Adapter Compatible High-Speed Juki Card Software

Security Target

VERSION: 1.92

Published by: Nippon Telegraph and Telephone Corporation Service Integration Laboratories
Date of issue: October 10, 2008
Prepared by: NTT Electronics Corporation

Note: This product falls under the category of goods subject to application for permission as specified in the Foreign Exchange and Foreign Trade Law. This product is intended for domestic use, and will require export and other permissions under the aforementioned Law in order to export the product.

Revision History

Ver.	Date	Rivised by	Content and Reason of Changes
1.00	03.06.26	Osuga	For ST evaluation
1.10	03.07.29	Osuga	Reflected matters pointed out
1.20	03.07.30	Osuga	Fixed matters pointed out
1.30	05.12.05	Osuga	Update due to change of target chip and version update of applicable CC supporting material
1.40	05.12.21	Osuga	Fixed matters pointed out
1.50	07.03.12	Osuga	Updated for CC evaluation
1.60	07.08.01	Osuga	Reflected comments on the description of rationales
1.70	07.08.29	Osuga	Update on matters pointed out during evaluation
1.80	07.09.14	Osuga	Update on matters pointed out during evaluation
1.81	07.09.20	Osuga	Update on matters pointed out during evaluation
1.82	07.10.05	Osuga	Corrected typos
1.83	07.10.26	Osuga	Update on matters pointed out during evaluation
1.84	07.12.06	Osuga	Fixed for consistency with functional design document
1.85	07.12.11	Osuga	Fixed for consistency with functional design document
1.86	08.02.22	Osuga	Corrected typos
1.87	08.03.28	Osuga	Fixed for consistency with implementation, and added reference materials
1.88	08.05.26	Osuga	Fixed for consistency with actual operations
1.89	08.06.03	Osuga	Update on matters pointed out and corrected typos
1.90	08.07.25	Osuga	Update on matters pointed out
1.91	08.08.22	Osuga	Added description with regard to state when card is granted
1.92	08.10.10	Osuga	Deleted parts of descriptions concerning the TOE operational environment

Table of Contents

1. ST Introduction

This chapter provides an identification and overview of the Security Target (ST) and describes the CC conformance of the ST.

1.1 ST Identification

Title: Adapter Compatible High-Speed Juki Card Software
Security Target

Version: 1.92

Date of issue: October 10, 2008

Published by: Nippon Telegraph and Telephone Corporation, Service Integration Laboratories

Prepared by: Katsumi Osuga, NTT Electronics Corporation

TOE covered: Adapter Compatible High-Speed Juki Card Software

TOE version: 2.00

Version of CC applied: CC Version 2.3 parts 1, 2, and 3 (2005), and Supplement-0512

Assurance level: EAL4 Augmented (augmented assurance requirement: AVA_MSU.3)

Keywords: Basic resident registration card, IC card, embedded software, resident registration code, authentication, certificate, protection of confidential information

1.2 ST Overview

The Target of Evaluation (TOE) covered by this Security Target (ST) is an embedded software that is loaded onto a basic resident registration card (hereafter referred to as “Juki card”). The TOE will be loaded onto high-speed Juki cards with hardware implement calculation functions used for cryptographic operations. The TOE provides a wide range of security functions, including user identification and authentication, access control to protect data stored on the card, cryptographic communication to prevent disclosure of confidential information during external communication, execution management to control functions that can be executed based on the results of user identification and authentication, separation of domains for the multiple applications loaded into the card, and data restoration to maintain the data in the event of a power failure. Note that cryptographic communication is performed at high speed with the support of calculation functions incorporated into the hardware.

TOE-loaded Juki cards are used for operation of the Basic Resident Registration Network

System (hereafter referred to as “Juki Net”).

This ST defines threats the TOE should counter and the objectives for addressing such threats. It also describes the security functions and assurance requirements it provides as well as summary specifications of the TOE implemented, and provides the rationale for these requirements and specifications.

1.3 CC Conformance Claim

This ST:

1) Conforms to CC Version 2.3 Part 2

2) Conforms to CC Version 2.3 Part 3, EAL4 Augmented

The augmented assurance requirement is AVA_MSU.3.

Reference materials [JIL] and [AIS] are also used as a means of assurance for AVA_MSU.3.

The strength of the security functions for the TOE of this ST is SOF-Basic.

Furthermore, while there is no Protection Profile (PP) to which this ST conforms, the following PPs are referenced:

"Security Requirement Specifications (Protection Profile) for Basic Resident Registration IC Cards ver. 2.0"

2. TOE Description

This chapter describes the type, usage, configuration, function and mechanism of the TOE.

2.1 TOE Type

The TOE covered by this ST is embedded software loaded onto Juki cards that are used with the Juki Net. The TOE is used to manage data recorded on Juki cards as well as applications (AP) loaded onto them, and satisfies specifications required by Juki cards.

2.2 Use of TOE

2.2.1 TOE Use Objectives

The objectives of the TOE loaded onto Juki cards are to allow the issuer to grant the cards to card holders safely, to identify card holders, and to ensure the protection of card holders' information stored on the cards.

Based on the basic resident registration data managed by municipalities, the Juki Net was introduced to improve efficiency of basic resident registration data administration by connecting the municipal systems across the country via telecommunication lines. Juki cards are used for services such as allowing to grant copies of resident registration certificates in various locations, as well as for special cases of registering new addresses when moving in or out, and confirming identification of residents. Juki cards are inserted into Juki card reader/writers installed at service counters of municipality offices and connected to service terminals of municipal systems, which are linked to the Juki Net. Juki cards provide various services by communicating with the service terminals of the municipality offices through the card reader/writers. The objective of the TOE is to provide security functions such as user authentication, access control, and cryptographic communication, and to ensure independence of applications when addressing the above needs.

2.2.2 Parties related to TOE

This section clarifies the roles of parties or devices related to the TOE during the phases of production up to and including the use of the TOE. Those related to the TOE include card manufacturers, card issuers, card holders, service terminals, and AP loading administrators (hereafter, these may simply be referred to as “manufacturers,” “issuers,” “holders,” “terminals,” and “AP loaders”). Except for manufacturers, all parties related to the TOE are collectively called “TOE-related parties.” Users of APs loaded into the TOE also do exist, but they are excluded from TOE-related parties since they do not directly relate to the TOE.

TOE Manufacturers

Card manufacturers: These are TOE manufacturers who are involved with the TOE only

during the fabrication phase prior to the use of the TOE.

TOE-related parties

Card issuers: Those who procure TOE-loaded cards from manufacturers and issue and grant them as Juki cards.

Card holders: Those who are granted a Juki card and keep it in their possession.

Service terminals: Issues commands to Juki cards to request various processing.

AP loading administrators: Those who administer AP loading in general in the AP management area of Juki cards

2.2.3 Usage of TOE

Use of Cards

By presenting pre-configured authentication data, TOE-related parties are allowed to access data they are authorized to access and perform functions they are authorized to perform after validity is confirmed by the TOE.

Issuance of Cards

The TOE is loaded by card manufacturers onto Juki cards in advance and delivered to card issuers in accordance with safe delivery procedures. Within the TOE's data area, municipalities which are the issuers of the cards, set up user data, authentication data required for authentication, and information required for TOE operations. When issuing cards, the card issuer sets tentative authentication data and disables some of the card's functions. The tentative authentication data are set in accordance with the policies of each municipality, and the contents of the data are appropriately controlled as confidential information by each municipality.

Granting of Cards

When granting a Juki card to a resident, the municipal government staffs who have knowledge of the tentative authentication data for the card being granted confirms the validity of the card. Then the resident to whom the card is being issued sets the authentication data used to confirm his or her identity. Once the card holder sets the authentication data, the holder is allowed to use the card as a Juki card.

Loading and Deletion of APs

Card issuers manage the area where applications are loaded and set security attributes that control the ability to load or delete applications in the area they manage. Based on the security attributes set by the card issuer, the TOE handles applications as user data and controls accesses to the area with regard to the loading and deletion of applications by the card issuer or the AP loading administrator to whom authority is delegated by the card issuer.

This enables card holders to use applications loaded on their card.

Invalidating Cards

If the card issuer invalidates a card, the TOE ceases to accept any requests, rendering all functions of the card unusable.

2.3 Configuration Encompassing the TOE

2.3.1 Hardware and Software Configuration

The software and peripheral hardware and software that comprise the TOE are as illustrated in **Fig. 1** and the TOE is represented by the shaded areas in the figure. Interfaces with external systems are realized by command and response messages transmitted via a card reader/writer.

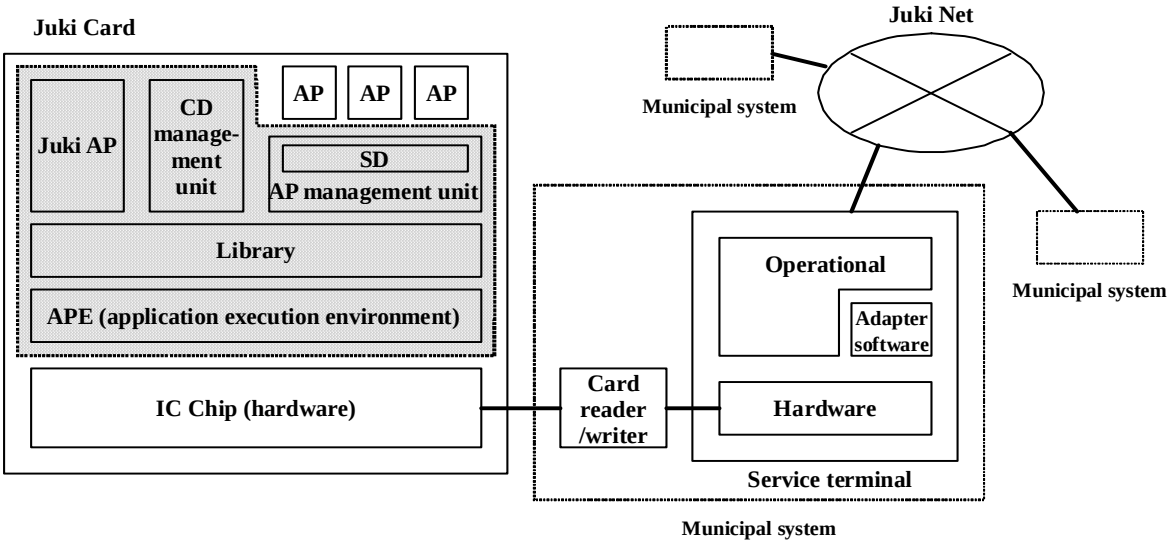


Fig. 1 TOE Configuration

The TOE, which is incorporated into the memory of the IC chip, consists of the application execution environment (APE), which provides an operational environment for applications; a library that performs common processing as middleware; the CD management unit, which provide functions related to the issuance of Juki cards and the management of state transition; the AP management unit, which controls the loading and deletion of applications; and various modules of Juki AP that realizes functions necessary to use services of the Juki Net. Furthermore, the library is composed of a security library, an RAM management library, and a flash management library. Juki AP which is an application, is loaded in advance onto Juki cards during the manufacturing phase, and does not belong within the management scope of the application management unit. In addition, an area called “SD” is created in the AP management unit, and applications can be loaded into that area. Access control of the loading and deletion of applications loaded by the TOE are performed as with user data, and domain separation is enforced between the loaded applications. The security functions provided by APs loaded into the SD exist outside this TOE.

Juki cards connect to service terminals through card reader/writers, and the service terminals connect to the Juki Net. Similarly, municipal systems are connected to the Juki

Net. Juki cards receive command messages transmitted from service terminals via card reader/writers using communications functions of the IC chip, execute processes in accordance with the content of the command messages, and return the results of the processing as response messages.

Software programs called “service software” runs on service terminals to perform services required by the Juki Net. Furthermore, on the service terminals, there is a software program referred to as “adapters” that generates command messages which support the implementation of Juki cards in accordance with the command specifications defined by the Juki specifications. The adapters invoked by the service software absorb the differences between the implementations of Juki cards from the various manufactures, and allow these cards to be used based on a common command specification.

2.3.2 Scope of TOE

The physical scope of the TOE is represented by the shaded area in **Fig. 1**, and the TOE, which consists of five modules, is loaded into the memory of the IC chip as software. All interfaces with external systems are provided through command and response messages.

The logical scope of the TOE, meanwhile, is represented by what is described as security functions in section **2.4.1 .**

2.3.3 TOE Operational Environment

Specifications of the TOE operational environment and TOE peripheral devices are as described below:

<IC Chip>
Manufacturer: Sharp Corporation
Model: SM4148 IC Card LSI

<Card reader/writer>

Card reader/writers with a contactless interface in accordance with ISO/IEC 14443 and JIS X 6322, or a contact interface in accordance with ISO/IEC 7816 and JIS X 6304.

<Adapter software>
Software created to support the implementation of Juki cards in accordance with the requirement specifications of Juki cards.

<Service software>
Software created to respond in accordance with the operation of Juki cards based on the requirement specifications.

2.4 Functions of the TOE and TOE Environment

This section describes the functions of the TOE and those of the TOE environment.

2.4.1 Functions of TOE

This sub-section describes the security functions of the TOE, which are implemented by the modules of the TOE shown in **Fig. 1**: APE, a library, the CD management unit, the AP management unit, and the Juki AP.

<<Security Functions of TOE>>

2.4.1.1 Identification and Authentication Functions

(1) Identification Functions

The TOE identifies users when a switch from one module to another occurs due to a Select command, and the currently operating module on the card is called a “process.” The identified user is associated with the process, which in turn runs on behalf of that user, and the command messages received are delivered to the currently selected process.

Note: In this ST, modules represent components of the TOE in terms of software programs loaded on the card, and processes represent programs in terms of modules that are running as subjects. When the CD management unit, Juki AP, and AP management unit modules run, they are regarded as a CD management process, a Juki AP process, and an AP management process, respectively.

(2) PIN Verification Functions

The TOE compares the PINs transmitted from outside with the cards’ pre-set data in order to authenticate TOE-related parties.

(3) External Authentication Functions

The TOE sends out random numbers it generates to external systems, and using the cards’ pre-set public keys or those included in verified public key certificates, decrypts encrypted data sent from external systems in order to authenticate external nodes.

2.4.1.2 Access Management Functions

(4) File Management Functions

The TOE secures and manages the file areas where data are stored in flash memory and controls accesses to the data stored in the files.

(5) SD Management Functions

The TOE has an area called “SD,” an AP management area in which APs are loaded.

(6) Application Management Functions

The TOE manages APs in the SD, and based on its access control, manages the loading, selection, and deletion of the APs.

(7) Key Management Functions

The TOE stores and updates key data in key storage files it manages.

2.4.1.3 Cryptographic Communication Functions

(8) Secure Messaging Functions

When communicating with external systems, the TOE uses secure messaging functions to encrypt data to be transmitted and to decrypt the data received. The TOE achieves high-speed encryption and decryption by employing IC card LSI's calculations functions for DES cryptographic operations.

2.4.1.4 Execution Management Functions

(9) Authentication Status Management Function

The TOE manages the results of PIN verification and external authentication as authentication status. When one of the modules (the CD management unit, the AP management unit, or Juki AP) is selected as the current process, the TOE clears or maintains the authentication status, and updates the authentication status when PIN verification and external authentication are performed in each process.

(10) State Transition Management Functions

The TOE manages the state of each of the modules (the CD management unit, the AP management unit, and Juki AP) and by using commands, effects the state transition of each module.

Note: State transition of each module is effected while running as a process, and the state of each module is maintained also while loaded as a module but not running.

(11) Command Execution Control Functions

The TOE controls command execution by determining whether the role of authenticated TOE-related parties, in accordance with the state of transition, allows for command execution.

2.4.1.5 Domain Separation Functions

(12) Domain Separation Functions

The TOE separates the operational areas of modules loaded on the card so that these

modules do not interfere with each another.

2.4.1.6 Data Restoration Functions

(13) Power Failure Detection Functions

When starting up, the TOE examines whether any power failure had occurred during a data write or data deletion.

(14) Failure Recovery Functions

The TOE begins a transaction prior to processing, and if the processing ends successfully, the TOE effectuates the contents written during the processing and completes the transaction. If the processing ends unsuccessfully, the contents written during the processing are discarded and the card is returned to a correct state.

<<TOE Non-Security Functions>>

The TOE's functions not directly related to security are described below:

(1) Communication Functions

The TOE receives command messages, which request command execution, and transmits response messages, which represent the results of processing.

(2) Command Analysis Functions

The TOE parses the command messages received and performs the requested processing.

(3) Memory Restriction Functions

The TOE restricts the size of memory areas that applications loaded on the card can use.

2.4.2 Functions of the TOE Environment

2.4.2.1 Functions of IC Chips

(1) Tamper Resistance Functions

The TOE environment protects programs and data loaded into IC chips from physical attacks.

(2) DES Calculation Functions

The TOE environment performs calculation functions for DES encryption using hardware.

2.4.2.2 Functions of Card Reader/Writers

(1) Residual Data Protection Functions

The TOE environment erases any residual data to prevent data entered by TOE-related parties from remaining on the device that may result in data leakage.

2.4.2.3 Functions of Service Terminals

Service terminals are installed in municipal government office buildings and operated by municipal government staff. Service software run on these terminals to issue cards, load APs, set PINs, and read resident registration codes. Service software control access after authentication of card issuers and AP loading administrators, and allow the secret keys of service terminals to be used only when the software is started up by authorized government staffs who issue the cards. In addition, in order to prevent disclosure of PINs entered by card holders for transmission to their Juki cards and resident registration codes read from Juki cards, these residual data are erased from the terminals after their use.

(1) Residual Data Protection Functions

Service terminals erase any residual data to prevent data entered by TOE-related parties from remaining on the device what may result in data leakages.

(2) Authentication Functions

Service terminals authenticate the validity of TOE-related parties who operate them and other service terminals to which they connect with over the network.

(3) Access Control Functions

Service terminals control access to their secret keys, which are managed on the terminals.

(4) Execution Management Functions

Service terminals restrict the roles of TOE-related parties who are allowed to configure security attributes and manage security functions.

2.5 Security Mechanism of TOE

This section explains the mechanisms required to implement the security functions of the authentication, access control, state transition, and cryptographic operations provided by the TOE.

2.5.1 Authentication Mechanisms of TOE

Table 2-1 indicates the authentication mechanisms in the process that correspond to the roles of TOE-related parties. If there are two or more authentication mechanisms for the same role, the TOE-related parties shall be authenticated using a single mechanism in accordance with the operation executed.

Table 2-1 TOE-Related Parties and Authentication Mechanism

Role of TOE -related party	Authentication mechanism	Relevant party
Card issuer	PIN verification using CD management unit transport PINs PIN verification using CD management unit tentative PINs PIN verification using CD management unit proprietary PINs PIN verification using Juki AP tentative PINs External authentication using issuing municipality public keys in the CD management unit PIN verification using AP management unit transport PINs External authentication using card issuer public keys in the AP management unit	Municipalities
Card holder	PIN verification using CD management unit card holder PINs PIN verification using Juki AP card holder PINs	Residents
Service terminal	External authentication using temporary public keys whose certificate has been verified by certificate verification public keys in the Juki CD External authentication using temporary public keys whose certificate has been verified by key management public keys in the Juki AP	Systems installed and operated in municipalities
AP loading administrator	External authentication using AP loading administrator public keys in the AP management unit	Municipalities

Note: There are certification authorities, though not a TOE-related party, that issue certificates of public keys for card issuers and AP loading administrators in the AP management unit. The certification authorities are established in each municipality and issue certificates under the direction of the municipality. Public keys of the certificate authorities are set in the AP management area at the time of card issuance, and used when authenticating card issuers or AP loading administrators.

PINs used for authentication may be entered and changed by authorized TOE-related parties depending on their role and in accordance with TSF data management rules. Tentative PINs are set by card issuers, and card holder PINs are set by card holders. The tentative PINs are set in accordance with the policies of each municipality, and the contents of the set tentative PINs are regarded as confidential information and managed appropriately by the municipality. Card issuers may set new values depending on the state of the TOE. In addition, authentication data may be reset from authorized service terminals.

Three consecutive failures of PIN verification or external authentication attempts would result in an inability to use the relevant authentication data in subsequent authentications. The failure count is managed for each set of authentication data, and the count is reset to zero if authentication succeeds. Once authentication is disabled, the authentication data will need to be reset. The failure count will be reset to zero when the data is reset.

CD management unit transport PINs and AP management unit transport PINs cannot be reset by TOE-related parties, and therefore, three consecutive authentication failures will result in the inability to use any functions that require authentication with these transport PINs.

2.5.2 TOE Access Management

As shown in **Fig. 2**, data used by the TOE are divided into three areas: the Juki AP area, the CD management area, and the AP management area. These domains are kept separated by APE so that each set of data can only be accessed by the Juki AP, the CD management unit, and the AP management unit, respectively. Each domain is assigned a module in executive form and an area for the data handled by the module. The modules of each domain can access data in their own domain, but are not allowed to access data in other domains. Each of the separated domains is loaded with one of the three modules of the CD management unit, Juki AP, and the AP management unit, and each module authenticates TOE-related parties independently and controls access to user data that exist in each domain. In addition, shared domains that are accessible from other domains can be established, and libraries are loaded into a shared domain making them available to each of the other domains.

