

Security Target

ST introduction

The reference of this ST is **A14-ST-E01-51** version **1.51**

TOE

The TOE is an IC Platform composed with the FeliCa Crypto Lib and the FeliCa Applet. Designed to meet the security functionality of the Public Transportation IC Card PP (PTPP)

TOE reference

The TOE is referred to as **RC-SA14 Series v1.0**, and is named and uniquely identified by its response to the Polling command sent from a Felica Reader/Write, as follows:

Field	Field	Value
IC	Hardware identifier	0x0200
IC	Hardware version	0x4242
IC dedicated software	Firmware version	0x03010202
FeliCa OS v5.0	OS version	0x031A

The user can check the Hardware version, Firmware version and OS revision by inputting “Request Product Information” command, and Hardware identifier by inputting “Get Chip ID” command. For more details, see section 5.3.2 and 5.3.3 of “RC-SA14 Series Inspection Procedure”.

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	ST31N600 A01	wafer	ANSSI-CC-2022/21	2022-10-21
IC dedicated software	ST31N600 A01	Embedded in the above	ANSSI-CC-2022/21	2022-10-21
FeliCa OS v5.0		Embedded in the above	To be certified	
(Pre)personalisation documentation	A14-Insp-E01-06	PDF or Paper	n/a	n/a
	A14-Insp_IDm-E01-06	PDF or Paper	n/a	n/a
Operational guidance	M1130-E01-11	PDF or Paper	n/a	n/a

An operational guidance other than the FeliCa specifications and (pre-)personalisation documentations are provided.

Any (pre-)personalisation performed by the developer of the TOE on behalf of its customers will lead to a state identical to states possible by executing the FeliCa commands for personalisation.

The TOE supports AES and DES, but the functionality using DES is out of scope of the evaluation.

Conformance claims

This ST claims strict compliance to the Public Transportation IC Card PP (called “[PTPP]” in the remainder of this document) under Common Criteria version 3.1, revision 5.

This ST is CC Part 2 conformant:

- Exactly, the SFRs of the [PTPP] are included by reference.
- Assignments for all open operations in the [PTPP] are provided in this ST.

The ST is CC Part 3 conformant:

- The assurance package is **EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.**

The rationale behind these claims is the requirement that the FeliCa security evaluation scheme requires compliance to this [PTPP] for this TOE type (FeliCa products).

Security Problem Definition

Refer to [PTPP]. In addition, this ST adds the following organisational security policy.

P.SecureID_System

TOE shall prove the identity of the TOE to an external entity and prevent unauthorised writing of the user data.

Objectives

Refer to [PTPP]. In addition, this ST adds the following TOE security objective.

O.SecureID_System

The TOE shall provide the means of the proof of the identity of the TOE to an external entity and prevent unauthorised writing of the user data.

The following table illustrates that the added policy is covered by at least one security objective.

Policy	Objective
P.SecureID_System	O.SecureID_System

The O.SecureID_System objective provides the means of the proof of the identity of the TOE to an external entity and prevention of unauthorised writing of the user data. Thus, the P.SecureID_System policy is covered by the objective.

Extended components definition

Refer to [PTPP].

Security Requirements

Security Functional Requirements

The [PTPP] defines the SFRs. TOE specific information is required to be assigned to the following SFRs, either:

- by the addition of the requested information as **highlighted in yellow** or
- as a selection from a two or more options, as **highlighted in blue**.

In all cases, the PTPP should be referenced for relevant application notes and other guidance.

SFR Reference	SFR	Assignment value/selection
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area] ¹	1: memory areas protected by an access control system in the Flash memory
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors] ² on all objects, based on the following attributes: [assignment: user data attributes] ³	2: bit corruption 3: data integrity checksum
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [assignment: action to be taken] ⁴ .	4: return an error code
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required] ¹⁵ .	15: Secure_read ¹ , Secure_write ² , management of security attribute
FIA_UID.1.1	The TSF shall allow Polling, Public read, Public write and [selection: [assignment: other list of TSF mediated actions], none] ¹⁷ on behalf of the user to be performed before the user is identified.	17: Requests ³ , Echo Back ⁴ , Reset Mode ⁵
FIA_UAU.1.1	The TSF shall allow Polling, Public_read, Public_write and [selection: [assignment: other list of TSF mediated actions], none]	18: Requests ³ , Echo Back ⁴ , Reset Mode ⁵

¹ Secure_read is a read operation to the user data files that require authentication with the Access Key corresponding to the Service.

² Secure_write is a write operation to the user data files that require authentication with the Access Key corresponding to the Service.

³ Requests is an operation to retrieve a configure, status or version information from the TOE that does not required authentication.

⁴ Echo Back is an operation to perform the communication test that does not required authentication.

⁵ Reset Mode is an operation to reset authentication status to “Not authenticated”.

