

# Security Target

## ST introduction

The reference of this ST is **A40-ST-E01-30** version **1.30**

## 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-SA40 Series and RC-SA41 Series** 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                    | <b>Hardware identifier</b> | <b>000089</b>   |
| IC                    | <b>Hardware version</b>    | <b>060C</b>     |
| IC dedicated software | <b>Firmware version</b>    | <b>80512030</b> |
| FeliCa OS v5.0        | <b>OS version</b>          | <b>0544</b>     |

**The user can check the TOE identifiers (Hardware identifier, Hardware version, Firmware version and OS version) by inputting “Request Product Information” and “Get Chip ID” command. For details, see M1247 or M1251 document below.**

## TOE overview

The TOE consists of the following:

| TOE component                             | Identification         | Form of delivery             | Certification identifier    | Certificate issue date |
|---|------------------------|------------------------------|-----------------------------|------------------------|
| <b>Hardware IC</b>                        | <b>IFX_CCI_000089h</b> | <b>wafer</b>                 | <b>BSI-DSZ-CC-1252-2025</b> | <b>2025-08-01</b>      |
| <b>IC dedicated software</b>              | <b>80.512.03.0</b>     | <b>Embedded in the above</b> | <b>BSI-DSZ-CC-1252-2025</b> | <b>2025-08-01</b>      |
| <b>FeliCa OS v5.0</b>                     |                        | <b>Embedded in the above</b> | <b>FAST-2400165-01</b>      |                        |
| <b>(Pre)personalisation documentation</b> | <b>M1247-E01-10</b>    | <b>PDF</b>                   | <b>n/a</b>                  | <b>n/a</b>             |
|   | <b>M1250-E01-10</b>    | <b>PDF</b>                   | <b>n/a</b>                  | <b>n/a</b>             |
|   | <b>M1251-E01-10</b>    | <b>PDF</b>                   | <b>n/a</b>                  | <b>n/a</b>             |
| <b>Operational guidance</b>               | <b>M1130-E01-11</b>    | <b>PDF</b>                   | <b>n/a</b>                  | <b>n/a</b>             |

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.

## 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 <b>[assignment: memory area]</b> <sup>1</sup>  | 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 <b>[assignment: integrity errors]</b> <sup>2</sup> on all objects, based on the following attributes: <b>[assignment: user data attributes]</b> <sup>3</sup> | 2: bit corruption<br>3: data integrity checksum   |
| FDP_SDI.2.2            | Upon detection of a data integrity error, the TSF shall <b>[assignment: action to be taken]</b> <sup>4</sup> .  | 4: return an error code   |
| FTP_ITC.1.3            | The TSF shall initiate communication via the trusted channel for <b>[assignment: list of functions for which a trusted channel is required]</b> <sup>15</sup> .   | 15: Secure_read <sup>1</sup> , Secure_write <sup>2</sup> , management of security attribute |
| FIA_UID.1.1            | The TSF shall allow <b>Polling, Public read, Public write and</b> <b>[selection: [assignment: other list of TSF mediated actions], none]</b> <sup>17</sup> on behalf of the user to be performed before the user is identified.             | 17: Requests <sup>3</sup> , Echo Back <sup>4</sup> , Reset Modes <sup>5</sup>               |
| FIA_UAU.1.1            | The TSF shall allow <b>Polling, Public_read, Public_write and</b> <b>[selection: [assignment: other list of TSF mediated actions], none]</b> <sup>18</sup> on behalf of the user to be performed before the user is authenticated.          | 18: Requests <sup>3</sup> , Echo Back <sup>4</sup> , Reset Modes <sup>5</sup>               |
| FIA_UAU.4.1            | The TSF shall prevent reuse of authentication data related to <b>[assignment: identified authentication mechanism(s)]</b> <sup>19</sup> .   | 19: the authentication mechanisms shown in Table1   |
| <del>FDP_ACF.1.3</del> | <del>The TSF shall explicitly authorise access of subjects to objects</del>   | Note: There are three iterations of this SFR in this ST.                                    |

|             |  |   |
|-------------|--|---|
|             | based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] <sup>25</sup> .  | 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] <sup>26</sup> .                                     | 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 <sup>27</sup> to restrict the ability to set and [selection: [assignment: other operations], none] <sup>28</sup> the security attributes ACL <sup>29</sup> to Administrator <sup>30</sup>                      | 28: none  |
| FAU_SAS.1.1 | The TSF shall provide the <b>test process before TOE Delivery</b> <sup>34</sup> with the capability to store Initialisation Data and [selection **: [assignment: other data], none] <sup>35</sup> in the [assignment: type of persistent memory] <sup>36</sup> | 35: none<br>36: Flash memory  |

<sup>1</sup> Secure\_read is a read operation to the user data files that require authentication with the Access Key corresponding to the Service.

<sup>2</sup> Secure\_write is a write operation to the user data files that require authentication with the Access Key corresponding to the Service.

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

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

<sup>5</sup> Reset Mode is an operation to reset authentication status to “Not authenticated”.

In addition to the SFRs defined in the [PTPP], 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.**

**Table1 : 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**.

**Table2 : Service Access Policy 1**

| Subject                         | Security attribute<br>Authentication status  | Object         | Security attribute ACL   | Operation     |
|---------------------------------|--|----------------|--|---------------|
| Process<br>representing<br>User | Not authenticated  | User data file | Read only,<br>Authentication not required  | Read          |
|                                 |  |                | Read/Write,<br>Authentication not required   | Read or Write |
|                                 | Successfully authenticated<br>with the Access Key<br>corresponding to the<br>Service | User data file | Read only,<br>Authentication with the Access Key<br>corresponding to the Service required  | Read          |
|                                 |  |                | Read/Write,<br>Authentication with the Access Key<br>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**.

**Table3 : Service Access Policy 2**

| Subject                   | Security attribute Authentication status                                       | Object         | Security attribute ACL  | Operation     |
|---------------------------|--|----------------|---|---------------|
| Process representing User | Not authenticated  | User data file | Read only,<br>Authentication not required   | Read          |
|                           |  |                | Read/Write,<br>Authentication not required  | Read or Write |
|                           | Successfully MAC verification with the Access Key corresponding to the Service | User data file | Read only,<br>Authentication with the Access Key corresponding to the Service required  | Read          |
|                           |  |                | Read/Write,<br>Authentication with the Access Key corresponding to the Service required | Read or 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 in Table 4**

**FDP\_ACF.1/SecureID Security attribute based access control**

FDP\_ACF.1.1/SecureID The TSF shall enforce the 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**.

**Table4 : FeliCa Secure ID System Policy**

| Subject                   | Security attribute Authentication status | Object                                | Security attribute ACL               | Operation |
|---------------------------|--|---------------------------------------|--------------------------------------|-----------|
| Process representing User | Not authenticated                        | RC_B<br>MAC_B<br>ID_S<br>MC_A<br>DATA | Read,<br>Authentication not required | Read      |
|                           |  |                                       | Authentication not required          |           |
|                           | Any status                               | RC_A<br>CK_A                          | Read, prohibited                     | None      |
| RC_B                      |  | Write, prohibited                     | None                                 |           |

|  |   |   |                                      |       |
|--|---|---|--------------------------------------|-------|
|  | Successfully MAC verification with CK_A | RC_A<br>MAC_B<br>ID_S<br>CK_A<br>MC_A<br>DATA | Write,<br>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"               |
|                   | FTP_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.