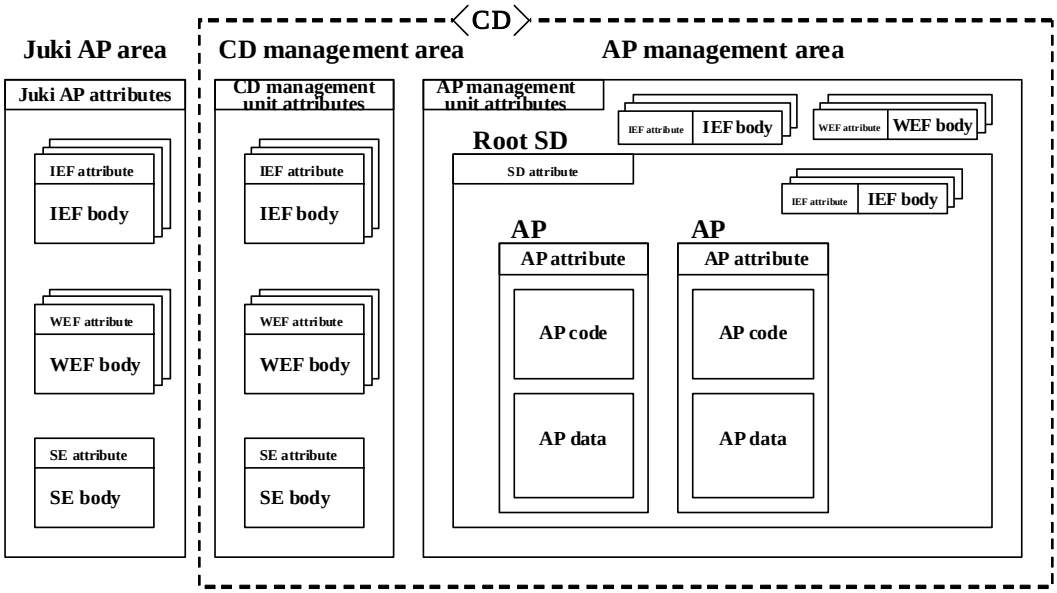


Fig. 2 Configuration of Data Areas

In the Juki card, a basic file called “EF” can be created as an area for data storage. EF has two areas: a data storage area called “IEF” in which authentication data for PINs or keys are stored, and a data storage area called “WEF” in which data used for work are stored. A data storage area called “SE” also exists as one of the security attributes to designate keys to be used for authentication and encryption. In addition, the Juki card has an area called “CD” to manage card-related information in general, and is composed of two areas: the CD management area and the AP management area. Within the AP management area, an area called “root SD” is created by the card manufacturer to manage all APs that are loaded on the card. The application storage area has two areas: one in which AP program codes are stored, and the other in which data used by APs are stored. Each data storage area has an area to store attributes that represent data management information. The root SD area has security attributes called “SD attributes” for configuring settings related to AP loading.

The CD management area has a number of IEF and WEF areas as well as one SE area. Only one SD area is created in the AP management area, and multiple APs are loaded into that area. Both the AP management area and the SD area have a number of IEF areas. The Juki AP area has a number of IEF and WEF areas as well as one SE area.

The concept of access control provided by the TOE is as shown in Fig. 3. Commands sent by a service terminal through a card reader/writer are passed on to the TOE’s communications unit first. The Select command chooses either the CD management unit module, the AP management unit module, or the Juki AP module, and the selected module runs as a CD management process, an AP management process, or a Juki AP process, acting on behalf of the user as a subject. The user is associated with the process running as a

subject by the current process identification information, and the command dispatch unit sends commands for processing to the currently chosen process which is either the CD management process, the AP management process, or the Juki AP process. The Select command changes the current-process identification information, and the first current process at the time of card startup is the AP management process. Data areas are accessed as commands are processed in the process running as a subject, and access control is enforced on accesses to user data.

The Select command can choose one of the three modules, but when switching from one module to another, user identification is performed, making the newly chosen module a subject that acts on behalf of the identified user when the module runs as a process. The Select command alone is distinguished from other commands and can be executed without user identification.

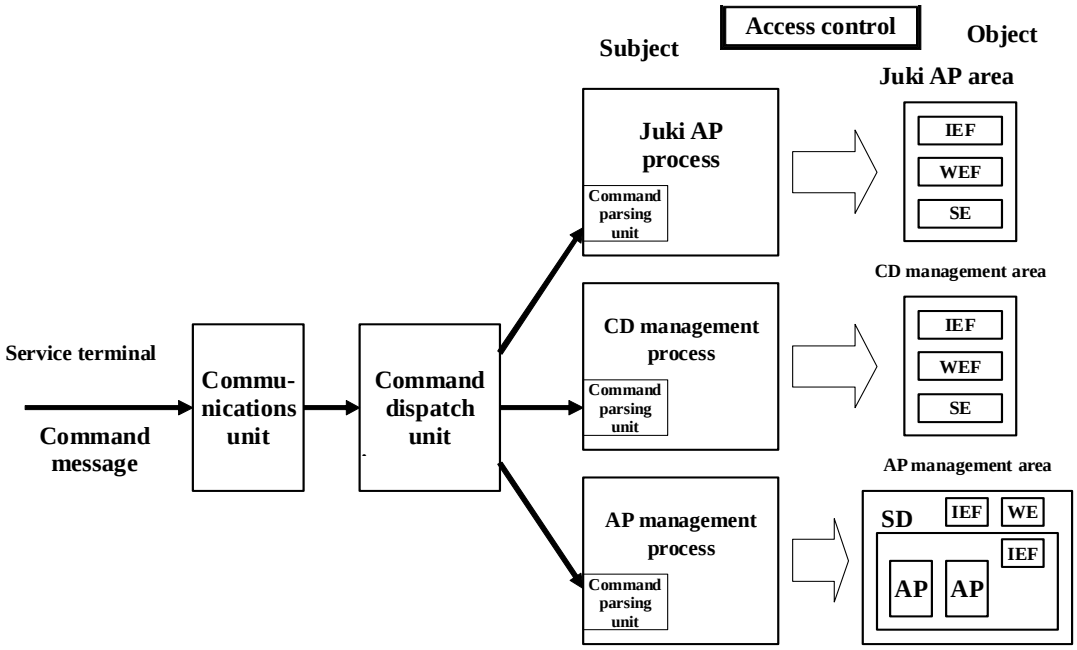


Fig. 3 Relationship between the Subject and the Object in Access Control

The mechanism of access control uses security attributes called “access management attributes” to define the access rights to the operation of access control. A security attribute called “authentication status” retains the results of the authentication of TOE-related parties, and if the conditions of access management attributes are satisfied, access to information in the object is permitted. Access control of each of the modules depends on the state of transition within the state transition diagram, and the current state is controlled by a security attribute called “state transition status.” Access management attributes are set by manufacturers in the area for IEF or WEF attributes during the fabrication phase and

cannot be changed during use of the TOE. The authentication status and the state transition status change in accordance with the behavior of each module, and both are kept in the CD management attribute, Juki application attribute, and application management attribute areas in **Fig. 2**.

Table 2-2 shows the relationship among subjects, users, and roles in access control. In **Table 2-2**, users represent parties or devices that exist outside the TOE, and is a generic term that refers to users that the subject acts a behalf of.

Table 2-2 Relationship between the Subjects, Users, and Roles in Access Control

Subject	User	Role
CD management process	CD management unit users	Card issuer Card holder
Juki AP process	Juki AP users	Card issuer Card holder Service terminal
AP management process	AP management unit users	Card issuer AP loading administrator

2.5.3 TOE State Transition

The CD management unit, the AP management unit, and the Juki AP modules undergo state transition as indicated in **Fig. 4** in conjunction with the operations performed by the TOE-related parties. In **Fig. 4**, the square frames denote different states, and in each of the three modules, the current state is managed by a security attribute called “state transition status,” and the value for state transition status varies according to state transition. The state transition status changes when a module is running as a process, but also when one process is switched to another and when the card is deactivated, the value for state transition status is maintained, allowing the state of modules to be managed.

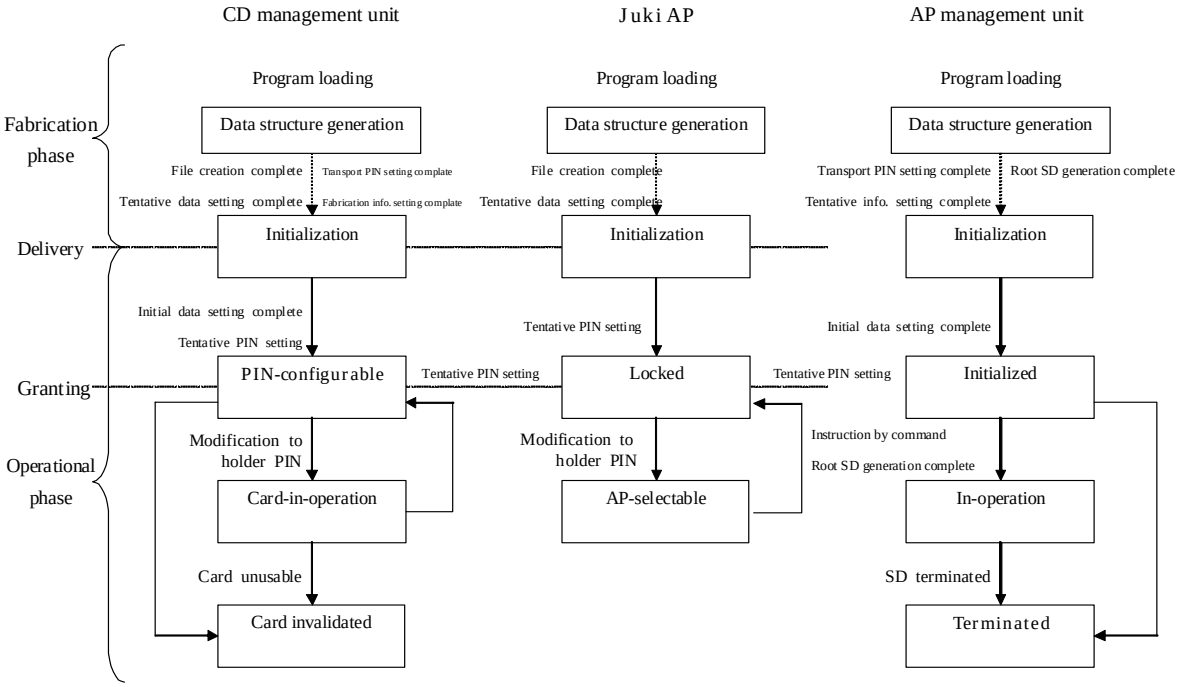


Fig. 4 TOE State Transition

First, the manufacturer loads all programs, including APE and libraries, which comprise the TOE into the IC chip memory. Following that, the manufacturer creates files, sets the transport PINs and tentative data, and then delivers the TOEs to the card issuing municipalities with the settings of the transport PIN and tentative data completed, and in accordance with the safe delivery procedures. While the domains of the modules are separated and the state transition for each module after delivery can be performed separately, the actual usage would be to perform the state transition of each module in a synchronized manner. Specifically, after the tentative PIN is set by the issuer, the card will be granted to a resident who will become the card holder, with the status of the CD management unit module and the Juki AP module in PIN-configurable state and locked state, respectively. The

state transition of the AP management unit is initiated based on the processing by the card issuer and is transitioned in accordance with the AP loading administration policies of the municipality. If the AP loading administrator will perform AP loading or deletion during the operational phase, the AP management unit will be transitioned to operational state before cards are granted. Conversely, if the AP loading administrator will not perform AP loading or deletion during the operational phase, cards will be granted with the AP management unit in initialized state. If the CD management unit transitions into card invalidated state, the card will stop accepting any commands and will become unusable.

The TOE covered by this ST is used by TOE-related parties within the scope designated by the “operational phase” in **Fig. 4**, and any use during fabrication phase is beyond this scope.

The following section explains the relationship between the state transitions of each module.

2.5.3.1 State Transition of the CD Management Unit

(1) Data Structure Generation State

This refers to the state in which the manufacturer is in the process of creating files required for Juki cards and setting tentative data in the IEF area. This state transitions into initialization state after the setting of tentative data is completed.

(2) Initialization State

This refers to the state of cards when they are delivered from the manufacturer; i.e., a state that satisfies the specifications required by Juki cards and allows setting of initial data.

(3) PIN-configurable State

This refers to a state in which the setting of initial data to register information required for card initialization and operation with the card is completed and a tentative PIN is set; i.e., a state in which a card is allowed to be granted to a resident who will become the card holder.

(4) Card-in-Operation State

This refers to a state that comes as a result of the completion of PIN settings by the card holder after the card is granted to him or her; i.e., a state in which the card can be used with the Juki system.

(5) Card Invalidated State

This refers to a state in which cards are made permanently unusable.

Table 2-3 State Transition of the CD Management Unit

State transition	Condition for the transition
Data structure generation => Initialization	Work by the manufacturer completed

Initialization => PIN configurable	CD management unit tentative PIN set by card issuer
PIN configurable => Card operational	CD management unit card holder PIN set by card issuer*
Card operational => Card invalidated	Instructed by command from card issuer
PIN configurable => Card invalidated	Instructed by command from card issuer
Card operational => PIN configurable	CD management unit tentative PIN set by card issuer

* In the CD management unit, the CD management unit tentative PIN and CD management unit card holder PIN are stored in the same area. When transitioning from PIN configurable state to card operational state, setting the CD management unit card holder PIN means to change the CD management unit tentative PIN to a CD management unit card holder PIN.

2.5.3.2 State Transition of the AP Management Unit

(1) Data Structure Generation State

This refers to a state in which initial data required for the AP management unit is being set. After the setting of the transport PIN is completed, a root SD is created directly in the CD, and cards are delivered by the manufacturer with card management data already set.

(2) Initialization State

This refers to a state in which initial data required for the operation of the AP management unit can be set.

(3) Initialized

This refers to a state in which the card issuer has set the public key issued by the certification authority, public key of the card issuer, encryption key for key distribution, and decryption key for key distribution.

(4) Operational

This refers to a state in which the AP management unit is in operation; i.e., a state in which AP loading is possible.

(5) Terminated State

This refers to a state in which the AP management unit has terminated, refusing to accept commands from the AP management unit.

Table 2-4 State Transition of the CD Management Unit

State transition	Condition for the transition
Data structure generation => Initialization	Work by the manufacturer completed
Initialization => Initialized	Instructed by command from card issuer
Initialized => Operational	Instructed by command from card issuer
Operational => Terminated	Instructed by command from card issuer
Initialized => Terminated	Instructed by command from card issuer

2.5.3.3 State Transition of the Juki AP

(1) Data Structure Generation State

This refers to a state in which files etc. required for Juki cards are being created and tentative data etc. are being set in the IEF area. This state transitions into initialization state after data setting is complete.

(2) Initialization State

This refers to a state in which processing to set initial data for the Juki AP can be performed.

(3) Locked State

This refers to a state in which the writing of initial data to the card in order to register information required for operation is completed and the Juki AP tentative PIN is set. While the card may be granted to the resident who will become the card holder, the possible functions will be limited to PIN setting and verification.

(4) AP-selectable State

This refers to a state in which, after the card is granted to a card holder, the PIN is set by the card holder, allowing it to perform processing with the Juki AP and to be used with the Juki system.

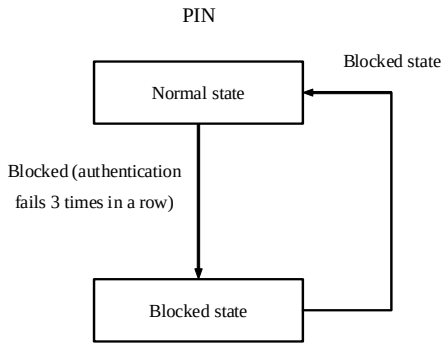
Table 2-5 State Transition of the Juki AP

State transition	Condition for the transition
Data structure generation => Initialization	Work by the manufacturer completed
Initialization => Locked	Juki AP tentative PIN set by the card issuer
Locked => AP selectable	Juki AP card holder PIN set by the card issuer*
AP selectable => Locked	Juki AP tentative PIN set by the card issuer

* In the Juki AP, the Juki AP tentative PIN and Juki AP card holder PIN are stored in the same area. When transitioning from locked state to AP selectable state, setting the Juki AP card holder PIN means to change the Juki AP tentative PIN to a Juki AP card holder PIN.

2.5.3.4 State Transition of PINs and Public Keys

Multiple PINs and public keys (excluding temporary public keys) used for authentication reside in each of the data areas, and both PINs and public keys change their state as indicated in the state transition diagrams shown in **Fig. 5** and **Fig. 6**. The state transition of PINs and public keys are managed separately, determining whether the PIN or public key concerned can be used for authentication or not, and are independent of the TOE state transition shown in **Fig. 4**.



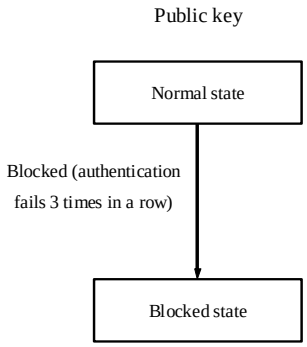


Fig. 5 State Transition Diagram of PINs **Fig. 6 State Transition Diagram of Public Keys**

(1) Normal State

This refers to a state in which PINs can be used for authentication in terms of PIN verification and public keys in terms of external authentication.

(2) Blocked State

This refers to a state in which authentication for PIN verification using PINs or external authentication using public keys has failed consecutively and the PINs or public keys can no longer be used for authentication. The state transition of PIN verification and the method to recover from a blocked state are shown in **Table 2-6**. Public keys cannot be recovered to a normal state once they transition into a blocked state.

Table 2-6 State Transition of PIN Verification and Method to Recover from Blocked State

Module	State <Role>	Normal => Blocked	Method to recover from blocked state
CD management unit	Initialization <Card Issuer>	Consecutive failure of transport PIN verification	none
	PIN configurable <Card Issuer>	Consecutive failure of CD management unit tentative PIN verification	none
	Card operational <Card Holder>	Consecutive failure of CD management unit card holder PIN verification	CD management unit tentative PIN set by card issuer
Juki AP	Initialization <Card Issuer>	Consecutive failure of transport PIN verification	none
	Locked <Card Issuer>	Consecutive failure of Juki AP tentative PIN verification	none
	AP selectable <Card Holder>	Consecutive failure of Juki AP card holder PIN verification	Juki AP tentative PIN set by the card issuer
AP management unit	Initialization <Card Issuer>	Consecutive failure of AP management unit transport PIN verification	none
	Initialized <Card Issuer>	Consecutive failure of AP management unit transport PIN verification	none
	Operational	No applicable PIN	not applicable

2.5.4 TOE Cryptographic operations

Details of cryptographic operations used in the TOE, where they are used, the purposes of their use, and the keys used for those purposes are as listed below:

Table 2-7 TOE Cryptographic operations and Its Use

Algorithm	Key size	Cryptographic operation	Purpose of use	Keys used
RSA	1024 bits	Decryption of authentication codes encrypted with secret keys of related party's to verify the authentication when authenticating externally	Authentication of related parties	Card issuing municipality public key, AP management unit card issuer public key, AP loading administrator public key
RSA	1024 bits	Decryption of the distributed (imported) session keys used for secure messaging	Distribution of cipher communication keys	Juki AP key distribution decryption key, AP management unit key distribution decryption key
RSA	1024 bits	Encryption for the creation of authentication codes for the internal authentication of card holders	Creation of authentication codes	CD management unit card secret key, AP management unit card secret key
RSA	1024 bits	Verification of the certificates of temporary public keys	Verification of certificates	Key management public key, certificate verification public key
RSA	1024 bits	Verification of the certificates of the card issuer and the AP loading administrator public keys for the AP management unit	Verification of certificates	Certification authority public key
RSA	1024 bits	Decryption of authentication codes encrypted with service terminal secret keys to externaly authenticate service terminals	Authentication of service terminals	Temporary public key
Triple-DES	168 bits	Decryption of imported CD management unit card secret keys	Data confidentiality	Import key

Triple-DES	168 bits	Command decryption and response encryption in secure messaging	Data confidentiality	Juki AP session key
Triple-DES	112 bits	Command decryption and response encryption in secure messaging	Data confidentiality	Fixed key, AP management unit session key

Note: The cryptographic keys for key distribution and decryption keys for key distribution correspond to public keys and secret keys of RSA encryption respectively, and different keys are used in the Juki AP and the AP management unit. Card secret keys are used to create authentication codes for the authentication of card holders from outside the TOE. The TOE provides functions for cryptographic operations using card secret keys; however, they do not provide any security function for protecting assets it expects in this ST. The AP management unit card secret key is the same as the unit's decryption keys for key distribution.

3. TOE Security Environment

This chapter describes the assets, assumptions, threats, and organizational security policies that comprise the TOE security environment.

3.1 Assets

Juki cards are produced by going through various production processes. This ST defines data in Juki cards delivered to municipalities that the TOE should protect and data that the TOE uses as a means of protecting the card data, as assets as follows:

The user data protected by the TOE are as listed below:

- Municipal data that are set by each municipality individually
- Card type identification data and card management data that are set by the manufacturer
- Resident registration codes used for user identification
- CD management unit card secret keys that are used for external card authentication
- Juki AP session keys and AP management unit session keys imported through key distribution
- Juki AP key distribution encryption keys that are distributed externally prior to the distribution of Juki AP session keys
- AP management unit key distribution encryption keys that are distributed externally prior to the distribution of AP management unit session keys
- Applications loaded by municipalities into Juki cards

Note: Municipal data includes card type identifier, card issuance number, municipality code, and the term of validity. Card type identification data includes software type identification data and OS type data. Card management data includes card type, hardware type, and maximum available size.

