Mobile FeliCa Applet Protection Profile

Version 1.0
No. FN15-F007-E01-00

FeliCa Networks, Inc.

Introduction

This document is the Protection Profile for Mobile FeliCa Applet and Mobile FeliCa Crypto Library.

Contents

1. PP Introduction

This document is the PP for Common Criteria evaluation of Mobile FeliCa Applet and Mobile FeliCa Crypto Library under the FeliCa Approval for Security and Trust scheme [FAST].
This PP 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 0 "Glossary and references".

1.1. PP Reference

This section provides the information necessary to identify and control this PP.

Table 1: PP identification

PP attribute	Value
Name	Mobile FeliCa Applet Protection Profile
Version	1.0
Reference	FN15-F007-E01-00
Issue Date	05 July 2023
Provided by	FeliCa Networks, Inc.

1.2. TOE Description

The TOE is an integrated circuit with an embedded smartcard operating system with Mobile FeliCa Applet and Mobile FeliCa Crypto Library.

The assumed usage of the TOE is a stored fare card, a post-pay card, seasonal ticket card and one-day ticket card for public transportation. To take a train, a customer just taps the card to the ticket gate and the fare is automatically deducted from the card. The TOE can be used not only for trains but also subways and buses.

The TOE can be also used for other purposes such as e-money, e-ticket, ID card, and so on. The e-money services allow a person to buy something quickly at kiosk, shopping malls, vending machines, and Internet. A person can enter an event hall or his/her office by touching the e-ticket or ID to gates of facilities.

The following figure illustrates the physical scope of the TOE, which is indicated in yellow, and the product, which is indicated in blue:

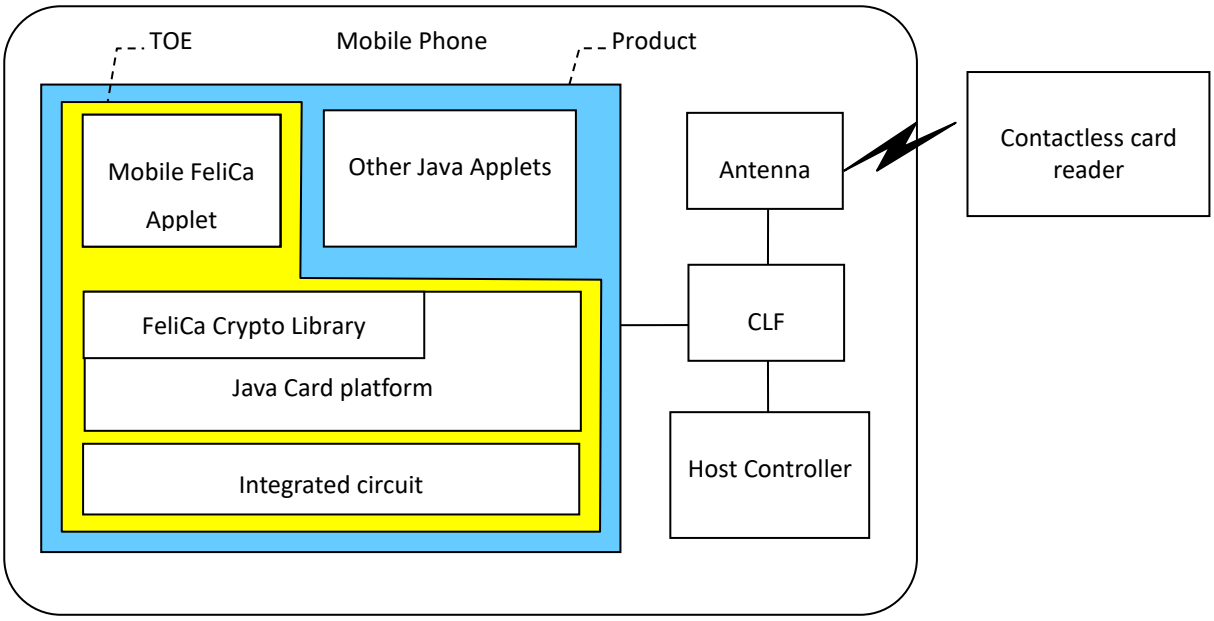


Figure 1: TOE physical scope

The components of the TOE are explained as follows:

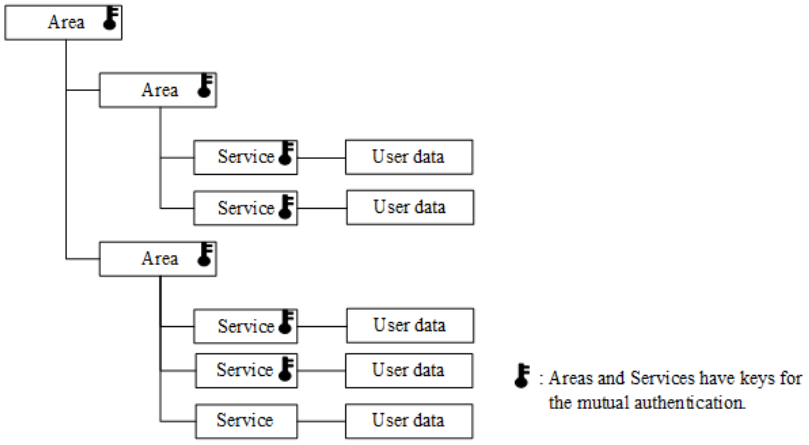
- Mobile FeliCa Applet constitutes the part of the TOE that is responsible for managing and providing access to the Areas and FeliCa Services.
- Java Card Platform has a Java Card System which manages and executes applets. It provides APIs for developing applets in accordance with the Java Card specification. Java Card Platform 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. Java Card Platform shall be certified by EMVCo, or Common Criteria against Java Card System PP [JC-PP].

- Integrated circuit 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. Integrated circuit shall be certified by EMVCo, or Common Criteria against [BSI-PP-0084].

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 2). The security measures of the TOE aim at protecting the access to the Areas and FeliCa Services (including associated user data), and maintaining the confidentiality and integrity of assets such as the user data and Access Key.

A FeliCa Service has the Service Attribute that defines the type of access to the user data and the security condition to access the user data. If a FeliCa Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the FeliCa Service. When the authentication is successfully completed, the TOE allows the external entity to access the user data according to the Service Attribute. This



mechanism prevents unauthorised access to the user data.

[1] The functionality implemented from using DES is part of the evaluation but the security in this functionality is not claimed.

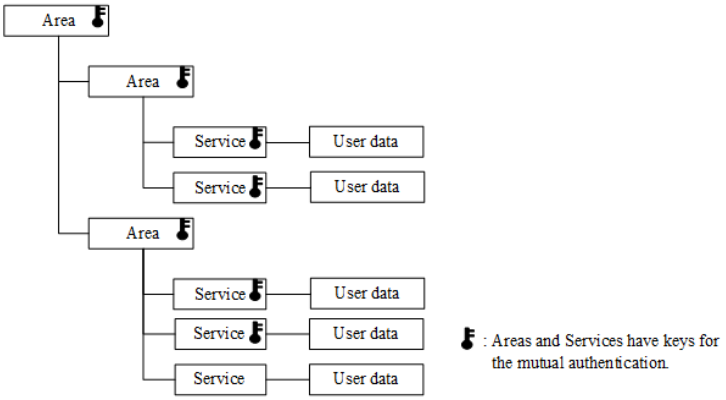


Figure 2: The FeliCa file system

An Area defines the management operation of the Area and the FeliCa Service. The external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Area. When the authentication is successfully completed, the TOE allows the external entity to perform the management operation (e.g., setting Service Attribute).

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].

The TOE offers the following features:

- it can send and receive the FeliCa command and the FeliCa response respectively with the CLF.

The TOE offers the following security features:

- mutual authentication between the external entity and the TOE
- three pass authentication based on ISO/IEC 9798-2
- management of FeliCa Services (e.g., setting Service Attribute)
- controlled access to the user data stored internally in the TOE
- trusted communication channel between the external entity and the TOE
- protection of confidentiality and/or integrity of assets stored internally in the TOE
- anti-tearing and rollback mechanism
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration
- prevent abuse of function
- support of unique identification of the TOE

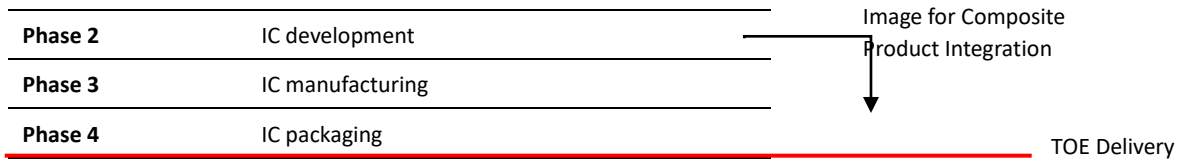
The security features are provided partly by the underlying hardware and partly by the Security IC Embedded Software and FeliCa Applet.

