not available after Phase 1 IC embedded software development.

7. Glossary and references

This chapter explains the terms, definitions and literary references (bibliography) used in this document. The list entries in this chapter are ordered alphabetically.

7.1. Terms and definitions

The following list defines the product-specific terms used in this document:

- **Administrator**
  The entity responsible for personalisation of the TOE. In most cases, this is a representative of a Service Provider. Synonymous with Personaliser. See also User.
- **Area**
  A part of the FeliCa file system. An area is similar to a directory in a general file system.
- **Contactless card reader**
  A contactless smartcard Reader/Writer that interacts with the TOE.
- **FeliCa file system**
  The structure of data in the TOE.
- **FeliCa Service**
  The part of the FeliCa file system that contains information that stipulates the method of access to data. In this context, a service is similar to a file in a general file system.
- **Mobile phone holder**
  A person who uses User Service.
- **Personaliser**
  See Administrator.
- **Service Provider**
  An entity that provides a specific service to a User.
- **User**
  For this product, an entity using any FeliCa Service that a personalised TOE offers. See also Administrator.
- **User Service**
  A specific service to a Mobile Phone holder that is made technically possible by the TOE. Each User Service is provided by a Service Provider to a Mobile Phone holder. An example of a User Service is a virtual train ticket or an electronic purse.

7.2. Acronyms

The following table lists and defines the product-specific abbreviated terms (acronyms) that appear in this document:

Table 9: Abbreviated terms and definitions

Term	Definition
ACL	Access Control List
CLF	Contactless Front-End
ID	Identification
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SWP	Single Wire Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions

7.3. Bibliography

The following list defines the literature referenced in this document:

[AAPS] “Common Criteria Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards”, Version 2.9, May 2013

[BSI-PP-0084] "Security IC Platform Protection Profile with Augmentation Packages", Version 1.0, January 2014

[CC] "Common Criteria for Information Technology Security Evaluation", Version 3.1 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1, Revision 4, September 2012

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 4, September 2012

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 4, September 2012

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 4, September 2012

[ST-Platform] "Sm@rtSIM CX Virgo v5.0 Security Target"

Security Target lite for Mobile FeliCa Applet on Sm@rtSIM CX Virgo platform

Version 1.51 Public
No. MAP01-ASEP01-E01-51
September 8, 2017

FeliCa Networks, Inc