In order to protect these data, the TOE uses the following TSF data (authentication data, security attributes, etc.):

- The transport PINs, tentative PINs, card holder PINs, and proprietary PINs of the CD management unit, as well as the tentative PINs and card holder PINs for the Juki AP, and the transport PINs for the AP management unit, all of which are used to authenticate TOE-related parties (identification).
- Public keys of card-issuing municipalities, card issuer public keys of the AP management unit, and AP loading administrator public keys, all of which are used to authenticate

external nodes

- Certificate verification public keys and key management public keys that are used to verify the certificate of temporary public keys
- Certificate authority public keys used to verify the certificates of the card issuer and AP loading administrator in the AP management unit
- Temporary public keys used to decrypt authentication codes encrypted with service terminal secret keys to externaly authenticate the service terminals
- Import keys used to decrypt imported CD management unit card secret keys
- Juki AP key distribution encryption keys and AP management unit key distribution decryption keys, both of which are used to decrypt distributed session keys
- Fixed keys used for encrypion and decryption of secure messaging

3.2 Assumptions

This section describes the assumptions that allow the TOE to implement its security functions.

These assumptions are as described below:

1) **A.CARD_SET_Data:**

Before the TOE is delivered to card holders, municipalities, which are card issuers and AP loading administrators, will set the TOE with user data and authentication data, as well as information required for the operation of the TOE. With regard to the human aspects of the data, municipalities shall be responsible of specifying safe values for these data, and shall ensure that they are properly set and safely managed by trained municipal government staff. With regard to the physical aspects, when setting/using TSF data, municipalities shall procure IT devices (card reader/writers and service terminals) capable of managing TSF data safely and use them within a safe municipal environment. Card holder residents, meanwhile, shall set appropriate PINs that are difficult to guess.

3.3 Threats

The assumed threats when a TOE is used are as described below:

A resident who is granted a Juki card accesses personal information (information for personal identification, including name, date of birth, gender, address, resident registration code, and other incidental information) managed by the municipality based on the resident registration code stored on the card, and receives various administrative services. As described below, these convenient cards may be attacked in various ways by people with different motives, and the resident granted with the Juki card may not only experience

infringement of their privacy but may also suffer property damage.

1) **T.Logical_Attack**:

Juki cards delivered to municipalities go through such processes as setting card-issuing municipality data and resident registration codes in the cards' memory elements, and card-face printing, and then are granted by each municipality to residents for use. As the Juki cards goes through these processes, attackers well-versed in IC card technology may exploit the logical interfaces (commands and responses) defined in the Basic Resident Registration card specifications in order to tamper with or steal user data or TSF data.

2) **T.Illegal_Term_Use:**

Attackers other than authorized municipal government staffs who are knowledgeable of the operation of service terminals used with the Basic Resident Registration Network may misuse or modify these terminals to gain unauthorized access to data exchanged with Juki cards or tamper with or steal user data or TSF data.

3) **T.Disturb_APL:**

A Juki card has many applications installed; i.e., user identification applications and municipalty specific applications loaded by the municipalities. Within the Juki card where multiple applications reside, the municipality's proprietary applications may tamper with or steal user data.

4) **T.Environment:**

When a power failure occurs during use of a Juki card, the rewrite of data may be interrupted. Later, when attempting to use the card, the user data or TSF data in the card may not have been rewritten correctly.

5) **T.Incomplete**:

Juki cards delivered to the municipalities will have various user data and TSF data set before they are granted to residents. Attackers may improperly obtain Juki cards that are set with user data and TSF data as described above before they are granted to residents and may misuse them as officially issued cards.

6) **T.Hardware:**

Attackers well versed in semiconductor or cryptographic technology may intercept or tamper with TOE assets or conjecture their secrets using the following means of hardware attacks:

- Using focused ion beam (FIB) workstations, electron beam probers (EBP), or atomic force

microscopes (AFM) to physically tamper with or tap computing circuits or memory elements (i.e., the tampering of the TOE itself or TSF data, or the interception of TSF data)
- Analyzing hardware processing status to infer TSF data
- Operating the IC cards under abnormal operating conditions and analyzing the results to infer the TSF data

3.4 Organizational Security Policy

The security policies for the organizations that use the TOE are as described below:

The Basic Resident Registration Card Specifications Ver.2.3 (**[Juki Specifications 23]**) are specifications for Juki cards but include descriptions that should be considered as organizational security policies. These requirements are as quoted below:

Note: "Security attributes" and "passwords" as mentioned in [**Juki Specifications 23]** correspond to "access control attributes" and "PINs," respectively, as mentioned in this ST. Furthermore, SC3 and SC4 correspond to P-5 or P-6 and N-4 of this ST, respectively.

1) P.Authentication:

In **[Juki Specifications 23]**, there is no descriptions pertaining to security policies with regard to the reading conditions of resident registration codes. From Table 8.9 "Juki Card AP Security Attribute Settings" in Chapter 7 "Juki Card Application Specifications," however, the following conditions are considered as implicitly established security policies:

- PIN-based user authentication has been completed (SC3)
- Municipal authentication based on a certificate issued by the National Juki-Net Center has been completed (SC4)

Note: Table 8.9 indicates access rights. The right to access resident registration codes is granted under the condition that "SC3: PIN-based user identification has been completed," and "SC4: Municipal authentication based on a certificate issued by the National Juki-Net Center has been completed."

2) P.Secret_Setting:

Section 2.3 "Basic Resident Registration Card Service Requirements" (1) in Chapter 1 "Overview" includes a provision that defines that "When setting a card's secret keys, a safe issuance method shall be employed." This needs to be reflected in the implementation of the TOE.

3) P.PIN_Initialize:

Section 2.3 “Basic Resident Registration Card Service Requirements” (3) in Chapter 1 “Overview” includes a provision that defines that “In order to ensure card reuse when the password is forgotten, a method shall be adopted that supports the setting of a new user password after PIN initialization.” This needs to be reflected in the implementation of the TOE.

4) P.Secure_Path:

Section 3.4 “Secure Messaging Functions” in Chapter 7 “Juki Card Application Specifications” includes a provision that defines that “Secure messaging functions are functions that perform encrypted communications to protect APDU, which are exchanged between IC cards and external systems, from unauthorized interception. In the Juki card AP, these functions are used to read resident registration codes.” This needs to be reflected in the implementation of the TOE.

Note: The application protocol data unit (APDU) is the data unit exchanged between Juki cards and card reader/writers. In this ST, APDUs from card reader/writers to Juki cards are referred to as “command messages” and those from Juki cards to card reader/writers are referred to as “response messages.”

4. Security Objectives

This chapter describes the security objectives for the TOE and the TOE environment.
This ST's security objectives for the TOE and the TOE environment are as described below:

4.1 TOE Security Objectives

This section describes security objectives for the TOE. The security objectives for the TOE consist of the following six items:

1) **O.Identification:**

The TSF must provide a mechanism to identify users of the CD management unit, those of the Juki AP, and those of the AP management unit.

2) **O.AccessManagement:**

The TSF must provide a mechanism to restrict the external command based means of accesses to user data and TSF data in the TOE, and allow only TOE-authenticated card issuers, card holders, service terminals, and AP loading administrators to have access only to the assets they are authorized depending on their roles.

3) **O.Domain:**

The TSF must provide a mechanism to protect itself from the municipality's proprietary applications and must prevent accesses to files that are under the control of other applications.

4) **O.Secure_Path:**

The TSF must provide a mechanism to prevent analysis of data formats of the data communicated with card reader/writers.

5) **O.Retention:**

The TSF must provide a mechanism that will restore user data and TSF data that were in use, when restarted in the event of a power failure during the use of a Juki card.

6) **O.Forgery:**

The TSF must provide a mechanism that does not allow the TSF to be used for administrative services until instructions (including the resident setting a password) are given by authenticated TOE-related parties.

4.2 Environmental Security Objectives

This section describes environmental security objectives.

Environmental security objectives consist of the following four items:

1) **OE.CARD_SET_Data:**

Before the TOE is delivered to card holders, municipalities, which are card issuers or AP loading administrators, must provide their personnel with training and education so that they can correctly set safe values in the TOE and safely manage such values.Municipalities must also provide guidance to residents, who are card holders, so that they set an appropriate PIN.

2) **OE.Term_TSF:**

In order to ensure safe management of TSF data used by Juki cards for authentication, card reader/writers and service terminals must erase the PINs that were entered during authentication, after processing them. In order to prevent resident registration codes read from Juki cards from being leaked, card reader/writers and service terminals must erase the codes after their use.

3) **OE.Term_Mgt:**

Service terminals must be used in safe municipal environments. Software running on service terminals must authenticate TOE-related parties to enforce access controls, and shall enable the secret keys of the service terminals to be used only when they are started up by authorized personnel.

4) **OE.Hardware:**

The TOE runs on safe hardware capable of withstanding the attacks listed below which are launched by attackers well-versed in semiconductor and cryptographic technology. The SM4148 IC Card LSI manufactured by Sharp Corporation that ensures this capability is used.

- Using focused ion beam (FIB) workstations, electron beam probers (EBP), or atomic force microscopes (AFM) to physically tamper with or tap computing circuits or memory elements (i.e., the tampering of the TOE itself or TSF data, or the interception of TSF data)
- Analyzing hardware processing status to infer TSF data
- Operating the IC cards under abnormal operating conditions and analyzing the results to infer the TSF data

5. IT Security Requirements

This chapter describes security functional requirements and security assurance requirements. These requirements consist of the functional components of CC Version 2.1 Part 2 and the assurance components of CC Version 2.1 Part 3, respectively.

5.1 TOE Security Requirements

This section describes TOE security functional requirements and security assurance requirements.

5.1.1 TOE Security Functional Requirements

5.1.1.1 Crytographic support (FCS)

This section defines TOE cryptographic support security requirements.

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: **No other components.**

> **FCS_CKM.2.1** The TSF shall distribute cryptographic keys [refinement: ***for distributing session keys***] in accordance with a specified cryptographic key distribution method [assignment: ***Session Key Setup Protocol***] that meets the following: [assignment: Requirement Specifications for Juki Cards Ver. ***2.3 and Requirement Specifications for the AP Management Unit***].

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
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

> **FCS_CKM.4.1** The TSF shall destroy [refinement: ***import keys, fixed keys, session keys, decryption keys for key distribution, and card secret keys in volatile memory***] in accordance with a specified cryptographic key destruction method [assignment: *reset to zero*] that meets the following: [assignment: ***no standard***].

Note: Card-issuing municipality public keys, cryptographic keys for Juki AP key distribution and those for AP management unit key distribution, as well as key management public keys, certificate verification public keys, temporary public keys, certification authority public keys, AP management unit card issuer public keys, and AP loading administrator public keys do not need to be destroyed in accordance with the reset-to-zero method because they are public keys.

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]
FMT_MSA.2 Secure security attributes

FCS_COP.1/T-DES Cryptographic operation

Hierarchical to: No other components.

FCP_COP.1.1/T-DES The TSF shall perform [assignment: ***cryptographic operations listed in Table 5-1***] in accordance with a specified cryptographic algorithm [assignment: ***triple-DES cipher***] and cryptographic key sizes [assignment: ***112 bits, 168 bits***] that meet the following: [assignment: ***ANSI X9.52***].

Note: DES calculation functions, which enable T-DES cryptographic operations, are provided by an IC card LSI on which the TOE runs.

Table 5-1 Triple-DES Cryptographic Operations

Cryptographic operation	Keys used	Key size
Decryption of imported CD management unit card secret keys	Import key	168 bits
Command decryption and response encryption in secure messaging	Juki AP session key	168 bits
	Fixed key, AP management unit session key	112 bits

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
FMT_MSA.2 Secure security attributes

FCS_COP.1/RSA Cryptographic operation

Hierarchical to: No other components.

FCP_COP.1.1/RSA The TSF shall perform [assignment: ***cryptographic operations listed in Table 5-2***] in accordance with a specified cryptographic algorithm [assignment: ***RSA cipher***] and cryptographic key sizes [assignment: ***1,024 bits***] that meet the following: [assignment: ***PKCS#1***].

Table 5-2 RSA Cryptographic Operations

Cryptographic operation	Keys used
Decryption of the authentication codes encrypted with related party's secret key, for the verification of authentication when authenticating externally	Card issuing municipality public key, AP management unit card issuer public key, AP loading administrator public key
Decryption of the distributed (imported) session keys used for secure messaging	Juki AP key distribution decryption key, AP management unit key distribution decryption key
Encryption for the creation of authentication codes for the internal authentication of card holders	CD management unit card secret key, AP management unit card secret key
Verification of the certificates of temporary public keys	Key management public key, certificate verification public key
Verification of the certificates of the card issuer and the AP loading administrator public keys for the AP management unit	Certification authority public key
Decryption of authentication codes encrypted with service terminal secret keys to externaly authenticate service terminals	Temporary public key

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
FMT_MSA.2 Secure security attributes

5.1.1.2 User Data Protection (FDP)

This section defines the TOE user data protection security requirements.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce [assignment: ***Juki card access control SFP***] on [assignment: ***the list of subjects, objects, and operations among subjects and objects***

listed in Table 5-3].

Table 5-3 Subjects, Objects and Operations in the TOE

Subject	Object	Operation
CD management process AP management process Juki AP process	EF (WEF and IEF)	read, write, and rewrite
	SD	AP loading, AP selection, AP deletion

<<Juki card access control SFP>>

Access control is enforced only on the pre-defined subjects, objects and and operations.

Note: “Write” refers to the first occasion of writing values into a data area, and “rewrite” refers to rewriting the values already written in the data area.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *Juki card access control SFP*] to objects based on the following: [assignment: *state transition status, authentication status, and access control attributes*].

Note: Access control attributes are security attributes for objects, and define for each object, the required authentication status to operate on the object.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Based on the authentication status of TOE-related parties authorized to execute operations from the subject to the objects defined in access control rules in Table 5-4 to Table 5-14, operations must be limited to TOE-related parties who satisfy the authorized authentication status*].

Note: In the access control rules listed in **Table 5-4** to **Table 5-14**, “none” means that there is no authentication status that authorizes an access, and “any” means that any authentication status will authorize an access.“P-x” and “N-x” denote an authentication status required for the authorization of an access. The symbol “&” indicates that the two authentication statuses listed are both required, and a slash (/) indicates that either of the two authentication statuses listed is required. Specifically,

in **Table 5-4**, when the state transition status for the subject (CD management process) is of initialization, the reading and writing of the object (municipal data) is allowed but modification is not allowed when the authentication status is of P-1 (PIN verification with the CD management unit transport PIN has been completed). The reading of the object (card type identification data) is possible in all authentication statuses, but the writing and rewrite is not allowed. Furthermore, the reading, writing, and rewrite of the object (CD management unit card secret keys) is allowed if the authentication status is of P-1.

Table 5-4 Access Control Rules of the CD Management Unit (Initialization State)

Subject: CD management process

Object (EF)	Read	Write	Rewrite
Municipal data	P-1	P-1	none
Card type identification data	any	none	none
CD management unit card secret key	P-1	P-1	P-1

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

Table 5-5 Access Control Rules of the CD Management Unit (PIN-Configurable State)

Subject: CD management process

Object (EF)	Read	Write	Rewrite
Municipal data	none	none	none
Card type identification data	any	none	none
CD management unit card secret key	none	none	none

Table 5-6 Access Control Rules of the CD Management Unit (Card Operational State)

Subject: CD management process

Object (EF)	Read	Write	Rewrite
Municipal data	any	none	none
Card type identification data	any	none	none
CD management unit card secret key	any	none	none

Table 5-7 Access Control Rule of the CD Management Unit (Card Invalidated State)

Subject: CD management process

Object (EF)	Read	Write	Rewrite
Municipal data	none	none	none
Card type identification data	none	none	none
CD management unit card secret key	none	none	none

Table 5-8 Access Control Rule of the Juki AP (Initialization State)

Subject: Juki AP process

Object (EF)	Read	Write	Rewrite
Resident registration code	P-1	P-1	none
Juki AP key distribution decryption key	P-1	P-1	none
Juki AP session key	P-1	none	P-1

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

Table 5-9 Access Control Rule of the Juki AP (Locked State)

Subject: Juki AP process

Object (EF)	Read	Write	Rewrite
Resident registration code	none	none	none
Juki AP key distribution decryption key	none	none	none
Juki AP session key	none	none	N-4

N-4: External authentication completed with temporary public key whose certificate has been verified with key management public key in the Juki AP (service terminal)

Table 5-10 Access Control Rule of the Juki AP (AP Selectable State)

Subject: Juki AP process

Object (EF)	Read	Write	Rewrite
Resident registration code	P-6 & N-4	none	none
Juki AP key distribution decryption key	N-4	none	none
Juki AP session key	P-6 & N-4	none	N-4

P-6: Verification of Juki AP holder PIN completed (card holder)

N-4: External authentication completed with temporary public key whose certificate has been verified with key management public key in the Juki AP (service terminal)

Table 5-11 Access Control Rule of the AP Management Unit (Initialization State)

Subject: AP management process

Object (SD)	AP loading	AP selection	AP deletion
root SD	P-7	any	P-7
Object (EF)	Read	Write	Rewrite
Card management data	any	none	none
AP management unit key distribution decryption key	none	P-7	P-7
AP management unit session key	none	none	none

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

Table 5-12 Access Control Rule of the AP Management Unit (Initialized State)

Subject: AP management process

Object (SD)	AP loading	AP selection	AP deletion
root SD	P-7	any	P-7
Object (EF)	Read	Write	Rewrite
Card management data	any	none	none
AP management unit key distribution decryption key	none	P-7	P-7
AP management unit session key	none	none	none

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

Table 5-13 Access Control Rule of the AP Management Unit (Operational State)

Subject: AP management process

Object (SD)	AP loading	AP selection	AP deletion
root SD	N-2/N-5	any	N-2/N-5
Object (EF)	Read	Write	Rewrite
Card management data	any	none	none
AP management unit key distribution decryption key	any	none	none
AP management unit session key	N-2/N-5	none	N-2/N-5

N-2: External authentication completed with card issuer public key in the AP management unit (card issuer)

N-5: External authentication completed with AP loading administrator public key in the AP management unit (AP loading administrator)

Table 5-14 Access Control Rules of the AP Management Unit (Terminated State)

Subject: AP management process

Object (SD)	AP loading	AP selection	AP deletion
root SD	none	none	none
Object (EF)	Read	Write	Rewrite
Card management data	none	none	none
AP management unit key distribution decryption key	none	none	none
AP management unit session key	none	none	none

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: ***none***].

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

FDP_ITC.1 Import of user data without security attributes
Hierarchical to: **No other components.**

FDP_ITC.1.1 The TSF shall enforce the [assignment: ***Juki card access control SFP***] when importing [refinement: ***CD management unit card secret keys, Juki AP session keys, AP management unit session keys, Juki AP key distribution cryptographic keys, and AP management unit key distribution cryptographic keys, which represent***] user data, controlled under SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the [refinement: ***CD management unit card secret keys, Juki AP session keys, AP management unit session keys, Juki AP key distribution cryptographic keys, and AP management unit key distribution cryptographic keys, which represent***] user data, when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing [refinement: ***CD management unit card secret keys, Juki AP session keys, AP management unit session keys, Juki AP key distribution cryptographic keys, and AP management unit key distribution cryptographic keys, which represent***] user data controlled under the SFP from outside the TSC:
[assignment: **none**].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

5.1.1.3 Identification and Authentication (FIA)
This section defines TOE identification and authentication security requirements.

FIA_AFL.1/VERIFY Authentication failure handling
Hierarchical to: No other components.

FIA_AFL.1.1/VERIFY The TSF shall detect when [assignment: ***three consecutive***] unsuccessful authentication attempts occur related to [assignment: ***PIN verification***].

FIA_AFL.1.2/VERIFY When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall: [assignment: *change the state transition status of the PIN in question to blocked state and stop its use for authentication, and when the CD management unit tentative PIN or a Juki AP tentative PIN is set by the card issuer, change the state transition status of the CD management unit tentative PIN or the Juki AP tentative PIN to normal state and remove the blocking of its use for authentication; otherwise, the blocking of the PIN's use cannot be removed*].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1/EXT_AUTH Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1/EXT_AUTH The TSF shall detect when [assignment: *three consecutive*] unsuccessful authentication attempts occur related to [assignment: *external authentication*].

FIA_AFL.1.2/EXT_AUTH When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall: [assignment: *change the state transition status of the public key used for external authentication (excluding temporary public keys) to blocked state and stop its use for authentication; the stop of its use for authentication cannot be unblocked*].

Note: If the use of a public key for authentication is stopped due to authentication failure, the stop cannot be unblocked.

Note: Failure of external authentication using a temporary public key shall be handled as failure of authentication with a pubic key used to verify the certificate of the temporary public key.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *current process identification information, authentication status*].

Dependencies: no dependencies.

Note: Current process identification information refers to information used to identify a currently selected process in operation.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: ***commands that use operations allowed when authentication status is "any" in Table 5-4 to Table 5-14 (select, transport PIN information acquisition, card type identification information acquisition, card state acquisition, random number acquisition, and certificate exchange)***] on behalf 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.