1.3. 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 2: 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.

1.4. Available non-TOE hardware/software/firmware

The TOE is designed to operate on NFC forum compliant platform. 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 respectively.

1.5. 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.

2. Conformance Claims

This chapter describes the conformance claims.

2.1. CC Conformance Claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (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 PP claims the following conformances:

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

2.2. PP Claim

This PP does not claim conformance to any other PP.

This PP requires strict conformance to the PP and ST claiming conformance to this PP.

2.3. Package Claim

The minimum level of assurance is:

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

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 threats to be countered by the TOE
- 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 user data stored in the TOE
- all the assets employed to protect confidentiality and/or integrity of the primary assets are secondary assets

Application note: Details of secondary assets are described FeliCa Security Analysis [FASA].

3.2. Threats

This section describes threats. The threats shall be counted by the TOE or/and its operational environment.

T.Logical_Attack

In the operational environment after issuing the TOE, an attacker may try to (i) disclose the assets of the TOE or (ii) alter the assets of the TOE without authentication.

T.Comm_Attack

An attacker may try to (i) disclose the assets that is sent or received through the communication channel or (ii) alter the messages on the communication channel.

T.Abuse_Func

An attacker may use functions of the TOE which may not be used after TOE delivery in order to (i) disclose or manipulate the assets of the TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE, (iii) manipulate (explore, bypass, deactivate or change) functions of the TOE or (iv) enable an attack disclosing or manipulating the assets of the TOE.

3.3. Organisational security policies

This section describes organisational security policies that apply to TOEs and operational environment.

P. TOE_Auth

TOE shall be able to authenticate the external entities and authenticate itself to the external entities.

P.Configure

The TOE is a tool to be used by the Administrator in a system that shall implement specific business rules. The TOE shall provide the means for the level of the access control to be specified explicitly by the Administrator for each asset.

P.Identification

An accurate identification shall be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

3.4. Assumptions

This section describes assumptions to be addressed in the operational environment of the TOE. These assumptions need to be true for the effective security functionality of the TOE.

A.Keys

Access Keys for TOE use are generated outside 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. Access Keys are then handled correctly without misoperation. The process of key generation and management shall be suitably protected and shall be performed in a controlled environment.

A.Process

It is assumed that security procedures are used after delivery of the TOE by the TOE manufacturer up to delivery to the customer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

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 be able to authenticate the external entities. And the TOE shall provide the means of controllable limited 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.Auth

The TOE shall be able to authenticate the external entities and authenticate itself to external entities.

O.Configure

The TOE shall provide the means of the access control to be specified explicitly set by the Administrator.

O.Comm_Attack

The TOE receives and sends the assets over a contactless interface and a contact interface, which is considered easy to eavesdrop or tap and alter. Therefore, the TOE shall provide secure channel that allow the TOE and an external entity to communicate with each other in a secure manner. The secure channel shall protect the confidentiality and integrity of the transferred assets.

O.Abuse_Func

The TOE shall prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical assets of the TOE, (ii) manipulate critical assets of the TOE, (iii) manipulate PT Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

O.Identification

The TOE shall provide the means to store Initialisation Data in its non-volatile memory. Initialisation Data (or parts of them) are used for TOE identification.

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. 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

Access Keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and handling of the keys shall be performed in a secure manner.

OE.Process

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

Table 3: Assumptions, Threats or Policies versus Security Objectives defined in the PP

Threat, policy or assumption	Objective
T.Logical_Attack	O.AC
T.Comm_Attack	O.Comm_Attack
T.Abuse_Func	O.Abuse_Func
P. TOE_Auth	O.Auth
	OE.TOE_Auth
P.Configure	O.Configure

Threat, policy or assumption	Objective
P.Identification	O.Identification
A.Keys	OE.Keys
A.Process	OE.Process

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

The O.AC objective makes sure that the TOE can authenticate the external entities and implements an access control system that protects the stored assets from unauthorised access. Thus, T.Logical_Attack threat is mitigated if the objective is valid.

The O.Comm_Attack objective provides a secure channel that shall be established between the TOE and an external entity; this secure channel shall protect all the transferred assets from disclosure and from integrity errors, whether as a result of an attack or environmental conditions (such as loss of power). Thus, the T.Comm_Attack threat is mitigated if the objective is valid.