	¹⁸ on behalf of the user to be performed before the user is authenticated.	
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)] ¹⁹ .	19: the authentication mechanisms shown in Table 1
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] ²⁵ .	Note: There are three iterations of this SFR in this ST. See below.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] ²⁶ .	Note: There are three iterations of this SFR in this ST. See below.
FMT_MSA.1.1	The TSF shall enforce the Service Access Policy ²⁷ to restrict the ability to set and [selection: [assignment: other operations], none] ²⁸ the security attributes ACL ²⁹ to Administrator ³⁰	28: none
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery ³⁴ with the capability to store Initialisation Data and [selection **: [assignment: other data], none] ³⁵ in the [assignment: type of persistent memory] ³⁶	35: none 36: Flash memory

In addition to the SFRs defined in the [PPTP], this ST adds “FIA_UAU.5 Multiple authentication mechanisms”.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **the list of multiple authentication mechanisms shown in Table 1** 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 1.**

Table 1 : List of Multiple authentication mechanisms

Authentication mechanism	Rules
Mutual authentication (AES)	If a Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Service.
Mutual authentication (CMAC)	If a Service requires MAC verification, the external entity and the TOE shall authenticate each other by using MAC verification by using Access Key that corresponds to the Service
FeliCa Secure ID authentication	If the external entity requests to write user data to Block in FeliCa Secure ID file system, the external entity and the TOE shall authenticate each other by using MAC verification with CK_A.

This ST iterates the SFRs “FDP_ACC.1” and “FDP_ACF.1” due to the presence of three authentication mechanisms described in the FIA_UAU.5.

FDP_ACC.1/AES

Subset access control

FDP_ACC.1.1/AES

The TSF shall enforce the Service Access Policy 1 on:

- **Subjects: subjects shown in Table 2**
- **Objects: objects shown in Table 2**
- **Operations: operations shown in Table 2**

FDP_ACF.1/AES

Security attribute based access control

FDP_ACF.1.1/AES

The TSF shall enforce the Service Access Policy 1 to objects based on:

- **Subjects: subjects shown in Table 2**
- **Objects: objects shown in Table 2**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 2**

FDP_ACF.1.2/AES

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

FDP_ACF.1.4/AES The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Table 2 : Service Access Policy 1

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 Service	User data file	Read only, Authentication with the Access Key corresponding to the Service required	Read
			Read/Write, Authentication with the Access Key corresponding to the Service required	Read or Write

FDP_ACC.1/CMAC Subset access control

FDP_ACC.1.1/CMAC The TSF shall enforce the **Service Access Policy 2** on:

- **Subjects: subjects shown in Table 3**
- **Objects: objects shown in Table 3**
- **Operations: operations shown in Table 3**

FDP_ACF.1/CMAC Security attribute based access control

FDP_ACF.1.1/CMAC The TSF shall enforce the **Service Access Policy 2** to objects based on:

- **Subjects: subjects shown in Table 3**
- **Objects: objects shown in Table 3**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 3**

FDP_ACF.1.2/CMAC 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/CMAC The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/CMAC The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Table 3 : Service Access Policy 2

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 MAC verification with the Access Key corresponding to the Service	User data file	Write, MAC verification with the Access Key corresponding to the Service required	Write

FDP_ACC.1/SecureID Subset access control

FDP_ACC.1.1/SecureID The TSF shall enforce the Secure ID System Policy on:

- **Subjects: subjects shown in Table 4**
- **Objects: objects shown in Table 4**
- **Operations: operations shown Table 4**

FDP_ACF.1/SecureID Security attribute based access control

FDP_ACF.1.1/SecureID The TSF shall enforce the FeliCa Secure ID System Policy to objects based on:

- **Subjects: subjects shown in Table 4**
- **Objects: objects shown in Table 4**

- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 4**

FDP_ACF.1.2/SecureID 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/SecureID The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SecureID The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Table 4 : FeliCa Secure ID System Policy

Subject	Security attribute Authentication status	Object	Security attribute ACL	Operation
Process representing User	Not authenticated	RC_B MAC_B ID_S MC_A DATA	Read, Authentication not required	Read
	Any status	RC_A CK_A	Read, prohibited	none
		RC_B	Write, prohibited	none
	Successfully MAC verification with CK_A	RC_A MAC_B ID_S CK_A MC_A DATA	Write, MAC verification with CK_A	Write

Regarding the Security Objectives defined in the [PTPP], the section 6.3 of the PP provides both the rationale for choosing specific Security Functional Requirements (SFRs) and how those requirements correspond to the specific Security Objectives. The following table gives an overview, how the SFRs are combined to meet the Security Objectives.

Objective	TOE Security Functional Requirements
O.Hardware_Attack	FDP_SDC.1 "Stored data confidentiality"
	FDP_SDI.2 "Stored data integrity monitoring and action"
	FPT_PHP.3 "Resistance to physical attack"
	FDP_ITT.1 "Basic internal transfer protection"
	FPT_ITT.1 "Basic internal TSF data transfer protection"
	FDP_IFC.1 "Subset information flow control"
	FRU_FLT.2 "Limited fault tolerance"
	FPT_FLS.1 "Failure with preservation of secure state"
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/AES "Subset access control"
	FDP_ACF.1/AES "Security attribute based access control"
	FDP_ACC.1/CMAC "Subset access control"
	FDP_ACF.1/CMAC "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"
	FPT_ITC.1 "Inter-TSF trusted channel"
O.SecureID_System	FIA_UAU.5 "Multiple authentication mechanisms"
	FDP_ACC.1/SecureID "Subset access control"
	FDP_ACF.1/SecureID "Security attribute based access control"
O.Configure	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.SecureID_System is achieved by the SFR FIA_UAU.5, FDP_ACC.1/SecureID and FDP_ACF.1/SecureID. The external entity and the TOE authenticate each other by FIA_UAU.5, if authentication is successfully completed, the external entity write user data in accordance with the policy that defined FDP_ACC.1/SecureID and FDP_ACF.1/SecureID.