Dependencies: FIA_UID.1 Timing of identification

Note: The foregoing [assignment] describes command names for command messages used in the interfaces with the TOE. Each command requires the execution of the following functions:
Select: Command to switch from one process running on the card to another.
Transport PIN information acquisition: Command to acquire information that identifies transport PINs.
Card type identification information acquisition: Command to acquire data that identify card types.
Card state acquisition: Command to obtain the current transition state of a card as its state changes.
Random number acquisition: Command to obtain random numbers used for external authentication.
Certificate exchange: Command to exchange certificates used for external authentication.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

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

[assignment: *external authentication*].

Dependencies: no dependencies.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [assignment: *the 12 types of authentication mechanisms listed in Table 5-15 depending on the role of TOE-related parties*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules for user authentication mechanisms depending on the role of TOE-related parties listed in Table 5-15*].

Table 5-15 User Authentication Mechanism Rules Corresponding to Roles

Role of TOE -related party	Corresponding user authentication mechanism	Authentication Status
Card issuer	PIN verification using CD management unit transport PINs	P-1
	PIN verification using CD management unit tentative PINs	P-2
	PIN verification using CD management unit proprietary PINs	P-4
	PIN verification using Juki AP tentative PINs	P-5
	External authentication using issuing municipality public keys in the CD management unit	N-1
	PIN verification using AP management unit transport PINs	P-7
	External authentication using card issuer public keys in the AP management unit	N-2
Card holder	PIN verification using CD management unit card holder PINs	P-3
	PIN verification using Juki AP card holder PINs	P-6
Service terminal	External authentication using temporary public keys whose certificate has been verified by certificate verification public keys in the CD management unit	N-3
	External authentication using temporary public keys whose certificate has been verified by key management public keys in the Juki AP	N-4
AP loading administrator	External authentication using AP loading administrator public keys in the AP management unit	N-5

Dependencies: no dependencies.

Note: N-3 is defined as an authentication status. It is, however, not used for access

control or TSF data management but is used to allow reading security attributes of the CD management unit.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *three conditions; i.e., one related to PIN verification and external authentication for the Juki AP when the Juki AP process is re-selected and switched from another process; one related to external authentication for the AP management process when the AP management process is re-selected and switched from another process; and one related to authentications other than PIN verification using a transport PIN, tentative PIN, or card holder PIN for Juki CD or external authentication using card-issuing municipality public keys when the Juki CD process is re-selected and switched from a process other than a Juki CD process or an AP management process*].

Dependencies: no dependencies.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: *Select*] 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.

Dependencies: no dependencies.

Note: “Select” refers to a command name for command messages used in the interfaces with the TOE and requests a switchover of processes running on the card.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of the user: [assignment: *current process identification information*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: ***The first current process identification information at the time of card startup shall be an AP management process***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: ***Current process identification information shall be changed when the process is switched with the Select command***].

Dependencies: FIA_ATD.1 User attribute definition

5.1.1.4 Security Management (FMT)

This section defines TOE security management security requirements.

FMT_MSA.1/STATUS Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1/STATUS The TSF shall enforce [assignment: ***Juki card access control SFP***] to restrict the ability to [selection: ***modify***] the security attributes [assignment: ***state transition status of the CD management unit, the AP management unit, and Juki AP, and the state transition status of PINs used for authentication***] to [assignment: ***card issuers***].

Note: The ability to “modify” the state transition status is restricted to the roles that are allowed operations that involve state transition marked with an asterisk (*) in **Table 5-16** to **Table 5-22**.

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

FMT_MTD.1/IEF Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1/IEF The TSF shall restrict the ability to [selection: ***modify***, [assignment: ***set***]] the [assignment: ***PINs or keys stored in IEF***] to [assignment: ***the***

roles of TOE-related parties allowed in accordance with rules in Table 5-16 to Table 5-26].

Note: In the management rules in **Table 5-16** to **Table 5-26**, "none" means that there is no authentication status that allows the operation."P-x" and "N-x" refer to the authentication status that allows the operations. A slash (/) indicates that either of the two authentication statuses listed is required, and an asterisk (*) shows that the operation involves state transition. Specifically, in **Table 5-16**, when the state transition status is of initialization, TSF data (CD management unit tentative PINs) can be modified and set and TSF data (proprietary PINs, card-issuing municipality public keys, certificate verification public keys, and temporary public keys) can be modified if the authentication status is of P-1 (PIN verification completed using CD management unit transport PINs), but other operations are not allowed. When the setting of TSF data (CD management unit tentative PINs) are operated, the state transition of the CD management unit is effected.

Note: "Modify" refers to changing a value that is already set, and "set" refers to reverting to an unset state and then defining a new value. In the management rules in Tables **Table 5-16** to **Table 5-20**, there are TSF data that are not allowed to be set even in an initialization state. This is because these are considered as "modification" since the manufacturer has already set tentative data at the time of IEF creation.

Note: The CD management unit transport PINs, import keys, fixed keys, and AP management unit transport PINs are pre-set by the manufacturer during fabrication, and except for the modification of the AP management unit transport PINs, these PINs and keys cannot be set or modified by TOE-related parties. CD management unit temporary PINs and CD management unit card holder PINs are stored and managed in the same area as CD management unit PINs, and Juki AP tentative PINs and Juki AP card holder PINs are stored managed in the same area as Juki AP PINs.

Table 5-16 IEF Management Rules of the CD Management Unit (Initialization State)

TSF data (IEF)	Modify	Set
CD management unit PIN	P-1	P-1*
Proprietary PIN	P-1	none
Issuing municipality public key	P-1	none
certificate verification public key	P-1	none
Temporary public key	P-1	none

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

Table 5-17 IEF Management Rules for the CD Management Unit (PIN-Configurable State)

TSF data (IEF)	Modify	Set
CD management unit PIN	P-2*	none
Proprietary PIN	none	none
Issuing municipality public key	none	none
certificate verification public key	none	none
Temporary public key	none	none

P-2: PIN verification with CD management unit tentative PIN completed (card issuer)

Table 5-18 IEF Management Rules of the CD Management Unit (Card Operational State)

TSF data (IEF)	Modify	Set
CD management unit PIN	P-3	N-1*
Proprietary PIN	none	none
Issuing municipality public key	none	none
certificate verification public key	P-4	none
Temporary public key	any	none

P-3: PIN verification with CD management unit holder PIN completed (card holder)

P-4: PIN verification with CD management unit proprietary PIN completed (card issuer)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

Table 5-19 IEF Management Rules of the CD Management Unit (Card Invalidated State)

TSF data (IEF)	Modify	Set
CD management unit card holder PIN	none	none
Proprietary PIN	none	none
Issuing municipality public key	none	none
certificate verification public key	none	none
Temporary public key	none	none

Table 5-20 IEF Management Rules of the Juki AP (Initialization State)

TSF data (IEF)	Modify	Set
Key management public key	**P-1**	none
Temporary public key	**P-1**	none
Juki AP PIN	**P-1**	P-1*
Juki AP key distribution decryption key	**P-1**	none

P-1: PIN verification with CD management unit transport PIN completed (card

issuer)

Table 5-21 IEF Management Rules of the Juki AP (Locked State)

TSF data (IEF)	Modify	Set
Key management public key	none	none
Temporary public key	any	none
Juki AP PIN	P-5*	none
Juki AP key distribution decryption key	none	none

P-5: Verification of Juki AP tentative PINs completed (card issuer)

Table 5-22 IEF Management Rules of the Juki AP (AP-Selectable State)

TSF data (IEF)	Modify	Set
Key management public key	none	none
Temporary public key	any	none
Juki AP PIN	P-6	N-1*
Juki AP key distribution decryption key	none	none

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

P-6: Verification of Juki AP holder PIN completed (card holder)

Table 5-23 IEF Management Rules of the AP Management Unit (Initialization State)

TSF data (IEF)	Modify	Set
AP management unit transport PIN	P-7	none
Certification authority public key	none	P-7
AP management unit card issuer public key	P-7	P-7
AP management unit key distribution decryption key	P-7	P-7

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

Table 5-24 IEF Management Rules of the AP Management Unit (Initialized State)

TSF data (IEF)	Modify	Set
AP management unit transport PIN	P-7	none
Certification authority public key	none	P-7
AP management unit card issuer public key	P-7	P-7
AP management unit key distribution decryption key	P-7	P-7

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

Table 5-25 IEF Management Rules of the AP Management Unit (Operational State)

TSF data (IEF)	Modify	Set
AP management unit transport PIN	none	none
Certification authority public key	none	none
AP management unit card issuer public key	none	none
AP management unit key distribution decryption key	none	none

Table 5-26 IEF Management Rules of the AP Management Unit (Terminated State)

TSF data (IEF)	Modify	Set
AP management unit transport PIN	none	none
Certification authority public key	none	none
AP management unit card issuer public key	none	none
AP management unit key distribution decryption key	none	none

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1/STATUS Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1/STATUS The TSF shall restrict the abilityto [selection: ***modify***] the [assignment: ***state transition status of the CD management unit, Juki AP, and the AP management unit***] to [assignment: ***role of TOE-related parties who has an authentication status in accordance with the rules in Table 5-27 to Table 5-29***].

Note: The codes in **Table 5-27** to **Table 5-29** indicate authentication statuses required for state transition. In **Table 5-27**, for example, this will mean that when the current state of the CD management unit is of “initialization state,” if the CD management unit tentative PIN is set by a role with authentication status “P-1”, the state will transition to “PIN-configurable state.”

Table 5-27 Management Rules of State Transition Statuses in the CD Management Unit

Current Status	State after	Authenticatio	Condition for the transition

	transition	n Status Required	
Initialization State	PIN-configurable State	P-1	Set CD management unit tentative PINs
PIN-configurable State	Card-in-Operation State	P-2	Modify CD management unit holder PINs
PIN-configurable State	Card Invalidated State	P-2	Instruction by command
Card-in-Operation State	PIN-configurable State	N-1	Set CD management unit tentative PINs
Card-in-Operation State	Card Invalidated State	N-1	Instruction by command

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

P-2: PIN verification with CD management unit tentative PIN completed (card issuer)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

Table 5-28 Management Rules of State Transition Statuses in the Juki AP

Current Status	State after transition	Authentication Status Required	Condition for the transition
Initialization State	Locked State	P-1	Set Juki AP tentative PIN
Locked State	AP-selectable State	P-5	Modify Juki AP holder PIN
AP-selectable State	Locked State	N-1	Set Juki AP tentative PIN

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

P-5: Verification of Juki AP tentative PINs completed (card issuer)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

Table 5-29 Management Rules of State Transition Statuses in the AP Management Unit

Current Status	State after transition	Authentication Status Required	Condition for the transition
Initialization State	Initialized State	P-7	Instruction by command
Initialized State	Operational State	P-7	Instruction by command
Initialized State	Terminated State	P-7	Instruction by command
Operational State	Terminated State	N-2	Instruction by command

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

N-2: External authentication completed with card issuer public key in the AP management unit (card issuer)

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: *security management functions listed in Table 5-30*].

Table 5-30 List of Management Functions

Functional requirements	Possible management functions	Functional requirements to implement
FCS_CKM.2	a) Management of changes of cryptographic key attributes. Examples of key attributes include key types, (e.g., public, secret, common), the term of validity, and intended uses (e.g., digital signature, key encryption, key exchange, data encryption)	a) none
FCS_CKM.4	Same as above	a) none
FCS_COP.1/T-DES	No foreseen management activity	No need
FCS_COP.1/RSA	No foreseen management activity	No need
FDP_ACC.1	No foreseen management activity	No need
FDP_ACF.1	a) Management of attributes used for decisions based on explicit access or refusal	a) FMT_MTD.1/IEF
FDP_ITC.1	a) Modification of additional control rules used for import	a) none
FIA_AFL.1/VERIFY	a) Management of thresholds for unsuccessful authentication attempts b) Management of actions taken in the event of authentication failure	a) none b) none
FIA_AFL.1/EXT_AUTH	Same as above	a) none b) none
FIA_ATD.1	a) If indicated in the assignment, the authorization administrator is allowed to define additional security attributes for users.	a) FMT_MTD.1/STATUS
FIA_UAU.1	a) Management of authentication data by administrators b) Management of authentication data by related users c) Management of the list of actions taken before users are authenticated	a) FMT_MTD.1/IEF b) FMT_MTD.1/IEF c) none
FIA_UAU.4	No foreseen management activity	No need
FIA_UAU.5	a) Management of authentication mechanisms b) Management of rules for authentication	a) none b) none
FIA_UAU.6	a) Re-authentication request is included in management actions if the authorization administrator is allowed to	a) none

	request re-authentication	
FIA_UID.1	a) Management of user identification information b) If the authorization administrator is allowed to change actions authorized prior to identification, management of such list of actions	a) none b) none
FIA_USB.1	a) The authorization administrator is allowed to define security attributes for default subjects b) The authorization administrator is allowed to change security attributes for default subjects	a) none b) none
FMT_MSA.1/STATUS	a) Management of the group of security attributes and roles that can affect each other	a) none
FMT_MTD.1/IEF	a) Management of the group of TSF data and roles that can affect each other	a) none
FMT_MTD.1/STATUS	Same as above	a) none
FMT_SMF.1	No foreseen management activity	No need
FMT_SMR.1	a) Management of the group of users that constitute part of the roles	a) none
FPT_RCV.2	a) Management of who is allowed to access recovery capabilities in maintenance mode b) Management of the list of failures/service interruptions processed through automatic procedures	a) none b) none
FPT_RVM.1	No foreseen management activity	No need
FPT_SEP.1	No foreseen management activity	No need
FTP_ITC.1	a) Setting of actions that request trusted channels if supported	a) none

Dependencies: no dependencies.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: ***card issuers, card holders, service terminals, and AP loading administrators***].

FMT_SMR.1.2 The TSF shall be able to associate users with roles [refinement: ***based on the authentication results of the authentication mechanisms listed in Table 5-15***].

Dependencies: FIA_UID.1 Timing of identification

5.1.1.5 Protection of TSF (FPT)

This section defines protection security requirements of the TSF.

FPT_RCV.2 Automated recovery
Hierarchical to: FPT_RCV.1

FPT_RCV.2.1 When automatic recovery from [assignment: ***abnormal termination due to power failure during data writing, command interruption, or communication anomaly***] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

Note: The TSF does not enter maintenance mode since it always returns to a secure state using automated procedures.

FPT_RCV.2.2 For [assignment: ***abnormal termination due to power failure during data writing, command interruption, or communications anomaly***], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

Dependencies: AGD_ADM.1 Administrator guidance
ADV_SPM.1 Informal TOE security policy model

FPT_RVM.1 Non-bypassability of the TSP
Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: no dependencies.

FPT_SEP.1 TSF domain separation
Hierarchical to: **No other components.**

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: no dependencies.

5.1.1.6 Trusted path/channel (FTP)

This section defines trusted path/channel security requirements.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote 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 [selection: ***trusted remote IT products***] to initiate communications via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: ***functions that require secure messaging, the import of CD management unit card secret keys, the reading of individual identification information, and AP loading***].

Dependencies: no dependencies.

5.1.2 Declaration of the Minimum Strength of Function

The minimum strength of function of this ST for the TOE is SOF-basic. This covers functions of the TOE security functional requirements that include permutational or probabilistic mechanisms. The strength of functions for cryptographic algorithms are beyond the scope of evaluation.

5.1.3 TOE Security Assurance Requirements

This section describes the TOE security assurance requirements.

Table 5-31 lists the required components of the TOE security assurance requirements. The EAL4 security assurance requirements are augmented with AVA_MSU.3.

Table 5-31 TOE Assurance Requirements

Class	Component	Name
Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures

	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing -- sample
Vulnerability assessment	AVA_MSU.3	Analysis and testing for insecure states
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.2 IT Environment Security Requirements

5.2.1 IT Environment Security Requirements

There are no security functional requirements for the IT environment.

6. TOE Summary Specifications

This chapter describes the TOE summary specifications.

6.1 IT Security Functions

Table 6-1 indicates the TOE security functional specifications to implement the TOE security functional requirements as described Section **5.1.1** . Correspondences are marked with an “O”.

Table 6-1 Correspondence of TOE Summary Specifications to Security Functional Requirements

	Security Functional requirements \ TOE Summary Specifications	SF.ACCESS_MANAGEMENT	SF.AUTHENTICATE	SF.SECURE_MESSAGING	SF.MANAGEMENT	SF.DOMAIN	SF.RETENTION
1	FCS_CKM.2			O			
2	FCS_CKM.4			O			
3	FCS_COP.1/T-DES			O			
4	FCS_COP.1/RSA		O	O			
5	FDP_ACC.1	O					
6	FDP_ACF.1	O					
7	FDP_ITC.1	O					
8	FIA_AFL.1/VERIFY		O				
9	FIA_AFL.1/EXT_AUTH		O				
10	FIA_ATD.1	O	O		O		
11	FIA_UAU.1		O				
12	FIA_UAU.4		O				
13	FIA_UAU.5		O				
14	FIA_UAU.6		O				
15	FIA_UID.1		O				
16	FIA_USB.1	O	O				
17	FMT_MSA.1/STATUS	O			O		
18	FMT_MTD.1/IEF	O					
19	FMT_MTD.1/STATUS				O		
20	FMT_SMF.1	O			O		
21	FMT_SMR.1	O	O		O		
22	FPT_RCV.2						O
23	FPT_RVM.1	O	O	O	O	O	O
24	FPT_SEP.1	O	O		O	O	
25	FTP_ITC.1			O			

6.1.1 Access Management Functions

SF.ACCESS_MANAGEMENT

TOE assets are placed in one of the three areas: CD management, Juki AP, and AP management areas. These domains are separated by **SF.DOMAIN** so that they can only be accessed by the CD management unit, Juki AP, and the AP management unit, respectively. Each domain is assigned a module in executive format and a data area handled by the module. The modules in each domain can access data in the same domain but cannot access data in other domains.

The CD management unit, Juki AP, and the AP management unit have a data storage area with a file structure as described in **Table 6-2**.

Table 6-2 Data Storage Area

EF	WEF	Record-structured data
	IEF	PIN/key

The basic file EF containts WEF files, which store data used for work in a record structure, and IEF files, which store PINs and keys, and each of these files are assigned access management and other attributes. A security attribute named “SE,” which is used to designate keys used for authentication and encryption, is stored in WEF.

SF.ACCESS_MANAGEMENT controls accesses to all user data stored in WEF and IEF and manages all TSF data. Access control for user data and management of TSF data are collectively referred to as access management here.

Defined by access management attributes, the TOE access management mechanism consist of authentication conditions, states, and operations. Access management attributes are set by card manufacturers and cannot be changed when the TOE is used.

Access management attributes

1) Define authentication conditions required for access management as security attributes named “authentication status.”

Define the authentication conditions of TOE-related parties based on user authentication.

2) Define states in which roles that meet authentication conditions of TOE-related parties can be executed

SF.ACCESS_MANAGEMENT confirms whether these access management attributes satisfy the user authentication conditions and states in the independent CD management, Juki AP, and AP management areas, and if they do, executes the defined operations on the objects that store user data or on the TSF data. Prior to **SF.ACCESS_MANAGEMENT**, **SF.AUTHENTICATE** identifies and authenticates TOE users, the current process identification information accosiate users with subjects, and the authentication statuses specify the role of users.

SF.MANAGEMENT enables each of the CD management unit, Juki AP, and AP management unit modules to maintain their independece, and when an authorized role performs a particular control in a defined state, state transition is effected.

There are three types of access control operations for user data: “read,” “write,” and “rewrite.”“Write” refers to the first occasion of writing values into a data area, and “rewrite” refers to rewriting the values already written in the data area.

There are two types of operations for the management of TSF data stored in IEF: “modify” and “set.”“Modify” refers to changing a value that is already set, and “set” refers to reverting to an unset state and then definining a new value.

The AP management unit has a SD structure as an AP loading area. There are three types of operations for SD: “AP loading,” “AP selection,” and “AP deletion.”

Table 6-3 to Table 6-5 present a summary of the above access management-related rules. With regard to the objects storing user data and the TSF data for each state of the individual modules, the respective table indicates operations authorized according to the role of TOE-related parties that have obtained the authentication statuses mentioned in the table. Note that the symbol “--” indicates that there is no authorized operation **Table 6-3** indicates, for example, that in the CD management unit in an initialization state, the “any” authentication status allows any TOE-related party to perform “read” operations on card type identification data, and that card issuers who have obtained an authentication status of P-1 can perform “read” and “write” operations on municipal data; “read” operations on card type identification data; “read,” “write,” and “rewrite” operations on CD management unit card secret keys; “set” and “modify” operations on CD management unit PINs; and “modify” operations on proprietary PINs, card-issuing municipality public keys, certificate verification public keys, and temporary public keys.