O.Abuse_Func objective (refer to Table 3) directly corresponds to the description of the threat. It is clear from the description of the objective, that the corresponding threat is removed if the objective is valid.

The P.TOE_Auth policy is covered by the O.Auth objective describing the proving part of the authentication and the OE.TOE_Auth operational environment the verifying part of the authentication. Thus, the P.TOE_Auth policy is covered by the objectives.

The O.Configure objective provides the capability to configure the access rules and operations for the authorised User and Administrator. Thus, the P.Configure policy is covered by the objective.

The O.Identification objective requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment the production environment shall support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. Therefore, the P.Identification policy is covered by this objective, as far as organisational measures are concerned.

The OE.Keys and the OE.Process operational environments directly correspond to the description of the A.Keys and A.Process assumptions respectively, thus these assumptions are met.

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.
- Selections appear in ***Italic bold*** font.
- Assignments appear in **bold** font.

FIA_UID.1Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **the authentication mechanisms shown in Table 4**.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide **the list of multiple authentication mechanisms shown in Table 4** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to **the rules describing how the multiple authentication mechanisms provide authentication shown in Table 4.**

Table 4: Service Access Policy

Subject	Security attribute Authentication status
Three pass mutual authentication	If a FeliCa Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the FeliCa Service via the contactless or the contact interface.
Two pass mutual authentication	If a FeliCa Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the FeliCa Service via the contact interface.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

- **Subjects: subjects shown in Table 5**
- **Objects: objects shown in Table 5**
- **Operations: operations shown in Table 5**

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

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

- **Subjects: subjects shown in Table 5**
- **Objects: objects shown in Table 5**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 5.**

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 Table 5.**

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.**

Table 5: Service Access Policy

Subject	Security attribute Authentication status	Object	Security attribute ACL	Operation
Process representing User	Not authenticated	User data file	Read only, Authentication not required	Read
			Read/Write, Authentication not required	Read or Write
	Successfully authenticated with the Access Key corresponding to the FeliCa Service	User data file	Read only, Authentication with the Access Key corresponding to the FeliCa Service required	Read
			Read/Write, Authentication with the Access Key corresponding to the FeliCa Service required	Read or Write

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy** to restrict the ability to **set** on the security attributes **ACL** to **Administrator**.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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 three 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

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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:

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

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:

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the **test process before TOE Delivery** with the capability to store **Initialisation Data** in the **non-volatile memory**.

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 6: TOE Security Functional Requirements versus Security Objectives

Objective	TOE Security Functional Requirements
O.AC	- FIA_UID.1 “Timing of identification”
	- FIA_UAU.1 “Timing of authentication”
	- FIA_UAU.4 “Single-use authentication mechanisms”
	- FIA_UAU.5 “Multiple authentication mechanisms”
	- FDP_ACC.1 “Subset access control
	- FDP_ACF.1 “Security attribute based access control”
O.Auth	- FIA_UID.1 “Timing of identification”
	- FIA_UAU.1 “Timing of authentication”
	- FIA_UAU.4 “Single-use authentication mechanisms”
	- FIA_UAU.5 “Multiple authentication mechanisms”
	- FTP_ITC.1 “Inter-TSF trusted channel”
O.Configue	- FMT_SMR.1 “Security roles”
	- FMT_MSA.1 “Management of security attributes”
	- FMT_SMF.1 “Specification of Management Functions”
O.Comm_Attack	- FTP_ITC.1 “Inter-TSF trusted channel”
O.Abuse_Func	- FMT_LIM.1 “Limited capabilities”
	- FMT_LIM.2 “Limited availability”
O.Identification	- FAU_SAS.1 “Audit storage”

The objective O.AC is achieved through 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 and SFR_UAU.5 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 authentication.

The objective O.Auth is achieved by the SFRs FTP_ITC.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.1 and FIA_UAU.1 which provide mutual authentication on the secure channel between the TOE and the external entity

The objective O.Configure is achieved by 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 objective O.Comm_Attack is directly realised through the requirement for the secure channel the SFR FTP_ITC.1 between the TOE and the external device.

The objective O.Abuse_Func is achieved by the SFRs FMT_LIM.1 and FMT_LIM.2 because the limitation of availability and capability of functions after the TOE delivery prevents an attacker from abusing functions.

The objective O.Identification is achieved by the SFR FAU_SAS.1. Initialisation Data (or parts of them) are used for TOE identification. The technical capability of the TOE to store Initialisation Data is provided according to the SFR FAU_SAS.1.