The dependencies of the other SFRs defined in the [PTPP] are listed in section 6.3 in the PP. The following table presents the list of the SFRs with the associated dependencies and how they are satisfied.

ID	SFR	Dependencies	Notes
FDP_SDC.1	Stored data confidentiality	None	
FDP_SDI.2	Stored data integrity monitoring and action	None	
FPT_PHP.3	Resistance to physical attack	None	
FDP_ITT.1	Basic internal transfer protection	FDP_ACC.1 or FDP_IFC.1	Included (FDP_IFC.1)
FPT_ITT.1	Basic internal TSF data transfer protection	None	
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Not satisfied (See [PTPP])
FRU_FLT.2	Limited fault tolerance	FPT_FLS.1	Included
FPT_FLS.1	Failure with preservation of secure state	None	
FTP_ITC.1	Inter-TSF trusted channel	None	
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	
FIA_UAU.5	Multiple authentication mechanisms	None	

FDP_ACC.1/AES	Subset access control	FDP_ACF.1/AES	Included
FDP_ACF.1/AES	Security attribute based access control	FDP_ACC.1/AES	Included
		FMT_MSA.3	Not satisfied (See [PTPP])
FDP_ACC.1/CMAC	Subset access control	FDP_ACF.1/CMAC	Included
FDP_ACF.1/CMAC	Security attribute based access control	FDP_ACC.1/CMAC	Included
		FMT_MSA.3	Not satisfied (See [PTPP])
FDP_ACC.1/SecureID	Subset access control	FDP_ACF.1/SecureID	Included
FDP_ACF.1/SecureID	Security attribute based access control	FDP_ACC.1/SecureID	Included
		FMT_MSA.3	Not satisfied (See [PTPP])
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1	Included (FDP_ACC.1a and FDP_ACC.1b)
		FMT_SMR.1	Included
		FMT_SMF.1	Included
FMT_SMF.1	Specification of Management Functions	None	
FMT_LIM.1	Limited capabilities	FMT_LIM.2	Included
FMT_LIM.2	Limited availability	FMT_LIM.1	Included
FAU_SAS.1	Audit storage	None	

Security Assurance Requirements and Rationale

See section "Conformance claims".

TOE Summary Specification

The TOE implements the SFRs by access control to the FeliCa services in accordance with the FeliCa specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

The additional TOE summary specification regarding the SFRs added in this ST are described below.

- "FIA_UAU.5 Multiple authentication mechanisms" defines the multiple authentication mechanisms which are provided by the TOE. Each Service defines either authentication mechanism by Service Attribute to access the user data.

If the external entity tries to access to the Service that requires Mutual authentication (AES), the TOE and the external entity shall perform the mutual authentication by using the Access Key corresponds to the Service. "FIA_UAU.4 Single-use authentication mechanisms" and "FTP_ITC.1 Inter-TSF trusted channel" are achieved by the mutual authentication between the TOE and the external entity according to the specification of "Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)". The TOE uses random numbers in the authentication mechanism to comply with the "FIA_UAU.4 Single-use authentication mechanisms" requirement. The random numbers are generated anew each time the authentication is started, and are discarded each time the TOE exits the authenticated state.

If the external entity tries to access to the Service that requires Mutual authentication (CMAC), "FIA_UAU.4 Single-use authentication mechanisms" is achieved by mutual authentication between the TOE and the external entity according to the specification of "Security Reference Manual – Communication with MAC (AES 128bit)". The TOE uses random numbers in the authentication mechanism to comply with the "FIA_UAU.4 Single-use authentication mechanisms" requirement. The random numbers are generated anew each time the authentication is started, and are discarded each time the TOE exits the authenticated state.

- "FDP_ACC.1/AES and FDP_ACC.1/CMAC Subset access control" and "FDP_ACF.1/AES and FDP_ACF.1/CMAC Security attribute based access control" are satisfied by providing an access control system based on security attributes of the Service. A 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 Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Service. When the authentication is successfully completed, the TOE allows the external entity to access the user data according to the Service Attribute. The security attributes are assigned to Services 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).
- "FDP_ACC.1/SecureID Subset access control" and "FDP_ACF.1/SecureID Security attribute based access control" are satisfied by providing an access control system based on security attributes of Blocks. The TOE and the external entity shall perform MAC verification with CK_A(FIA_UAU.5) to write the user data.

References

- [PTPP] JICSAP (Japan ID Connect with Secure Authentication Promotional association) Public Transportation IC Card Protection Profile, version 1.12, 1 August 2018.