Table 6-3 Access Management in the CD Management Unit

			Object			TSF data				
State	Role of TOE -related party	Authentication Status	Municipal data	Card type identification data	CD management unit card secret key	CD management unit PIN	Proprietary PIN	Issuing municipality public key	certificate verification public key	Temporary public key
Initialization State	TOE-related parties	any	–	Read	–	–	–	–	–	–
	Card issuer	P-1	Read Write	Read	Read Write Rewrite	Set, modify CD management unit tentative PINs	Modify	Modify	Modify	Modify
PIN-configurable State	TOE-related parties	any	–	Read	–	–	–	–	–	–
	Card issuer	P-2	–	Read	–	Modify CD management unit holder PINs	–	–	–	–
Card-in-Operation State	TOE-related parties	any	Read	Read	Read	–	–	–	–	Modify
	Card holder	P-3	Read	Read	Read	Modify CD management unit holder PINs	–	–	–	Modify
	Card issuer	P-4	Read	Read	Read	–	–	–	Modify	Modify
	Card issuer	N-1	Read	Read	Read	Set CD management unit tentative PINs	–	–	–	Modify
Card Invalidated State	TOE-related parties	any	–	–	–	–	–	–	–	–

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

P-2: PIN verification with CD management unit tentative PIN completed (card issuer)

P-3: PIN verification with CD management unit holder PIN completed (card holder)

P-4: PIN verification with CD management unit proprietary PIN completed (card issuer)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

Table 6-4 Access Management in the Juki AP

			Object			TSF data			
State	Role of TOE-related party	Authentication Status	Resident registration code	Juki AP key distribution decryption key	Juki AP session key	Key management public key	Temporary public key	Juki AP PIN	Juki AP key distribution decryption key
Initialization State	TOE-related parties	any	–	–	–	–	–	–	–
	Card issuer	P-1	Read Write	Read Write	Read Rewrite	Modify	Modify	Set, Modify Juki AP tentative PINs	Modify
Locked State	TOE-related parties	any	–	–	–	–	Modify	–	–
	Card issuer	P-5	–	–	–	–	Modify	Modify Juki AP holder PIN	–
	Service terminal	N-4	–	–	Rewrite	–	Modify	–	–
AP-selectable State	TOE-related parties	any	–	–	–	–	Modify	–	–
	Card issuer	N-1	–	–	–	–	Modify	Set Juki AP tentative PIN	–
	Service terminal	N-4	–	Read	Rewrite	–	Modify	–	–

	Card holder	P-6	–	–	–	–	Modify	Modify Juki AP holder PIN	–
	Service terminal and card holder	N-4 & P-6	Read	Read	Read Rewrite	–	Modify	Modify Juki AP holder PIN	–

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

P-5: Verification of Juki AP tentative PINs completed (card issuer)

P-6: Verification of Juki AP holder PIN completed (card holder)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

N-4: External authentication completed with temporary public key whose certificate has been verified with key management public key in the Juki AP (service terminal)

Table 6-5 Access Management in the AP Management Unit

			Object				TSF data			
State	Role of TOE -related party	Authentication Status	Root SD	Card management data	AP management unit key distribution decryption key	AP management unit session key	AP management unit transport PIN	Certification authority public key	AP management unit card issuer public key	AP management unit key distribution decryption key
Initialization State	TOE-related parties	any	AP selection	Read	–	–	–	–	–	–
	Card issuer	P-7	AP loading AP selection AP deletion	Read	Write Rewrite	–	Modify	Set	Set Modify	Set Modify
Initialized State	TOE-related parties	any	AP selection	Read	–	–	–	–	–	–
	Card issuer	P-7	AP loading	Read	Write	–	Modify	Set	Set	Set

			AP selection AP deletion		Rewrite				Modify	Modify
Operational State	TOE-related parties	any	AP selection	Read	Read	-	-	-	-	-
	Card issuer	N-2	AP loading AP selection AP deletion	Read	Read	Read Rewrite	-	-	-	-
	AP loading administrator	N-5	AP loading AP selection AP deletion	Read	Read	Read Rewrite	-	-	-	-
Terminated State	TOE-related parties	any	-	-	-	-	-	-	-	-

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

N-2: External authentication completed with card issuer public key in the AP management unit (card issuer)

N-5: External authentication completed with AP loading administrator public key in the AP management unit (AP loading administrator)

6.1.2 Identification and Authentication Functions

SF.AUTHENTICATE

SF.AUTHENTICATE identifies users when either the CD management unit, the AP management unit, or Juki AP is selected by the Select command. The identified users and the processes that runs on behalf of users are associated with each other through identification information of the current process. The Select command changes the identification information of the current process, and the first process that runs upon card startup is the AP management process. **SF.AUTHENTICATE** performs PIN verification and external authentication to authenticate the users for which the CD management process, the Juki AP process, or the AP management process runs. In addition, **SF.AUTHENTICATE** allows only the execution of the Select command without user identification, and allows the execution of commands for Select, transport PIN information acquisition, card type identification information acquisition, card state acquisition, random number acquisition, and certificate exchange without user identification.

PIN verification:

The IEF in the TOE that stores PIN information is designated from a service terminal and the user's PIN is transmitted. **SF.AUTHENTICATE** compares the user PIN received with the PIN in the designated PIN information storage IEF, and if they match, it sets the authentication status as PIN verification complete with the target PIN.PIN verification deals with 3- to 16-byte PINs.(PINs are imported to the PIN information storage IEF with **SF.ACCESS_MANAGEMENT.**)

External authentication:

Users are authenticated in the manner described below by using a pair of the user's public key and secret key to verify using the public keys stored in IEF within the TOE, that a random numbers generated by the TOE is correctly encrypted with the user's secret key at the service terminal.

(1) The TOE generates a random number and sends it to the service terminal.

(2) Using the corresponding secret key, the service terminal encrypts the random number and sends it to the TOE as an authentication code.

(3) **SF.AUTHENTICATE** uses the public key that corresponds with the secret key to decrypt the authentication code it receives in the CD management process or Juki AP process and compares the decrypted code with the random number. If they match, it sets the authentication status as external authentication completed with the public key used for decryption.

There are two cases in external authentication: one in which public keys of corresponding TOE-related parties stored in IEF of the TOE in advance are used, and the other in which the service terminal sends a certificate with their signed public key to the TOE (certificate verification command), which uses the certificate it receives as a verified public key (temporary public key).(Modification of key management public keys and temporary keys are done by **SF.ACCESS_MANAGEMENT.**)

Service terminals have secret keys for certificate verification. The Juki CD uses certificate verification public keys that correspond with the secret keys, and the Juki AP users key management public keys that correspond with the secret keys.

Table 6-6 lists the cryptographic operations performed in external authentication for SF.AUTHENTICATE and the keys used.

Table 6-6 Cryptographic Operations Performed in External Authentication and the Keys Used

Cryptographic operation	Keys used	Algorithm	Key size
Decryption of authentication codes encrypted with secret keys of related party's to verify the authentication when authenticating externally	Card issuing municipality public key, AP management unit card issuer public key, AP loading administrator public key	RSA	1024 bits
Verification of the certificates of temporary public keys	Key management public key, certificate verification public key	RSA	1024 bits
Decryption of authentication codes encrypted with service terminal secret keys to externaly authenticate service terminals	Temporary public key	RSA	1024 bits

RSA cipher that conforms to PKCS#1 is provided as cryptographic functions for encryption and decryption.

The number of attempts allowed is established for each PIN and public key (excluding temporary public keys), and for PIN verification and external authentication using the PIN or public key stored in the card, the number of consecutive unsuccessful attempts made until successful termination is kept as an error counter. Failure of external authentication using a temporary public key shall be handled as failure of authentication with a pubic key used to verify the certificate of the temporary public key. The allowed retry count may have an upper limit or may be limitless. The allowed number of retries is set to “three attempts” by the manufacturer in advance, and cannot be changed by TOE-related parties. If the value on the error counter reaches this upper limit, the relevant key or PIN is set to blocked state. Authentication using a blocked key is not possible. State transition of PINs and public keys

are managed independently, and the default state value when the card is issued is normal state while the default error counter value is zero. When a card issuer sets a CD management unit tentative PIN while the CD management unit is in card operational state, and when the card issuer sets a Juki AP tentative PIN while the Juki AP is in AP-selectable state, the state transition status of the relevant CD management unit tentative PIN or Juki AP tentative PIN is returned to the normal state, making the PIN usable for authentication. Once the other PINs and public keys enter a blocked state, they cannot be returned to a normal state.

The authentication status for the CD management unit, the Juki AP, and the AP management unit represents information that includes the results of PIN verification or external authentication and is managed in accordance with rules as shown in Table 6-7. Authentication status is maintained also when a state transitions. As a result, when the Juki AP is re-selected, re-authentication will be required for PIN verification and external authentication, and when the AP management unit is re-selected, re-authentication will be required for external authentication.

Table 6-7 Authentication Status Management Rules

1.	The authentication status established with PIN verification using transport PINs, tentative PINs, or card holder PINs in the CD management unit or with external authentication using card-issuing municipality public keys is effective until the card is deactivated. Authentication status established with PIN verification or external authentication using other PINs or keys is effective while the CD management unit or the AP management unit is selected.
2.	Authentication status established with PIN verification or external authentication in Juki AP is effective while the Juki AP is selected.
3.	Authentication status established with PIN verification in the AP management unit is effective until the card is deactivated, and authentication status established with external authentication in the AP management unit is effective while the unit is selected.
4.	If there is a changeover of APs other than those mentioned above, authentication status is inherited.
5.	An already established authentication status is cleared if external authentication for the AP management unit is re-started, and for other cases, the status is cleared if PIN verification or external authentication fails.

The external authentication procedure in the AP management unit involves the card and the service terminal mutually exchanging random numbers and certificates generated and mutually verifying the certificates exchanged, then transmitting data obtained by encrypting a session key and a hash value for the random number both generated by the service terminal using the terminal's secret key. The AP management unit performs external authentication by decrypting the data using the public key that corresponds to the terminal's certificate verified in advance.

Table 6-8 Correspondence of Authentication Mechanism and the Role of Related Parties

Roles of TOE -related parties	Authentication mechanism
Card issuer	PIN verification using CD management unit transport PINs PIN verification using CD management unit tentative PINs PIN verification using CD management unit proprietary PINs PIN verification using Juki AP tentative PINs External authentication using issuing municipality public keys in the CD management unit PIN verification using AP management unit transport PINs External authentication using card issuer public keys in the AP management unit
Card holder	PIN verification using CD management unit card holder PINs PIN verification using Juki AP card holder PINs
Service terminal	External authentication using temporary public keys whose certificate has been verified by certificate verification public keys in the Juki CD External authentication using temporary public keys whose certificate has been verified by key management public keys in the Juki AP
AP loading administrator	External authentication using AP loading administrator public keys in the AP management unit

6.1.3 Cryptographic Communication Functions

SF.SECURE_MESSAGING

SF.SECURE_MESSAGING implements secure messaging for the communications between the CD management unit, Juki AP or the AP management unit and service terminals, and encrypts commands and responses exchanged with the service terminals.

When the CD management unit receives a command from a service terminal designating the use of secure messaging, secure messaging is enforced. The same key is used to encrypt and decrypt communications between the TOE and service terminals. As the common key for the CD management unit, the fixed key pre-set by the card manufacturer is used as the cryptographic communication key.

In the Juki AP, when a command to read personal identification information is received from a service terminal, secure messaging is enforced, and the resident registration code read is encrypted.

When the AP management unit receives a command from a service terminal designating the use of secure messaging, secure messaging is enforced. The same key is used to encrypt and decrypt communications between the TOE and service terminals.

In the Juki AP and the AP management unit, the Juki AP session key and AP management unit session key are used, respectively, as common keys to encrypt and decrypt communications with service terminals. These session keys are generated by service terminals and are delivered to the TOE using cryptographic communications. In accordance with the session key setup protocol defined in **[Juki Specification 23]** and the requirement specifications for the AP management unit, key distribution cryptographic keys used for distribution are delivered to service terminals.Key distribution cryptographic keys are

imported as user data without attribute information when the card is issued.(They are imported into the TOE with **SF.ACCESS_MANAGEMENT**.)

Service terminals use the key distribution cryptographic keys (Juki AP key distribution cryptographic key or AP management unit key distribution cryptographic key) delivered by the TOE to encrypt session keys and perform key distribution. The Juki AP or the AP management unit decrypts the encrypted session key using a session key distribution decryption key (Juki AP key distribution decryption key or AP management unit key distribution decryption key) and obtains a session key. After decryption, the session key distribution decryption key residing in the volatile memory is reset to zero.

The session key shared in the AP management unit after authentication (AP management unit session key) is retained in the AP management area, and is used for subsequent processing jobs.

Table 6-9 shows the cryptographic operations performed in the cryptographic communications of **SF.SECURE_MESSAGING** and the keys used for such communications.

Table 6-9 Cryptographic Operations Performed in Cryptographic Communications and the Keys Used

Cryptographic operation	Keys used	Algorithm	Key size
Command decryption and response encryption in secure messaging	Juki AP: Juki AP session key	Triple-DES	168 bits
	CD management unit: fixed key AP management unit: AP management unit session key	Triple-DES	112 bits
Decryption of the distributed (imported) session keys used for secure messaging	Juki AP key distribution decryption key AP management unit key distribution decryption key	RSA	1024 bits

Triple-DES cipher, which conforms with ANSI X.9.52, and RSA cipher, which conforms PKCS#1, are provided as cryptographic functions used for encryption and decryption. The hardware implements the calculation functions of DES cipher, and the TOE (which is software) sets the data to be calculated and the cryptographic key and uses them as triple-DES cipher. After calculation, the cryptographic key set in volatile memory of the hardware is reset to zero and discarded.

The fixed key in the volatile memory, which was used in the CD management unit, is reset

to zero and discarded immediately after calculation. The session key in the volatile memory, which was used in the Juki AP, is reset to zero and discarded when the process is switched over by the Select command. The session key in the volatile memory, which was used in the AP management unit, is reset to zero and discarded in accordance with the management rules specified in **Table 6-10**.

Table 6-10 Management Rules for Session Keys in the AP Management Unit

1.	Session key is reset to zero when the process is switched over by the Select command.
2.	Session key is reset to zero when the next external authentication command is initiated.
3.	Session key is reset to zero if the decryption of cryptographic communication fails.

The CD management unit card secret key generated by a service terminal is imported into the card in accordance with the card secret key setup protocol defined in **[Juki Specification 23].**(The key is imported into the TOE with **SF.ACCESS_MANAGEMENT**.)The CD management unit card secret key is encrypted using a key called “import key.”The CD management unit reads the pre-set import key in the card and uses it for decryption in the volatile memory. After decryption, the import key residing in the volatile memory is reset to zero.

Table 6-11 shows the cryptographic operations performed in **SF.SECURE_MESSAGING** in relation with card secret keys and the keys used for these operations.

Table 6-11 Cryptographic Operations Performed in Relation with Card Secret Keys and the Keys Used

Cryptographic operation	Keys used	Algorithm	Key size
Decryption of imported CD management unit card secret keys	Import key	Triple-DES	168 bits
Encryption for the creation of authentication codes for the internal authentication of card holders	CD management unit card secret key, AP management unit card secret key	RSA	1024 bits

The CD management unit card secret key is imported as user data without attribute information, and is subject to access control via **SF.ACCESS_MANAGEMENT**. After being read out by a “read” operation, it is used for encryption to create authentication codes in the “internal authentication” command for card holders. The AP management unit card secret key which is identical to the AP management unit key distribution decryption key is managed by **SF.ACCESS_MANAGEMENT** as TSF data and is used for encryption to create

authentication codes in internal authentication of the AP management unit. The their use, the CD management unit card secret key and AP management unit card secret key in the volatile memory are reset to zero and discarded. While the TOE implements cryptographic operations using RSA secret keys, these operations do not provide any security function to protect the assets assumed by the TOE of this ST.

6.1.4 Execution Management Functions

SF.MANAGEMENT

The TOE defines the independent states of the three modules; i.e., the CD management unit, Juki AP, and the AP management unit, and provides controls to enable the roles authenticated and authorized by the TOE within the defined state to perform operations on the assets.

SF.MANAGEMENT manages state transitions, and **SF.ACCESS_MANAGEMENT** restricts executable operations in each state. **SF.MANAGEMENT** retains the state transition statuses of each of the CD management unit, Juki AP, and AP management unit modules, and effects state transition only when a TOE-related party authorized to perform an operations involving state transition executes such an operation.

Table 6-12 shows state transition status management rules for the state transition of each module. **Table 6-12** also indicates the authentication statuses and conditions required for the state transition of each module. In the CD management unit, for example, the transition from initialization state to PIN-configurable state requires a card issuer whose authentication status is P-1 to set a tentative PIN.

Table 6-12 State Transition Status Management Rules

Module	State transition	Authentication Status	Condition for the transition
CD management unit	Initialization => PIN configurable	P-1	Set tentative PIN
	PIN configurable => Card operational	P-2	Modify holder PIN
	Card operational => Card invalidated	N-1	Instruction by command
	PIN configurable => Card invalidated	P-2	Instruction by command
	Card operational => PIN configurable	N-1	Set tentative PIN
AP management unit	Initialization => Initialized	P-7	Instruction by command
	Initialized => Operational	P-7	Instruction by command
	Operational => Terminated	N-2	Instruction by command
	Initialized => Terminated	P-7	Instruction by command
Juki AP	Initialization => Locked	P-1	Set tentative PIN
	Locked => AP selectable	P-5	Modify holder PIN

	AP selectable => Locked	N-1	Set tentative PIN

P-1: PIN verification with CD management unit transport PIN completed (card issuer)

P-2: PIN verification with CD management unit temporary PIN completed (card issuer)

P-5: Verification of Juki AP tentative PINs completed (card issuer)

P7: PIN Verification with AP management unit transport PIN completed (card issuer)

N-1: External authentication completed with issuing municipality public key in the CD management unit (card issuer)

N-2: External authentication completed with card issuer public key in the AP management unit (card issuer)

While each of the CD management unit, the AP management unit, and Juki AP modules is running as a process, the operations allowed on user data and TSF data are controlled by their state transition status. As a result, the TOE controls whether to execute the commands issued by service terminals depending on the state transition status of each module. It refuses the execution of a command if the operation required by the command is not authorized.

6.1.5 Domain Separation Functions

SF.DOMAIN

Domain separation functions involve placing restrictions on applications loaded into the card and accessible data areas for access control so that the CD management area can only be accessed from the CD management unit, the AP management area from the AP management unit, and the Juki AP area from the Juki AP.

SF.DOMAIN divides the memory area of the Juki card into several areas in order to control writing and reading in the memory area. It identifies the addresses of the memory areas where the currently running program is loaded and where the data accessed by the running program is stored, and determines which of the divided memory areas the addresses corresponds to. Whether or not reading from and writing to the memory area where the data is stored from the area the program is loaded is managed by a table, and the reading and writing are controlled by the values in this table. The table, which manages whether to allow reading and writing, is set by the manufacturer along with loading programs during the fabrication phase, and the settings of table cannot be changed when cards are in use as Juki cards.

6.1.6 Data Restoration Functions

SF.RETENTION

When processing any command that requires the operation of security functions in the CD management unit, the AP management unit, or the Juki AP, **SF.RETENTION** initiates a transaction when processing data writes. If the process ends successfully, SF.RETENTION effectuates the content written during the processing and ends the transaction, and if the process ends unsuccessfully due to command interruption or communication failures, it discards the content written during the transaction and ends the transaction.

SF.RETENTION controls all accesses to flash memory and constantly monitors the flash memory to determine whether a power failure has occurred while data in the flash memory were being changed for data writing or deletion. SF.RETENTION examines the memory access state flag during initial startup and automatically recovers to the correct state according to the type of data that was being accessed when the last operation ended and to the state of failures, if any. Since automatic recovery does not fail, no manual recovery maintenance mode is provided.

The original user data and TSF data values are retained when applying any changes to them, allowing data to be restored using the retained values when changes did not complete successfully.

6.2 Strength of Security Functions

In the TOE of this ST, the following security functions are implemented using probabilistic or permutational mechanisms: PIN verification and external authentication functions realized by **SF.AUTHENTICATE**, secure messaging functions realized by **SF.SECURE_MESSAGING**, and encryption functions used when importing user data.

The encryption functions for secure messaging and importing are implemented using cryptographic algorithms. Since cryptographic algorithms are not covered by the evaluation of the strength of security functions, these two functions are also not covered by the evaluation.

PIN verification includes probabilistic mechanisms making it possible for attackers to perform probabilistic attempts, but during the fabrication phase, the manufacturer sets the maximum number of retries allowed to three times, and this value cannot be changed by any of the TOE-related parties. Three- to 16-byte PINs can be set, and if PIN verification fails for three consecutive times, the relevant PIN or public key will enter a blocked state and will become unusable for subsequent authentications.

External authentication uses cryptographic algorithms for authentication but cryptographic algorithms are not covered by the evaluation of the strength of security functions.However, the authentication include probabilistic mechanisms because it uses random numbers making it possible for attackers to perform probabilistic attempts, and the size of the random numbers used is 127 bytes for the Juki CD unit and the Juki AP and 16 bytes for the AP management unit. But even when considering the AP management unit whose strength of security functions is low, it would require, on average, 2^{127} retries for a successful replay attack, which means that the strength satisfies the requirements for SOF-basic.

Therefore, the probabilistic or permutational mechanisms included in the TOE of this ST are PIN verification and external authentication, and both PIN verification and external authentication achieve the SOF-basic strength of security functions.

6.3 Means of Assurance

The assurance requirements of EAL4 augmented are satisfied by creating the documents that describe the means of assurance indicated in **Table 6-13**. In addition, this ST titled "Adapter-compatible High-speed Juki Card Software Security Target" is also available as a document to be referenced when meeting the assurance requirements of the ASE class and those listed below.