Application note: O.AC, O.Auth, O.Configue and O.Comm_Attack are supported by the FeliCa specific cryptographic protocols implemented in FeliCa Crypto Library. The packages for the FeliCa specific cryptographic protocols are defined in the Chapter 6 Package “FeliCa Crypto Library”.

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

Table 7: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
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	
FIA_UAU.5	Multiple 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_SMR.1	Security roles	FIA_UID.1	Included
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
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 PP.

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. Package “FeliCa Crypto Library”

The chapter defines packages for FeliCa Crypto Library.

The developer of FeliCa Crypto Library and FeliCa Applet shall specify the FeliCa specific cryptographic protocols they implement in the FAST ST template.

The cryptographic security services described in these packages implement the same organizational security policy but in different extend.

P. FeliCa cryptographic operations

The TOE provides FeliCa cryptographic operations for the Mobile FeliCa Applet.

6.1.1. Package “DES1”

The TOE shall provide “FeliCa cryptographic operations DES1 (O.DES1)” as specified below.

O.DES1 FeliCa cryptographic operations DES1

The TOE provides FeliCa cryptographic operations implementing DES1.

The security objective “FeliCa cryptographic operations DES1 (O.DES1)” enforces the organizational security policy P.FeliCa cryptographic operations.

The TOE shall meet the requirement “FeliCa cryptographic operations – DES1” as specified below.

FCS_COP.1/DES1 Cryptographic operation

	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, Or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/DES1	The TSF shall perform **following list of FeliCa specific cryptographic protocols** in accordance with a specified cryptographic protocols **FeliCa specific cryptographic protocols:** **DES1** and cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES1].**	

FCS_CKM.1/DES1 Cryptographic key generation

	Hierarchical to:	No other components.
	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/DES1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FeliCa specific cryptographic protocols: DES1** and specified cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES1]**.

FCS_CKM.4/DES1 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/DES1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: **None**.

The FCS_COP.1/DES1, FCS_CKM.1/DES1 and FCS_CKM.4/DES1 meet the security objective “FeliCa cryptographic operations DES1”.

All the dependencies of the security functional requirements defined in this package are fulfilled within the package.

6.1.2. Package “DES2”

The TOE shall provide “FeliCa cryptographic operations DES2 (O.DES2)” as specified below.

O.DES2 FeliCa cryptographic operations DES2

The TOE provides FeliCa cryptographic operations implementing DES2.

The security objective “FeliCa cryptographic operations DES2 (O.DES2)” enforces the organizational security policy P.FeliCa cryptographic operations.

The TOE shall meet the requirement “FeliCa cryptographic operations – DES2” as specified below.

FCS_COP.1/DES2 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes,
or FDP_ITC.2 Import of user data with security attributes,
Or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/DES2 The TSF shall perform **following list of FeliCa specific cryptographic protocols** in accordance with a specified cryptographic protocols **FeliCa specific cryptographic protocols:**
DES2 and cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES2].**

FCS_CKM.1/DES2 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/DES2 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FeliCa specific cryptographic protocols: DES2** and specified cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES2]**.

FCS_CKM.4/DES2 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/DES2 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: **None**.

The FCS_COP.1/DES2, FCS_CKM.1/DES2 and FCS_CKM.4/DES2 meet the security objective “FeliCa cryptographic operations DES2”.

All the dependencies of the security functional requirements defined in this package are fulfilled within the package.

6.1.3. Package “DES3”

The TOE shall provide “FeliCa cryptographic operations DES3 (O.DES3)” as specified below.

O.DES3 FeliCa cryptographic operations DES3

The TOE provides FeliCa cryptographic operations implementing DES3.

The security objective “FeliCa cryptographic operations DES3 (O.DES3)” enforces the organizational security policy P.FeliCa cryptographic operations.

The TOE shall meet the requirement “FeliCa cryptographic operations – DES3” as specified below.

FCS_COP.1/DES3 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes,
or FDP_ITC.2 Import of user data with security attributes,

Or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/DES3 The TSF shall perform **following list of FeliCa specific cryptographic protocols** in accordance with a specified cryptographic protocols **FeliCa specific cryptographic protocols: DES3** and cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES3].**

FCS_CKM.1/DES3 Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/DES3 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FeliCa specific cryptographic protocols: DES3** and specified cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-DES3]**.

FCS_CKM.4/DES3 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/DES3 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: **None**.