Table 6-13 Means of Assurance

Assurance Requirement Component		Assurance Method (reference documents)
ACM_AUT.1	Partial CM automation	Adapter-compatible High-speed Juki Card Software ver.2.0 Configuration Management Rules AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Version Management Rules AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration List AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration Management Records AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Version Management Records
ACM_CAP.4	Generation support and acceptance procedures	
ACM_SCP.2	Problem tracking CM coverage	
ADO_DEL.2	Detection of modification	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Guidance General Document AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Delivery and Operation General Document AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Module Management Ledger
ADO_IGS.1	Installation, generation, and start-up procedures	
ADV_FSP.2	Fully defined external interfaces	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Functional Specifications
ADV_HLD.2	Security enforcing high-level design	AP Execution Environment Operation Manual Juki CD Unit Functional Specifications CM Unit Functional Specifications Juki AP Unit Functional Specifications Security Library for CC Authentication - Functional Specifications Common RAM Management Library for CC Authentication - Functional Specifications Flash Management Library for CC Authentication - Functional Specifications
ADV_IMP.1	Subset of the implementation of the TSF	AP Execution Environment Source Codes Juki CD Unit Source Codes CM Unit Source Codes Juki AP Unit Source Codes Security Library for CC Authentication - Source

		Codes Common RAM Management Library for CC Authentication - Source Codes Flash Management Library for CC Authentication - Source Codes
ADV_LLD.1	Descriptive low-level design	AP Execution Environment Detailed Design Specifications Juki CD Unit Detailed Design Specifications CM Unit Detailed Design Specifications Juki AP Unit Detailed Design Specifications Security Library for CC Authentication - Detailed Design Specifications Common RAM Management Library for CC Authentication - Detailed Design Specifications Flash Management Library for CC Authentication - Detailed Design Specifications
ADV_RCR.1	Informal correspondence demonstration	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Correspondence Table AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Security Functional Requirements Correspondence Table AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 TOE Summary Specifications Paragraph Correspondence Table AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Detailed Design Specifications
ADV_SPM.1	Informal security policy model	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Security Policy Model
AGD_ADM.1	Administrator guidance	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Card Issuer Guidance Document AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 AP Loading Administrator Guidance Document
AGD_USR.1	User guidance	
ALC_DVS.1	Identification of security measures	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Development Security Management Rules AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Document Management Rules
ALC_LCD.1	Developer defined life-cycle model	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Life Cycle Model
ALC_TAT.1	Well-defined development tools	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Development Tool Management Rules AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Tool Management Records
ATE_COV.2	Analysis of coverage	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Item Correspondence Table
ATE_DPT.1	Testing: high-level design	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Depth Analysis Document

ATE_FUN.1	Functional test	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Items AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Testing Procedures AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Results
ATE_IND.2	Independent testing -- sample	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Environment AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Programs AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Test Data AdapterAdapter-compatible High-speed Juki Card Software ver.2.00
AVA_MSU.3	Analysis and testing for insecure states	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Developer Misuse Prevention Analysis Report
AVA_SOF.1	Strength of TOE security function evaluation	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Developer Strength of Security Function Evaluation Report
AVA_VLA.2	Independent vulnerability analysis	AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Developer Vulnerability Analysis Report

7. PP Claims

This chapter describes references as well as the refinements and augmentations to the PP.

7.1 PP References

There are no PPs to which this ST conforms.

7.2 PP Refinements

There are no refinements to any PPs in this ST.

7.3 PP Augmentations

There are no augmentations to any PPs in this ST.

8. Rationales

This chapter describes rationales for what have been stated in the sections up to Chapter 7.

8.1 Rationales for the Security Objectives

Table 8-1 indicates how the security objectives of the TOE and its environment correspond to the threats, assumptions, and organizational policy in this ST.

Table 8-1 Correspondence of Security Environment to Security Objectives

Security Environment \ Security Objectives		TOE Objectives						Environmental Objectives			
		1) O.Identification	2) O.AccessManagement	3) O.Domain	4) O.Secure_Path	5) O.Retention	6) O.Forgery	1) OE.CARD_SET_Data	2) OE.Term_TSF	3) OE.Term_Mgt	4) OE.Hardware
Threats	1) T.Logical_attack	X	X								
	2) T.Illegal_Term_use								X	X	
	3) T.Distub_APL			X							
	4) T.Environment					X					
	5) T.Incomplete						X				
	6) T.Hardware										X
Assumptions	1) A.CARD_SET_Data							X	X	X	
Organizational Policy	1) P.Authentication	X	X								
	2) P.Secret_Setting	X	X								
	3) P.PIN_Initialize	X	X								
	4) P.Secure_Path				X						

The rationales for the six threats are as described below:

1) **T.Logical_Attack** is countered with **O.Identification** and **O.AccessManagement**.

Users (users of the CD management unit, Juki AP, and the AP management unit) who access from outside the TOE are identified by **O.Identification**.

In addition, **O.AccessManagement** authenticates users that correspond to roles, clarifying user data and TSF data that can only be accessed by card issuers, card holders, and

authenticated TOE-related parties, and as a result, preventing the exploitation of the user data and TSF data. Furthermore, **O.AccessManagement** restricts means of access to user data and TSF data in the TOE from outside the TOE to operations based on authorized commands.

2) **T.Illegal_Term_Use** is countered with **OE.Term_TSF** and **OE.Term_Mgt**.

When TOE-related parties are authenticated, data used for authentication are transmitted to the TOE from outside via card reader/writers. After the processing by **OE.Term_TSF** is completed, these data are erased to protect them from leakage. If the equipment is ever stolen, data exploitation can be prevented through the unauthorized use prevention mechanism provided by **OE.Term_Mgt.**

3) **T.Disturb_APL** is countered with **O.Domain**.

O.Domain clarifies files that are placed under the control of an application, preventing accesses (read, write, etc.) to files that are managed by other applications.

4) **T.Environment** is countered with **O.Retention**.

O.Retention provides a mechanism to restore user data and TSF data when a power failure occurs during the use of Juki cards.

5) **T.Incomplete** is countered with **O.Forgery**.

If a Juki card is ever stolen before being granted to a resident, **O.Forgery** prevents the card to be used for administrative services by people other than TOE-related parties authenticated by the TOE.

6) **T.Hardware** is countered with **OE.Hardware**.

OE.Hardware ensures the security of the hardware running the TOE.

The rationales for the single assumption is as described below:

1) **A.CARD_SET_Data** is countered with **OE.CARD_SET_Data**, **OE.Term_TSF**, and **OE.Term_Mgt**.

Outside the TOE, the TOE-related parties who know the TSF are card issuers, card holders, service terminals, and the AP loading administrators. Training and guidance are provided so that appropriate values are set by **OE.CARD_SET_Data** for TSF data related to card issuers and card holders. **OE.Term_TSF** protects service terminals from the leakage of secrets, and **OE.Term_Mgt** ensures that service terminals are handled by authorized personnel.

The rationales for the four organizational security policies are as described below:

1) **P.Authentication** is countered with **O.Identification** and **O.AccessManagement**.

O.Identification identifies users (users of the CD management unit, Juki AP, and the AP management unit) who access from outside the TOE, and **O.AccessManagement** limits accesses (read) to user data (resident registration codes) to TOE-related parties who have finished resident authentication and issuer (municipality) authentication.

2) P.Secret_Setting is countered with **O.Identification** and **O.AccessManagement**.

O.Identification identifies users (users of the CD management unit, Juki AP, and the AP management unit) who access from outside the TOE, and **O.AccessManagement** restricts the setting of TSF data (key) to card issuers.

3) **P.PIN_Initilize** is countered with **O.Identificationb** and **O.AccessManagement**.

Since **[Juki Specification 23]** does not specify who has the PIN initialization rights, it is considered that the right to **P.PIN_Initialize** lies with card issuers. **O.Identification** and **O.AccessManagement** guarantee that only authenticated card issuers can gain the access required for setting tentative PINs, which are TSF data, in Juki cards.

4) **P.Secure_Path** is countered with **O.Secure_Path**.

Since **O.Secure_Path** takes measures to prevent analysis of data formats for communications between Juki cards and card reader/writers, user data and TSF data cannot be deduced even if communications data are intercepted.

8.2 Rationales for the Security Requirements

8.2.1 Rationales for the TOE Security Functional Requirements

Table 8-2 indicates how the security functional requirements correspond to the security objectives. TEO security functional requirements meet all security objectives, and all security functional requirements contribute to one or more security objectives.

Table 8-2 Correspondence of Security Objectives to Security Requirements

Security Objectives / Security Functional Requirements	TOE Objectives					
	O.Identification	O.AccessManagement	O.Domain	O.Secure_Path	O.Retention	O.Forgery
FCS_CKM.2				X		
FCS_CKM.4				X		
FCS_COP.1/T-DES				X		
FCS_COP.1/RSA		X				
FDP_ACC.1		@		&		@
FDP_ACF.1		@		&		@
FDP_ITC.1		@		X		
FIA_AFL.1/VERIFY		X				
FIA_AFL.1/EXT_AUTH		X				
FIA_ATD.1	@	@				@
FIA_UAU.1		@				
FIA_UAU.4		X				
FIA_UAU.5		@				
FIA_UAU.6		X				
FIA_UID.1	X	&				&
FIA_USB.1	@	@				
FMT_MSA.1/STATUS		@				
FMT_MTD.1/IEF		@				@
FMT_MTD.1/STATUS		@				@
FMT_SMF.1		@				@
FMT_SMR.1		@				@
FPT_RCV.2					@	
FPT_RVM.1	@	@	@	@	@	@
FPT_SEP.1	@	@	@			@
FTP_ITC.1				@		
AGD_ADM.1					&	
ADV_SPM.1					&	

Note: The symbols in the table have the following meanings:Blanks indicate that there is no relationship.

@: Main security functional requirement for the security objective

X: Security functional requirement that enhances the main security functional

requirement for the security objective

&: Security requirement required due to the dependency of the security functional requirement marked with @ or X.

The rationale for the sufficiency of the security functional requirements covering the security objectives is as described below. While there are four objectives cited as environmental security objectives, there are none related to the IT environment.

1) **O.Identification** is a security objective to allow the TSF to identify users, and the main security functions of **O.Identification** are fulfilled by the following five functional requirements:

FIA_ATD.1 (User attribute definition)
FIA_UID.1 (Timing of identification)
FIA_USB.1 (User-subject binding)
FPT_RVM.1 (Non-bypassability of the TSP)
FPT_SEP.1 (Domain separation)

FAI_USB.1 associates a user identified by transmitting the Select command with a process that is selected and run on the card as a subject on behalf of the user by using the current process's identification information. **FIA_ATD.1** acts on behalf of a user who accesses the TOE, that is, users of the CD management unit, Juki AP, and the AP management unit, and maintains identification information of the current process running in the card as a subject.
In addition, mediated actions that TSF can perform prior to identification are limited to "select" defined in **FIA_UID.1**.
Furthermore, in order to prevent each functional requirement from being bypassed, **FPT_RVM.1** always requires invocation of identification functions before other TOE functions are activated, and in order to protect each functional requirement from unauthorized interference, **FPT_SEP.1** separates and maintains the separation of the TSF and subject domains.

2) **O.AccessManagement** is a security objective to allow the TSF to authenticate users and limit accesses to assets, and the main security function of **O.AccessManagement** are fulfilled by the following 14 functional requirements:

FIA_ATD.1 (User attribute definition)
FIA_UAU.1 (Timing of authentication)
FIA_UAU.5 (Multiple authentication mechanisms)
FIA_USB.1 (User-subject binding)
FDP_ACC.1 (Subset access control)
FDP_ACF.1 (Security attribute based access control)
FDP_SMF.1 (Specification of management functions)

FMT_MSA.1/STATUS (Management of security attributes)

FMT_MTD.1/IEF (TSF data management)

FMT_MTD.1/STATUS (TSF data management)

FMT_SMR.1 (Security role)

FPT_RVM.1 (Non-bypassability of the TSP)

FPT_SEP.1 (Domain separation)

FAI_USB.1 associates a user identified by transmitting the Select command with a process that is selected and run on the card as a subject on behalf of the user by using the current process's identification information. **FIA_ATD.1** acts on behalf of a user who accesses the TOE, that is, users of the CD management unit, Juki AP, and the AP management unit, and maintains the identification information of the process running in the card as a subject and the authentication statuses that represent the authentication results of the roles of users. **FIA_UAU.1** clarifies TSF-mediated actions provided without TOE identification and authentication processing. In other words, identification and authentication are mandatory for TSF-mediated actions not listed in the assignment for **FIA_UAU.1**. The list of specific TOE-related parties (card issuers, card holders, service terminals, and AP loading administrators), possible operations, and assets is clarified by **FDP_ACC.1**, and the rules to be applied then are specified by **FDP_ACF.1**.

FIA_UAU.5 clarifies user authentication mechanisms supported by the TOE. The roles of TOE-related parties authenticated based on the authentication mechanisms defined in **FIA_UAU.5** are maintained by **FMT_SMR.1**, making the managerial roles (setting of keys, tentative PINs, and status required to make the TOE available for administrative services) with regard to the TOE of the Juki cards clear. **FMT_SMF.1** makes it clear that actions that are considered as management function for the security functional requirements **FDP_ACF.1**, **FIA_ATD.1**, and **FIA_UAU.1** are enabled by **FMT_MTD.1/IEF** and **FMT_MTD.1/STATUS**. In addition, **FMT_MTD.1/IEF** clarifies the relationship between managerial roles and TSF data, and **FMT_MTD.1/STATUS** manages state transition in accordance with the operations on objects. Furthermore, **FMT_MSA.1/STATUS** clarifies methods of managing security attributes. These requirements are necessary to ensure that requirements that correspond to the TOE security objectives are applied efficiently.

Furthermore, in order to prevent each functional requirement from being bypassed, **FPT_RVM.1** always requires invocation of access control functions before other TOE functions are activated, and in order to protect each functional requirement from unauthorized interference, **FPT_SEP.1** separates and maintains the separation of the TSF and subject domains.

The following are six supporting requirements that enhance **O.AccessManagement.**

FIA_AFL.1/VERIFY,**FIA_AFL.1/EXT_AUTH** (Authentication failure handling)

FIA_UAU.4 (Single-use authentication mechanisms)

FIA_UAU.6 (Reauthentication)

FDP_ITC.1 (Import of user data without security attributes)

FCS_COP.1/RSA (Cryptographic operation)

FIA_AFL.1/VERIFY and **FIA_AFL.1/EXT_AUTH** clarify the behavior of TSF when authentication fails, reducing attackers' chances to launch attacks. The authentication mechanism of service terminals used for issuing Juki cards and providing other Juki-related services makes it difficult to spoof as a card issuing service terminal because **FIA_UAU.4** requires the generation of non-reusable authentication data such as challenges. **FIA_UAU.6** clarifies the timing of re-authentication, preventing assets deployed in the work area from being leaked.

The external authentication mechanism of the service terminals used for the issuing of Juki cards and provision of other services, which is one of the authentication mechanisms defined in **FIA_UAU.5**, uses algorithms specified in **FCS_COP.1/RSA**. The initial settings of keys are imported into the TOE from outside in accordance with the policies defined in **FDP_ACC.1** and **FDP_ACF.1** and specified in **FDP_ITC.1**.

FIA_UID.1, a requirement needed due to the dependency of **FIA_UAU.1** and **FMT_SMR.1**, clarifies the timing of user identification. **FMT_MSA.3** will also be needed due to dependencies but is excluded from the dependencies because all objects are already created at the time of manufacture and the default values cannot be overwritten.

3) **O.Domain**, a security objective to protect the TSF from applications and allow the TSF to prevent access to files placed under the control of other applications, is fulfilled by the following two functional requirements:

FPT_RVM.1 (Non-bypassability of the TSP)

FPT_SEP.1 (Domain separation)

FPT_SEP.1 protects the TSF from the municipality's proprietary applications, based on the area in which applications are loaded or data are stored. These domains are also protected by dividing the TSF into the CD management unit, the Juki AP, and the AP management unit. Furthermore, in order to prevent each functional requirement from being bypassed, **FPT_RVM.1** always requires invocation identification functions before other TOE functions are activated.

4) **O.Secure_Path** is a security objective to allow the TSF to prevent the analysis of communications data formats, and the main security function of **O.Secure_Path** is fulfilled by the following two functional requirements:

FTP_ITC.1 (Inter-TSF trusted channel)

FDP_ITC.1 (Import of user data without security attributes)

FTP_ITC.1 enforces measures to prevent tampering of communications data and leakage of confidential information in communication channels between the TOE and remote IT

products. Additionally, the cryptographic keys used are imported into the TOE from outside in accordance with the policies defined in **FDP_ACC.1** and **FDP_ACF.1** and specified in **FDP_ITC.1**.

The following are four supporting requirements that enhance **O.Secure_Path:**

FCS_CKM.2 (Cryptographic key distribution)

FCS_CKM.4 (Cryptographic key destruction)

FCS_COP.1/T-DES (Cryptographic operation)

FPT_RVM.1 (Non-bypassability of the TSP)

In order to reinforce **FTP_ITC.1**, cryptographic operations using the algorithms and key size specified in **FCS_COP.1/T-DES**, the key distribution specified in **FCS_CKM.2**, and key destruction of **FCS_CKM.4** are used as measures to prevent tampering and leakage. The initial settings of keys are defined in **FDP_ACC.1** and **FDP_ACF.1**, and imported into the TOE from outside in accordance with the policy specified in **FDP_ITC.1**.

FDP_ACC.1 and **FDP_ACF.1** are requirements needed due to dependencies. Policies for the setting, distribution, and destruction of keys used for the encryption of the communication channel are defined in **FDP_ACC.1** and **FDP_ACF.1**. **FMT_MSA.3** will also be necessary due to dependencies but is excluded from dependencies since the alternative initial values cannot be specified to overwrite the default values of the initial key settings.

Furthermore, in order to prevent functions related to the encryption of communications data from being bypassed, **FPT_RVM.1** enforces the keys to be used for cryptographic operations to be always shared before starting any communications.

5) **O.Retention** is a security objective to allow the TSF to restore data that was in use when a power failure occurred, and the main security function of **O.Retention** is fulfilled by the following two functional requirements:

FPT_RCV.2 (Automated recovery)

FPT_RVM.1 (Non-bypassability of the TSP)

If a power failure occurs during a data write, **FPT_RCV.2** allows the detection of a previous data write interruption on the next occasion of card activation, and the restoration of the correct user data and TSF data depending on how the data write was interrupted.

AGD_ADM.1 and **ADV_SPM.1** are requirements needed due to dependencies. A**GD_ADM.1** describes the maintenance mode for functional requirements, and **ADV_SPM.1** describes what the secure state is.

Any time a failure occurs, **FPT_RVM.1** requires the functional requirements of **FPT_RCV.2** to be invoked allowing the correct data to be restored.

6) **O.Forgery** is a security objective to allow the TSF to restrict executable functions until it receives instructions from TOE-related parties, and the main security function of **O.Forgery**

is fulfilled by the following nine functional requirements:

FIA_ATD.1 (User attribute definition)

FDP_ACC.1 (Subset access control)

FDP_ACF.1 (Security attribute based access control)

FMT_MTD.1/IEF (TSF data management)

FMT_MTD.1/STATUS (TSF data management)

FMT_SMR.1 (Security role)

FMT_SMF.1 (Specification of management functions)

FPT_RVM.1 (Non-bypassability of the TSP)

FPT_SEP.1 (Domain separation)

FIA_ATD.1 acts on behalf of a user who access the TOE, that is, users of the CD management unit, Juki AP, and the AP management unit, and maintains the identification information of the process running in the card as a subject and the authentication statuses that represent the authentication results of the roles of users. **FMT_MTD.1/STATUS** enforces the management of the state of the TOE in its state transition. The list of TOE-related parties (card issuers, card holders, service terminals, and the AP loading administrators), possible operations, and assets, is clarified by **FDP_ACC.1**, and the applicable rules of each of the states managed according to **FMT_MTD.1/STATUS** are specified by **FDP_ACF.1** and **FMT_MTD.1/IEF**.**FMT_SMR.1** defines roles that make the provision of administrative services possible, and since **FMT_SMF.1** makes it clear that actions that are considered as management functions for the security functional requirements of **FDP_ACC.1** and **FIA_ATD.1** are implemented by **FMT_MTD.1/IEF** and **FMT_MTD.1/STATUS**, cards cannot be exploited even if they are stolen before they are issued.

Furthermore, in order to prevent each functional requirement from being bypassed, **FPT_RVM.1** always requires invocation of identification functions before other TOE functions are activated, and in order to protect each functional requirement from unauthorized interference, **FPT_SEP.1** separates and maintains the separation of the TSF and subject domains.

FIA_UID.1 is a requirement needed due to dependencies since it clarifies the timing of identification.

8.2.2 Verification of the Dependencies of Security Functional Requirements

Table 8-3 shows the correspondences between the security functional requirements of the TOE. The column indicating rationales shows the row numbers (#) in the same table for other security functional requirements on which the security functional requirement depends or the section numbers in this ST where the relevant explanations are given. Security functional requirements with no dependencies are denoted by the symbol "-."Components that are delimited by a slash (/) in the brackets indicate that either of the components is required and either can be selected. Of the selectable components, those that are not covered as dependencies by security functional requirements of the TOE are indicated as "Not selected" in the rationales column.