The FCS_COP.1/DES3, FCS_CKM.1/DES3 and FCS_CKM.4/DES3 meet the security objective “FeliCa cryptographic operations DES3”.
All the dependencies of the security functional requirements defined in this package are fulfilled within the package.

6.1.4. Package “AES1”

The TOE shall provide “FeliCa cryptographic operations AES1 (O.AES1)” as specified below.

O.AES1 FeliCa cryptographic operations AES1

The TOE provides FeliCa cryptographic operations implementing AES1.

The security objective “FeliCa cryptographic operations AES1 (O.AES1)” enforces the organizational security policy P.FeliCa cryptographic operations.

The TOE shall meet the requirement “FeliCa cryptographic operations – AES1” as specified below.

FCS_COP.1/AES1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes,
or FDP_ITC.2 Import of user data with security attributes,
Or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AES1 The TSF shall perform **following list of FeliCa specific cryptographic protocols** in accordance with a specified cryptographic protocols **FeliCa specific cryptographic protocols: AES1** and cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-AES1].**

FCS_CKM.1/AES1 Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AES1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FeliCa specific cryptographic protocols: AES1** and specified cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-AES1]**.

FCS_CKM.4/AES1 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/AES1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: **None**.

The FCS_COP.1/AES1, FCS_CKM.1/AES1 and FCS_CKM.4/AES1 meet the security objective “FeliCa cryptographic operations AES1”.
All the dependencies of the security functional requirements defined in this package are fulfilled within the package.

6.1.5. Package “AES2”

The TOE shall provide “FeliCa cryptographic operations AES2 (O.AES2)” as specified below.

O.AES2 FeliCa cryptographic operations AES2

The TOE provides FeliCa cryptographic operations implementing AES1.

The security objective “FeliCa cryptographic operations AES2 (O.AES2)” enforces the organizational security policy P.FeliCa cryptographic operations.

The TOE shall meet the requirement “FeliCa cryptographic operations – AES2” as specified below.

FCS_COP.1/AES2 Cryptographic operation

	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, Or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES2	The TSF shall perform **following list of FeliCa specific cryptographic protocols** in accordance with a specified cryptographic protocols **FeliCa specific cryptographic protocols: AES2** and cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-AES2].**	

FCS_CKM.1/AES2 Cryptographic key generation

	Hierarchical to:	No other components.
	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/AES2	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **FeliCa specific cryptographic protocols: AES2** and specified cryptographic key sizes **as defined for these cryptographic protocols** that meet the following: **specifications for the listed protocols in [FeliCa-Spec-AES2]**.	

FCS_CKM.4/AES2 Cryptographic key destruction

	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/AES2 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following: **None**.

The FCS_COP.1/AES2, FCS_CKM.1/AES2 and FCS_CKM.4/AES2 meet the security objective “FeliCa cryptographic operations AES2”.

All the dependencies of the security functional requirements defined in this package are fulfilled within the package.

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**

  An entity responsible for personalisation of the TOE. In most cases, a Service Provider is a representative example of Administrator.

- **Access Key**

  A key that corresponds to an Area and a Service.

- **Area**

  A part of the FeliCa file system. An area is similar to a directory in a general file system.

- **Card reader**

  A contactless and a contact 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.

- **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 8: 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. Following FAST scheme decisions, newer versions of these documents can be used:

[AAPS] “JIL Application of Attack Potential to Smartcards”, Version 3.2, November 2022.

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

[CC] “Common Criteria for Information Technology Security Evaluation”, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1 Revision 5, April 2017

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1 Revision 5, April 2017

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1 Revision 5, April 2017

[CC CEM] “Common Methodology for Information Technology Security Evaluation”, Version 3.1 Revision 5, April 2017

[FAST]	FeliCa Approval Security and Trust scheme v2.0
[FeliCa-Spec-DES1]	FAST FeliCa Crypto Library Specifications for DES1 v1.0
[FeliCa-Spec-DES2]	FAST FeliCa Crypto Library Specifications for DES2 v1.0
[FeliCa-Spec-DES3]	FAST FeliCa Crypto Library Specifications for DES3 v1.0
[FeliCa-Spec-AES1]	FAST FeliCa Crypto Library Specifications for AES1 v1.0
[FeliCa-Spec-AES2]	FAST FeliCa Crypto Library Specifications for AES2 v1.0

8. Change History

Version	Date	Author
1.0	05 July 2023	FeliCa Networks, Inc.

Mobile FeliCa Applet Protection Profile

Version 1.0

No. FN15-F007-E01-00

05 July 2023

FeliCa Networks, Inc