The components #1, #2, #3, #4, #6, and #7 do not satisfy the dependencies defined in CC Part 2 (**[CC-2]**). However, the reasons for the omission of dependencies are described in Section **8.2.3** . Otherwise, all other dependencies are satisfied.Regarding component #22, the dependencies for **FPT_RCV.2** are satisfied by the security assurance requirements set forth in Section 5.1.3 .

Table 8-3 Dependencies of Security Functional requirements

#	Component	Name	Dependencies	Rationales
1	**FCS_CKM.2**	Cryptographic key distribution	[FDP_ITC.1 /FDP_ITC.2 /FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	#7 Not selected Not selected #2 Section 8.2.3
2	**FCS_CKM.4**	Cryptographic key destruction	[FDP_ITC.1 /FDP_ITC.2 /FCS_CKM.1] FMT_MSA.2	#7 Not selected Not selected Section 8.2.3
3	**FCS_COP.1/T-DES**	Cryptographic operation	[FDP_ITC.1 /FDP_ITC.2 /FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	#7 Not selected Not selected #2 Section 8.2.3
4	**FCS_COP.1/RSA**	Cryptographic operation	[FDP_ITC.1 /FDP_ITC.2 /FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	#7 Not selected Not selected #2 Section 8.2.3
5	**FDP_ACC.1**	Subset access control	FDP_ACF.1	#6
6	**FDP_ACF.1**	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	#5 Section 8.2.3
7	**FDP_ITC.1**	Import of user data without security attributes	[FDP_ACC.1 /FDP_IFC.1] FMT_MSA.3	#5 Not selected Section 8.2.3
8	**FIA_AFL.1/VERIFY**	Authentication failure handling	FIA_UAU.1	#11
9	**FIA_AFL.1/EXT_AUTH**	Authentication failure handling	FIA_UAU.1	#11
10	**FIA_ATD.1**	User attribute definition	none	-
11	**FIA_UAU.1**	Timing of authentication	FIA_UID.1	#15

12	**FIA_UAU.4**	Single-use authentication mechanisms	none	-
13	**FIA_UAU.5**	Multiple authentication mechanisms	none	-
14	**FIA_UAU.6**	Re-authenticating	none	-
15	**FIA_UID.1**	Timing of identification	none	-
16	**FIA_USB.1**	User-subject binding	FIA_ATD.1	#10
17	**FMT_MSA.1/STATUS**	Management of security attributes	[FDP_ACC.1 /FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	#6 Not selected #21 #22
18	**FMT_MTD.1/IEF**	TSF data management	FMT_SMF.1 FMT_SMR.1	#21 #22
19	**FMT_MTD.1/STATUS**	TSF data management	FMT_SMF.1 FMT_SMR.1	#21 #22
20	**FMT_SMF.1**	Specification of management functions	none	-
21	**FMT_SMR.1**	Security role	FIA_UID.1	#15
22	**FPT_RCV.2**	Automated recovery	AGD_ADM.1 ADV_SPM.1	Section 5.1.3 Section 5.1.3
23	**FPT_RVM.1**	Non-bypassability of the TSP	none	-
24	**FPT_SEP.1**	TSF domain separation	none	-
25	**FTP_ITC.1**	Inter-TSF trusted channel	none	-

Table 8-4 indicates the dependencies of functional components, showing their direct, indirect, or optionally selected dependencies. The columns indicate the components depended on by the functional components, and the rows list all the functional components. Symbols in the cells of the table indicate that the component of the corresponding column is directly required (marked with an “X”) or optionally required (marked with an “O”) by the component of the corresponding row. Components that are selected are marked with @. Those which do not have any symbol in their row mean that they do not depend on other components. Functional components required by the TOE are displayed in bold letters. Components omitted in accordance with rationale explanations are marked with an asterisk (*). In order to satisfy the dependencies of all functional components, all components comprising the columns need to be a TOE requirement, but components that are not a requirement (those not displayed in bold letters) are not required because alternatives are selected or because they are omitted in accordance with rationale explanations. Therefore, there are no dependencies lacking as required by the TOE.

Table 8-4 Dependencies of Security Functional requirements

	Depended Security Requirements / Security Functional Requirements	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_ITC.1	FDP_ITC.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2(*)	FMT_MSA.3(*)	FMT_SMF.1	FMT_SMR.1	AGD_ADM.1	ADV_SPM.1
1	FCS_CKM.2	O	X				@	O					X					
2	FCS_CKM.4	O					@	O					X					
3	FCS_COP.1/T-DES	O	X				@	O					X					
4	FCS_COP.1/RSA	O	X				@	O					X					
5	FDP_ACC.1				X													
6	FDP_ACF.1			X										X				
7	FDP_ITC.1			@		O								X				
8	FIA_AFL.1/VERIFY									X								
9	FIA_AFL.1/EXT_AUTH									X								
10	FIA_ATD.1																	
11	FIA_UAU.1										X							
12	FIA_UAU.4																	
13	FIA_UAU.5																	
14	FIA_UAU.6																	
15	FIA_UID.1																	
16	FIA_USB.1								X									
17	FMT_MSA.1/STATUS			@		O									X	X		
18	FMT_MTD.1/IEF														X	X		
19	FMT_MTD.1/STATUS														X	X		
20	FMT_SMF.1																	
21	FMT_SMR.1										X							
22	FPT_RCV.2																X	X
23	FPT_RVM.1																	
24	FPT_SEP.1																	
25	FTP_ITC.1																	

8.2.3 Reasons for Omissions of Dependencies

As shown in **Table 8-3**, in terms of the dependencies of the TOE security functional requirements, **FCS_CKM.2**, **FCS_CKM.4**, **FCS_COP.1/T-DES**, and **FCS_COP.1/RSA** require **FMT_MSA.2**, and **FDP_ACF.1** and **FDP_ITC.1** require **FMT_MSA.3**, but both are not provided by this TOE.

In this ST, in order to implement the functions of authentication and secure messaging for service terminals, FCS_COP.1 requires the use of cryptographic algorithms.However, the keys required for these algorithms are generated by the issuer of Juki cards, and values confirmed as safe by the card-issuing municipality are entered as the keys. Since safe keys are generated outside the TOE, it is not necessary for the TOE to confirm their safety, and

therefore FMT_MSA.2 is excluded from the security functional requirements.

Objects that are subject to access control in this ST are all generated at the time of manufacture, and the default values cannot be overwritten. Therefore, **FMT_MSA.3** is excluded from the security functional requirements.

Due to the dependencies of **FCS_COP.1/RSA**, **FDP_ITC.1**, **FDP_ITC.2**, or **FCS_CKM.1** is required. Public keys used for external authentication and key distribution decryption keys used for decryption of encrypted session keys are generated and provided outside the TOE, but these keys are considered as TSF data and are “set” and “modified” in accordance with TSF data management rules and not imported as user data.

8.2.4 Mutually Complementary Security Functional Requirements

In the relationship of dependencies between the TOE security functional requirements as shown in Section **8.2.2** , security functions with dependencies complement the other.
In order to achieve the control of access to user data and TSF data provided by **FDP_ACC.1**, **FDP_ACF.1**, and **FMT_MTD.1/IEF**, the non-bypassability of **FPT_RVM.1** and the domain separation functions of **FPT_SEP.1** provide the complementation.

8.2.5 Competition of Security Function Requirements

While the TOE provides security functional requirements for identification and authentication, access control, cryptographic communications, execution management, domain separation, and data restoration, the TOE runs in a single-process LSI, and its processing sequence is determined in advance, therefore, no competition occurs among these security functional requirements.

8.2.6 Validity of Minimum Function Strength Levels

The TOE of this ST focuses on the safety of handling personal information, and is distributed nation-wide to many residents to be used for personal identification as well as for the use in various administrative services provided by the municipalities. The Juki cards require functions to identify and authenticate users associated with authorized roles. While Juki cards handle personal information, it does not handle monetary assets as in financial cards.

Therefore, SOF-Basic which is resistant to attacks by attackers with low attack potential is appropriate for the security mechanism of the authentication for the TOE.

8.2.7 Validity of the Security Assurance Requirements

The wide range of administrative service related information stored on Juki cards is attractive to criminals. And once any technical defects of Juki cards are exploited to commit forgery, the extent of the impact on society will be significant, and therefore, Juki cards are required to provide a high level of reliability. In general, ensuring a high level of reliability would require a certain amount of cost for development and security evaluations, which in turn would affect the price of the cards.

Therefore, EAL4, the highest assurance level for consumer products, is an appropriate choice since it encompasses evaluations of low-level designs and source codes and also evaluates details of the TOE, thereby achieving a high level of reliability.

Additionally, since Juki cards are granted to residents and used by them, they may be used improperly. For this reason, in the development phase, it is necessary to analyze insecure situations caused by improper uses of the TOE from various viewpoints, and the assurance against improper use is reinforced with the augmentation of AVA_MSU.3. The augmentation of AVA_MSU.3 requires ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, and AGD_USR.1 as dependencies, but the same or higher level assurance requirements are already chosen, therefore satisfying the dependencies of the assurance requirements.

8.2.8 Mutually Complementary Security Functional Requirements

Table 8-5 indicates the mutually complementary security functional requirements and security objectives.

Table 8-5 Mutually Complementary Security Functional requirements and Security Objectives

Objectives		Complementary Security Requirements
TOE	1) O.Identification	FIA_ATD.1, FIA_UID.1, FIA_USB.1, FPT_RVM.1, FPT_SEP.1
	2) O.AccessManagement	FCS_COP.1/RSA, FDP_ACC.1, FDA_ACF.1, FDP_ITC.1, FIA_AFL.1/VERIFY, FIA_AFL.1/EXT_AUTH, FIA_ATD.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, FIA_USB.1, FMT_MSA.1/STATUS, FMT_MTD.1/IEF, FMT_MTD.1/STATUS, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1
	3) O.Domain	FIA_ATD.1, FPT_RVM.1, FPT_SEP.1
	4) O.Secure_Path	FCS_CKM.2, FCS_CKM.4, FCS_COP.1/T-DES, FDP_ACC.1, FDA_ACF.1, FDP_ITC.1, FTP_ITC.1, FPT_RVM.1
	5) O.Retention	FPT_RCV.2, FPT_RVM.1
	6) O.Forgery	FDP_ACC.1, FDA_ACF.1, FIA_UID.1, FMT_MTD.1/STATUS, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1

The TOE has only logical interfaces as its external interfaces and does not have interfaces that allow the portion of mutually supporting functional requirements as cited in **Table 8-5** that is executed to be bypassed from outside Juki cards, look at the progress in the processing of the portion, or halt the processing. Any municipality proprietary application loaded in response to a resident's request are beyond the scope of the TOE, but the TSF are protected with FPT_RVM.1 and FPT_SEP.1, preventing the processing in the TOE from being bypassed, spied on, or halted. Programs that comprise the TOE are protected with FPT_SEP.1 from interferences and program code modifications by unreliable subjects in the TOE while they are running.

Since Juki card TOE does not record the execution of security functions, it does not provide any means of protecting recording functions. Functions are executed in the TOE by commands sent from systems external to the TOE, and since logs of the commands that have been sent are kept on the external systems as records, those records can be used for audits.

8.3 TOE Summary Specification Rationales

8.3.1 Rationales for TOE Security Functions

Table 6-1 indicates how security functional requirements correspond to TOE summary specifications. All security functional requirements are met by one or more TOE summary specifications, satisfying the sufficiency of security functional requirements. In addition, one or more security functional requirements correspond to the TOE summary specifications, satisfying the necessity of implementation.

The following explains the validity of the implementations for each of the security functional requirements.

8.3.1.1 Crytographic support (FCS)

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2 is a functional requirement for the distribution of cryptographic keys for key distribution.

SF.SECURE_MESSAGING distributes cryptographic keys for key distribution when receiving session keys generated and distributed by service terminals. Therefore, **FCS_CKM.2** is satisfied by **SF.SECURE_MESSAGING**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 is a functional requirement for key destruction achieved by resetting to zero.

SF.SECURE_MESSAGING resets fixed keys and session keys used for cryptographic communications, key distribution decryption keys used to distribute session keys, import keys used to import secret keys, and card secret keys used in cryptographic operations to zero after they are used on the volatile memory, and destroys them.

Therefore, **FCS_CKM.4** is satisfied by **SF.SECURE_MESSAGING**.

FCS_COP.1 Cryptographic operations

FCS_COP.1/T-DES is a functional requirement for triple-DES ciphers.

SF.SECURE_MESSAGING uses triple-DES cipher when encrypting secure messaging data and importing CD management unit card secret keys.

Therefore, **FCS_COP.1/T-DES** is satisfied by SF.SECURE_MESSAGING.

SF.AUTHENTICATE provides RSA encryption functions used for external authentication.

FCS_COP.1/RSA is a functional requirement for RSA cipher.

SF.SECURE_MESSAGING uses RSA encryption which is performed for card secret keys and

for the distribution of session keys used for secure messaging.

Therefore, **FCS_COP.1/RSA** is satisfied by **SF.AUTHENTICATE** and **SF.SECURE_MESSAGING**.

8.3.1.2 User Data Protection (FDP)

FDP_ACC.1 Subset access control

FDP_ACC.1 is a functional requirement for the operation of access control.

In each of the CD management, AP management, and Juki AP processes, **SF.ACCESS_MANAGEMENT** enforces access control on subjects and objects, as well as operations between them, in accordance with the rules listed in **Table 6-3** to **Table 6-5**.

Therefore, **FDP_ACC.1** is satisfied by **SF.ACCESS_MANAGEMENT**.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1 is a functional requirement for the enforcement of access control.

In each of the CD management, AP management, and Juki AP processes, **SF.ACCESS_MANAGEMENT** enforces access control based on the state of security attributes in accordance with the rules listed in **Table 6-3** to **Table 6-5**.

Therefore, **FDP_ACF.1** is satisfied by **SF.ACCESS_MANAGEMENT.**

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1 is a functional requirement for the import of user data.

SF.ACCESS_MANAGEMENT imports, without security attributes, the session keys used to encrypt secure messaging, key distribution encryption used to distribute session keys, and CD management unit card secret keys for card holders.

Therefore, **FDP_ITC.1** is satisfied by **SF.ACCESS_MANAGEMENT**.

8.3.1.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1/VERIFY is a functional requirement for the handling of authentication failures for PIN verification.

If the number of consecutive failures for PIN verification exceeds the preset number of retries allowed, **SF.AUTHENTICATE** enforces a block state on the verified PIN stored in the corresponding IEF so that it cannot be used for subsequent authentications, and allows the card issuer to release the block.

Therefore, **FIA_AFL.1/VERIFY** is satisfied by **SF.AUTHENTICATE**.

FIA_AFL.1/EXT_AUTH is a functional requirement for the handling of authentication failure for external authentication.

If the number of consecutive failures for external authentication exceeds the preset number of retries allowed, **SF.AUTHENTICATE** enforces a block state on the public key stored in the corresponding IEF so that it cannot be used for subsequent authentications and does not allow its release for use.

Therefore, **FIA_AFL.1/EXT_AUTH** is satisfied by **SF.AUTHENTICATE**.

FIA_ATD.1 User attribute definition

FIA_ATD.1 is a functional requirement for the definition of user attributes.

SF.ACCESS_MANAGEMENT uses for access control, the party number or node number that corresponds to the IEF in which the verified PINs maintained in the CD management unit, the AP management unit, and Juki AP or the externally authenticated public keys are stored.

SF.MANAGEMENT uses for execution management, the party number or node number that corresponds to the IEF in which the verified PINs maintained in the CD management unit, the AP management unit, and Juki AP or the externally authenticated public keys are stored.

SF.AUTHENTICATE maintains the party number or node number that corresponds to the IEF in which the verified PINs or the externally authenticated public keys are stored.

Therefore, **FIA_ATD.1** is satisfied by **SF.ACCESS_MANAGEMENT**, **SF.MANAGEMENT**, and **SF.AUTHENTICATE**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1 is a functional requirement for the timing of authentication.

Irrespective of whether authenticated or not, **SF.AUTHENTICATE** authorizes the execution of select, transport PIN information acquisition, card type identification information acquisition, card state acquisition, the acquisition of random numbers, and certificate exchange.

Therefore, **FIA_UAU.1** is satisfied by **SF.AUTHENTICATE.**

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4 is a functional requirement for single-use authentication mechanisms.

SF.AUTHENTICATE enforces the use of newly generated random numbers for each authentication attempt of an external authentication.

Therefore, **FIA_UAU.4** is satisfied by **SF.AUTHENTICATE.**

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5 is a functional requirement for multiple authentication mechanisms.

In the CD management unit, **SF.AUTHENTICATE** matches a TOE-related party with either the CD management unit transport PIN, CD management unit tentative PIN, or CD management unit card holder PIN for authentication.
In the Juki AP, **SF.AUTHENTICATE** matches a TOE-related party with a Juki AP tentative PIN or Juki AP card holder PIN for authentication.
In the AP management unit, **SF.AUTHENTICATE** matches a TOE-related party with an AP management unit transport PIN for authentication.
In the CD management unit, **SF.AUTHENTICATE** uses the card-issuing municipality public keys to authenticate card issuers, and uses the temporary public keys whose certificate have been verified with certificate verification public keys to authenticate service terminals.
In the Juki AP, **SF.AUTHENTICATE** uses the card-issuing municipality public keys to authenticate card issuers, and uses the temporary public keys whose certificate have been verified with key management public keys to authenticate service terminals.
In the AP management unit, **SF.AUTHENTICATE** uses the card issuer public keys to authenticate card issuers.
In the AP management unit, **SF.AUTHENTICATE** uses the AP loading administrators public keys to authenticate the AP loading administrators.
Therefore, **FIA_UAU.5** is satisfied by **SF.AUTHENTICATE**.

FIA_UAU.6 Re-authenticating

FIA_UAU.6 is a functional requirement for re-authentication.
When the Juki AP unit is re-selected, **SF.AUTHENTICATE** demands re-authentication with PIN verification and external authentication, and when the AP management unit is re-selected, it demands re-authentication with external authentication.
Therefore, **FIA_UAU.6** is satisfied by **SF.AUTHETICATE**.

FIA_UID.1 Timing of identification

FIA_UID.1 is a functional requirement for the timing of identification.
SF.AUTHENTICATE authorizes only the execution of the Select command for all users without requiring identification of the users.
Therefore, **FIA_UID.1** is satisfied by **SF.AUTHENTICATE**.

FIA_USB.1 User-subject binding

FIA_USB.1 is a functional requirement for the association of users to subjects.
For access control, **SF.ACCESS_MANAGEMENT** uses the current process identification information that associates an identified user with the process that is running on the user's behalf as a subject.
Using the current process identification information, **SF.AUTHENTICATE** associates the user that sent the Select command with the process that was selected and is running on the

user's behalf as a subject.

Therefore, **FIA_USB.1** is satisfied by **SF.ACCESS_MANAGEMENT** and **SF.AUTHENTICATE**.

8.3.1.4 Security Management (FMT)

FMT_MSA.1 Management of security attributes

FMT_MSA.1/STATUS is a functional requirement for the management of state transition statuses, which are a security attribute.

In the CD management unit and Juki AP, **SF.ACCESS_MANAGEMENT** performs the management of state transition statuses, which are a security attribute for the PINs used for authentication in accordance with the rules listed in **Table 6-3** and **Table 6-4**. In **Table 6-3** and **Table 6-4**, only card issuers can set new tentative PINs and modify the state transition status.

In the CD management unit, the Juki AP, and the AP management unit, **SF.MANAGEMENT** performs the management of the state transition status, which is a security attribute for each of the modules, in accordance with the management rules listed in **Table 6-12**. In **Table 6-12**, only card issuers can modify the state transition status.

Therefore, **FMT_MSA.1/STATUS** is satisfied by **SF.ACCESS_MANAGEMENT** and **SF.MANAGEMENT**.

FMT_MTD.1 TSF data management

FMT_MTD.1/IEF is a functional requirement for the management of PINs and keys, both of which are TSF data.

In the CD management unit, the AP management unit, and the Juki AP, **SF.ACCESS_MANAGEMENT** manages PINs and keys, both of which are TSF data, in accordance with the rules listed in **Table 6-3** to **Table 6-5**. The rules in **Table 6-3** enforce the IEF management rules of the CD management unit in **Table 5-16** to **Table 5-19**, those in **Table 6-4** enforce the IEF management rules of the Juki AP in **Table 5-20** to **Table 5-22**, and those in **Table 6-5** enforce the IEF management rules of the AP management unit in **Table 5-23** to **Table 5-26**.

Therefore, **FMT_MTD.1/IEF** is satisfied by **SF.ACCESS_MANAGEMENT**.

FMT_MTD.1/STATUS is a functional requirement for the management of state transition statuses, which are TSF data.

In the CD management unit, the AP management unit, and Juki AP, **SF.MANAGEMENT** manages the state transition statuses, which are TSF data, in accordance with the management rules listed in **Table 6-12**. Management rules in **Table 6-12** enforce the state

transition status management rules in **Table 5-27** to **Table 5-29**.

Therefore, **FMT_MTD.1/STATUS** is satisfied by **SF.MANAGEMENT**.

FMT_SMF.1 Specification of management functions

FMT_SMF.1 is a functional requirement for the specification of management functions.

Table 8-6 shows a list of security functions that implement the management functions and explains rationales for cases where there are no such security functions.

SF.ACCESS_MANAGEMENT enforces the rules used for access authorization decisions in access control by **FDP_ACF.1** and implements management functions for the PINs and public keys, both of which are authentication data used for authentication by **FIA_UAU.1**.

SF.MANAGEMENT implements the management function for the current process identification information and authentication statuses, both of which are user security attributes used in **FIA_ATD.1**.

Therefore, **FMT_SMF.1** is satisfied by **SF.ACCESS_MANAGEMENT** and **SF.MANAGEMENT**.

Table 8-6 List of Management Functions and Rationale Explanations

Functional requirements	Possible management functions	Security functions to implement
FCS_CKM.2	a) Management of changes of cryptographic key attributes. Examples of key attributes include key types, (e.g., public, secret, common), the term of validity, and intended uses (e.g., digital signature, key encryption, key exchange, data encryption)	a) None (cryptographic key attributes cannot be changed)
FCS_CKM.4	Same as above	a) None (cryptographic key attributes cannot be changed)
FCS_COP.1/T-DES	No foreseen management activity	No need
FCS_COP.1/RSA	No foreseen management activity	No need
FDP_ACC.1	No foreseen management activity	No need
FDP_ACF.1	a) Management of attributes used for decisions based on explicit access or refusal	a) SF.ACCESS_MANAGEMENT
FDP_ITC.1	a) Modification of additional control rules used for import	a) None (Rules cannot be modified)
FIA_AFL.1/VERIFY	a) Management of thresholds for unsuccessful authentication attempts b) Management of actions taken in the event of authentication failure	a) None (Thresholds are fixed) b) None (Actions taken are fixed)
FIA_AFL.1/EXT_AUTH	Same as above	a) None (Thresholds are fixed) b) None (Actions taken are fixed)
FIA_ATD.1	a) If indicated in the assignment, the authorization administrator is allowed to define additional security attributes for users.	a) SF.MANAGEMENT
FIA_UAU.1	a) Management of authentication data by administrators b) Management of authentication data by related users c) Management of the list of actions taken before users are authenticated	a) SF.ACCESS_MANAGEMENT b) SF.ACCESS_MANAGEMENT c) None (Actions taken are fixed)
FIA_UAU.4	No foreseen management activity	No need
FIA_UAU.5	a) Management of authentication mechanisms b) Management of rules for authentication	a) None (Authentication mechanisms are fixed) b) None (Rules for authentication are fixed)
FIA_UAU.6	a) Re-authentication request is included in management actions if the authorization administrator is allowed to request re-authentication	a) None (Even authorized users cannot request re-authentication)
FIA_UID.1	a) Management of user identification information b) If the authorization administrator is allowed to change actions authorized prior to identification, management of	a) None (User identification information is fixed) b) None (Actions cannot be changed)

	such list of actions	
FIA_USB.1	a) The authorization administrator is allowed to define security attributes for default subjects b) The authorization administrator is allowed to change security attributes for default subjects	a) None (Default subjects are fixed) b) None (Default subjects cannot be changed)
FMT_MSA.1/STATUS	a) Management of the group of security attributes and roles that can affect each other	a) None (groups do not exist)
FMT_MTD.1/IEF	a) Management of the group of TSF data and roles that can affect each other	a) None (groups do not exist)
FMT_MTD.1/STATUS	Same as above	a) None (groups do not exist)
FMT_SMF.1	No foreseen management activity	No need
FMT_SMR.1	a) Management of the group of users that constitute part of the roles	a) None (groups do not exist)
FPT_RCV.2	a) Management of who is allowed to access recovery capabilities in maintenance mode b) Management of the list of failures/service interruptions processed through automatic procedures	a) None (The TSF does not enter maintenance mode) b) (The list of failures/service interruptions is fixed)
FPT_RVM.1	No foreseen management activity	No need
FPT_SEP.1	No foreseen management activity	No need
FTP_ITC.1	a) Setting of actions that request trusted channels if supported	a) None (Actions that request trusted channels are fixed)

FMT_SMR.1 Security roles

FMT_SMR.1 is a functional requirement for security roles.

In controlling access, **SF.ACCESS_MANAGEMENT** uses the maintained security roles.

SF.AUTHENTICATE maintains the security role of users authenticated through PIN verification and external authentication.

SF.MANAGEMENT uses security roles maintained through the management of the state transition for each module.

Therefore, **FMT_SMR.1** is satisfied by **SF.ACCESS_MANAGEMENT**, **SF.AUTHENTICATE**, and **SF.MANAGEMENT**.

8.3.1.5 Protection of TSF (FPT)

FPT_RCV.2 Automated recovery

FPT_RCV.2 is a functional requirement for automated recovery.

If a power failure occurs during data write, **SF.RETENTION** restores the user data and TSF data to the correct state when restarted.

Therefore, **FPT_RCV.2** is satisfied by **SF.RETENTION**.

FPT_RVM.1　Non-bypassability of the TSP

FPT_RVM.1 is a functional requirement for addressing the bypass of the TSP.

SF.ACCESS_MANAGEMENT performs access control functions prior to the execution of accesses to files managed by the CD management unit, the AP management unit, and the Juki AP.
Therefore, **FPT_RVM.1** is satisfied by **SF.ACCESS_MANAGEMENT**.

When there are accesses by users of the CD management unit, the AP management unit, or the Juki AP, **SF.AUTHENTICATE** performs identification and authentication functions prior to the execution of such accesses.
Therefore, **FPT_RVM.1** is satisfied by **SF.AUTHENTICATE**.

Prior to the execution of cryptographic communications, **SF.SECURE_MESSAGING** shares encryption keys used for cryptographic operations with cards and service terminals.
Therefore, **FPT_RVM.1** is satisfied by **SF.SECURE_MESSAGING**.

SF.MANAGEMENT manages state transition management and performs controls according to the authorized roles. Identification and authentication functions are performed prior to the performing these controls.
Therefore, **FPT_RVM.1** is satisfied by **SF.MANAGEMENT**.

SF.DOMAIN performs identification and authentication functions and controls domain accesses.
Therefore, **FPT_RVM.1** is satisfied by **SF.DOMAIN**.

SF.RETENTION enforces failure detection functions to be activated when a failure occurs, and restores any data with anomalies caused by the failure.
Therefore, **FPT_RVM.1** is satisfied by **SF.RETENTION**.

FPT_SEP.1　TSF domain separation

FPT_SEP.1 is a functional requirement for TSF domain separation.

When **SF.ACCESS_MANAGEMENT** controls accesses to files managed by the CD management unit, the AP management unit, and the Juki AP, access control functions are separated from other functions.
Therefore, **FPT_SEP.1** is satisfied by **SF.ACCESS_MANAGEMENT**.

When **SF.AUTHENTICATE** identifies and authenticates users of the CD management unit,

the AP management unit, and Juki AP, identification and authentication functions are separated from other functions.
Therefore, **FPT_SEP.1** is satisfied by **SF.AUTHENTICATE**.

SF.MANAGEMENT manages state transition management, and the function of effecting state transition according to the authorized roles is separated from other functions.
Therefore, **FPT_SEP.1** is satisfied by **SF.MANAGEMENT**.

SF.DOMAIN separates the operational environment of the APs so that APs loaded onto the card do not gain unauthorized access to each other's program and data areas.
Therefore, **FPT_SEP.1** is satisfied by **SF.DOMAIN**.

8.3.1.6 Trusted path/channel (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1 is a functional requirement for inter-TSF trusted channels.
SF.SECURE_MESSAGING establishes a trusted path between cards and service terminals through secure messaging.
Therefore, **FTP_ITC.1** is satisfied by **SF.SECURE_MESSAGING**.

8.3.2 Rationales for the Strength of Security Functions

Section **5.1.2** states that the minimum strength of the functions for the TOE security requirements is “SOF-basic.” As described in the strength of security functions in Section **6.2**, this TOE achieves the SOF-basic level, which is equivalent to the minimum strength of functions, and satisfies the minimum strength of security functions as required of the TOE.

8.3.3 Rationales for Combinations of Security Functions

Some of the security functional requirements are satisfied by a number of security functions in the TOE summary specifications, and two or more security functions may be required to be combined to meet a security functional requirement. The security functional requirements listed below are satisfied by two or more security functions:

FCP_COP.1/RSA is satisfied by two security functions: **SF_AUTHENTICATE** and **SF.SECURE_MESSAGING**.

FIA_ATD.1 is satisfied by three security functions: **SF_ACCESS_MANAGEMENT**, **SF_AUTHENTICATE**, and **SF.MANAGEMENT**.

FIA_USB.1 is satisfied by two security functions: **SF_ACCESS_MANAGEMENT** and **SF_AUTHENTICATE**.

FMT_MSA.1/STATUS is satisfied by two security functions: **SF_ACCESS_MANAGEMENT** and **SF_MANAGEMENT**.

FMT_SMF.1 is satisfied by two security functions: **SF_ACCESS_MANAGEMENT** and **SF_MANAGEMENT**.

FMT_SMR.1 is satisfied by three security functions: **SF_ACCESS_MANAGEMENT**, **SF_AUTHENTICATE**, and **SF.MANAGEMENT**.

FPT_RVM.1 is satisfied by six security functions: **SF_ACCESS_MANAGEMENT**, **SF_AUTHENTICATE**, **SF.SECURE_MESSAGING**, **SF_MANAGEMENT**, **SF_DOMAIN**, and **SF_RETENTION**.

FPT_SEP.1 is satisfied by four security functions: **SF_ACCESS_MANAGEMENT**, **SF_AUTHENTICATE**, **SF_MANAGEMENT**, and **SF_DOMAIN**.

8.3.4 Rationales for Means of Assurance

Table 6-13 indicates reference documents corresponding to the assurance requirements, and the following explains the justifications of reference documents for the individual assurance requirements:

ACM_AUT.1 (Partial CM automation)

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration Management Rules” defines how to manage the modification and approval of components related to the overall development of the TOE.

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Version Management Rules” defines how to manage the granting and recording of version numbers to each component of the TOE.

Therefore, **ACM_AUT.1** can be satisfied by the rules mentioned above.

ACM_CAP.4 (Generation support and acceptance procedures)

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration List” describes a list of components related to TOE development and the dependencies among those components.

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration Management Records” records the history of, and results of approval for, modifications to the configuration list.

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Version Management Records” records the history of modifications to components, which are managed in accordance with the version management rules.

Therefore, **ACM_CAP.4** can be satisfied by the regulations mentioned above.

ACM_SCP.2 (Problem tracking CM coverage)

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration List” describes a list of components related to TOE development and the dependencies among those components.

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Configuration Management Records” records the history of, and results of approval for, modifications to the configuration list.

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Version Management Records” records the history of modifications to components, which are managed in accordance with the version management rules.

Therefore, **ACM_SCP.2** can be satisfied based on the content of the records mentioned above,

by tracking the TOE components for which any issues have occurred.

ADO_DEL.2 (Detection of modification)

“AdapterAdapter-compatible High-speed Juki Card Software ver.2.0 Delivery and Operation General Document” describes the appropriate module delivery procedures.

“Adapter-compatible High-speed Juki Card Software ver.2.0 Module Management Ledger” records of modules loaded when the TOE was manufacture and of the shipment.

Therefore, **ADO_DEL.2** can be satisfied by the regulations mentioned above.

ADO_IGS.1 (Installation, generation, and start-up procedures)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Delivery and Operation General Document” describes the procedures and precautions for loading the TOE software into cards (hardware) when manufacturing.

“Adapter-compatible High-speed Juki Card Software ver.2.0 Guidance General Document” describes how to use the TOE after it is delivered.

The methods of TOE installation and setup of initial data are clarified by the above mentioned documents, thus satisfying **ADO_IGS.1**.

ADV_FSP.2 (Fully defined external interfaces)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Functional Specifications” describes in an informal form, the specifications and external interfaces for all security functions that are provided by the TOE.

Therefore, **ADV_FSP.2** can be satisfied by the specifications mentioned above.

ADV_HLD.2 (Security execution high-level design)

“AP Execution Environment Operation Manual” describes in an informal form, the details of the high-level design for APE.

“Juki CD Unit Functional Specifications” describes in an informal form, the details of the high-level design for the CD management unit.

“CM Unit Functional Specifications” describes in an informal form, the details of the high-level design for the AP management unit.

“Juki AP Unit Functional Specifications” describes in an informal form, the details of the high-level design for the Juki AP.

“Security Library for CC Authentication - Functional Specifications” describes in an informal form, the details of the high-level design for security libraries.

“Common RAM Management Library for CC Authentication - Functional Specifications” describes in an informal form, the details of the high-level design for RAM management libraries.

“Flash Management Library for CC Authentication - Functional Specifications” describes in

an informal form, the details of the high-level design for flash management libraries.
Therefore, **ADV_HLD.2** can be satisfied by the design specifications mentioned above.

ADV_IMP.1 (Subset of the implementation of the TSF)

“AP Execution Environment Source Codes” describes the implementation of APE.
“Juki CD Unit Source Codes” describes the implementation of the CD management unit.
“CM Unit Source Codes” describes the implementation of the AP management unit.
“Juki AP Unit Source Codes” describes the implementation of Juki AP.
“Security Library for CC Authentication - Source Codes” describes the implementation of security libraries.
“Common RAM Management Library for CC Authentication - Source Codes” describes the implementation of RAM management libraries.
“Flash Management Library for CC Authentication - “Source Codes” describes the implementation of flash management libraries.
The foregoing describes the implementation of all security functions implemented in the TOE.
Therefore, **ADV_IMP.1** can be satisfied by the source codes mentioned above.

ADV_LLD.1 (Descriptive low-level design)

“AP Execution Environment Detailed Design Specifications” describes in an informal form, functional specifications for the APE.
“Juki CD Unit Detailed Design Specifications” describes in an informal form, the details of the low-level design for the CD management unit.
“CM Unit Detailed Design Specifications” describes in an informal form, the details of the low-level design for the AP management unit.
“Juki AP Unit Detailed Design Specifications” describes in an informal form, the details of the low-level design for the Juki AP.
“Security Library for CC Authentication - Detailed Design Specifications” describes in an informal form, the details of the low-level design for security libraries.
“Common RAM Management Library for CC Authentication - Detailed Design Specifications” describes in an informal form, the details of the low-level design for RAM management libraries.
“Flash Management Library for CC Authentication - Detailed Design Specifications” describes in an informal form, the details of the low-level design for flash management libraries.
Therefore, **ADV_LLD.1** can be satisfied by the design specifications mentioned above.

ADV_RCR.1 (Informal correspondence demonstration)

“Adapter-compatible High-speed Juki Card Software ver.2.0 TOE Summary Specifications

Paragraph Correspondence Table" describes the correspondence of TOE summary specifications in the ST to functions in the functional specifications.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Security Functional Requirement Correspondence Table" describes the correspondence of functional specifications to functions in the high-level design specifications.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Detailed Design Specifications" describes the correspondence of functions in the high-level design specifications to those in the low-level design specifications.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Correspondence Table" describes the correspondence of functions in the low-level design specifications to the source codes.
Therefore, **ADV_RCR.1** can be satisfied by the correspondence tables mentioned above.

ADV_SPM.1 (Informal security policy model)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Security Policy Model" describes the security policy model assumed by developers as the TOE usage method. It also describes what the secure state is in the automatic recovery of **FPT_RCV.2**.
Therefore, **ADV_SPM.1** can be satisfied by the document mentioned above.

AGD_ADM.1 (Administrator guidance)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Card Issuer Guidance" describes the guidelines for the operation of the TOE, and includes contents required of a guidance document. It also describes the maintenance mode in the automatic recovery of **FPT_RCV.2**.
"Adapter-compatible High-speed Juki Card Software ver.2.0 AP Loading Administrator Guidance Document" describes guidelines for the operation of the TOE, and includes contents required of a guidance document. It also describes the maintenance mode in the automatic recovery of **FPT_RCV.2**.
Therefore, **AGD_ADM.1** can be satisfied by the documents mentioned above.

AGD_USR.1(User guidance)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Card Issuer Guidance" describes the guidelines for the use of the TOE, and includes contents required of a guidance document.
"Adapter-compatible High-speed Juki Card Software ver.2.0 AP Loading Administrator Guidance Document" describes the guidelines for the use of the TOE, and includes contents required of a guidance document.
Therefore, **AGD_USR.1** can be satisfied by the documents mentioned above.

ALC_DVS.1 (Identification of security measures)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Development Security

Management Rules" defines the management methods for the TOE development environment.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Document Management Rules" defines management methods of documents used for development.
The environment and procedures of TOE development are clarified by the above mentioned rules, thus satisfying **ALC_DVS.1**.

ALC_LCD.1 (Developer defined life-cycle model)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Life Cycle Model" defines the TOE life cycle model intended by the developer.
Therefore, **ALC_LCD.1** can be satisfied by the document mentioned above.

ALC_TAT.1 (Well defined development tools)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Development Tool Management Rules" defines management methods for tools used for development.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Tool Management Records" includes records of tool management practiced in accordance with the rules mentioned above.
Therefore, **ALC_TAT.1** can be satisfied by the documents mentioned above.

ATE_COV.2 (Analysis of coverage)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Test Item Correspondence Table" includes the correspondence of the items of tests conducted by TOE developers to functions described in the design specifications, as well as the results of the analysis of their coverage.
Therefore, **ATE_COV.2** can be satisfied by the correspondence table mentioned above.

ATE_DPT.1 (Test: High-level design)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Test Depth Analysis" includes the results of analysis of the depth of items of tests conducted by TOE developers.
Therefore, **ATE_DPT.1** can be satisfied by the document mentioned above.

ATE_FUN.1 (Functional test)
"Adapter-compatible High-speed Juki Card Software ver.2.0 Test Items" describes the items of tests conducted by the developer for the high-speed Juki card software ver.2.0.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Testing Procedures" describes the procedures for tests conducted by the developer for the high-speed Juki card software ver.2.0.
"Adapter-compatible High-speed Juki Card Software ver.2.0 Test Results" describes the results of tests conducted by the developer for the high-speed Juki card software ver.2.0.

Therefore, **ATE_FUN.1** can be satisfied by the results mentioned above.

ATE_IND.2 (Independent testing - sample)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Test Environment” includes environment for tests conducted by the developer.

“Adapter-compatible High-speed Juki Card Software ver.2.0 Test Programs” includes programs used for tests conducted by the developer.

“Adapter-compatible High-speed Juki Card Software ver.2.0 Test Data” includes data necessary for tests conducted by the developer.

“Adapter-compatible High-speed Juki Card Software ver.2.00” is the TOE itself developed by the developer.

Therefore, independent testing by the evaluator will be supported by the above mentioned deliverables and by comparing the results with the results of test conducted by the developer, **ATE_IND.2** can be satisfied.

AVA_MSU.3 (Analysis and testing of insecure states)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Developer Misuse Prevention Analysis Reports” includes the measures taken by the developer to prevent the misuse of the TOE and the results of analysis of insecure states.

Therefore, **AVA_MSU.3** can be satisfied by the report mentioned above.

AVA_SOF.1 (Strength of TOE security function evaluation)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Developer Strength of Security Function Evaluation Report” includes the results of the strength of TOE security function evaluations performed by the developer.

Therefore, **AVA_SOF.1** can be satisfied by the report mentioned above.

AVA_VLA.2 (Independent vulnerability analysis)

“Adapter-compatible High-speed Juki Card Software ver.2.0 Developer Vulnerability Analysis Report” includes the results of the TOE vulnerability analysis performed by the developer.

Therefore, **AVA_VLA.2** can be satisfied by the report mentioned above.

Appendix A Glossary

Definitions of abbreviations and terms used in this ST are sorted out below.

<CC related abbreviations>
Terms below must be used as defined in CC part 1.

CC: Common Criteria
EAL: Evaluation Assurance Level
IT: Information Technology
PP: Protection Profile
SOF: Strength of Function
ST: Security Target
TOE: Target of Evaluation
TSF: TOE Security Functions

<Standard related abbreviations>
Definitions of standard related abbreviations are as below.

ANSI: American National Standards Institute
PKCS: Public-Key Cryptography Standards

<Abbreviations and terms related to cards in general>
The abbreviations and terms below are used in this ST based on the definitions below.

Juki card:	Basic Resident Registration IC card
Juki net:	Basic Resident Registration network system
CD:	Card Domain. Only one exists in the card, and is an area managed by the card issuer.
AP:	Application. Programs loaded in the card. Multiple programs reside on the card and can be added after the card is issued.
SD:	Security Domain. An area that manages the AP loaded on the card.
Manufacture:	A role that loads the TOE onto the cards and delivers them to the municipality. Corresponds with Manufacturing vendors.
Issuer:	A role that issues the TOE loaded cards. Corresponds with municipalities.
Holder:	A role that owns the granted TOE loaded card.

	Corresponds with citizens.
APE:	Application execution environment. Manages the domain separation of the APs loaded onto the chip.
CD managing unit:	Manages the security configuration of CD.
AP managing unit:	Manages the AP loaded onto the card.
Juki AP:	Juki card AP. AP for Juki cards used with municipal services.
EF:	An area to store basic files and data.
IEF:	An area to store data used for authentication of PINs and keys.
WEF:	An area to store data for operations.
SE:	One of the security attributes, used to determine the key for authentication and decryption.
Access control attributes:	Security attribute to manage the conditions for access control operations.
Authentication status:	Security attributes that hold authentication results.
Adapter:	Software that operates on the service terminals. Based on the interfaces specified in the Juki specifications, it generates the command messages corresponding to the implementation of the Juki card. It absorbs the Juki card implementation differences among manufacturers to enable the use of Juki card through a common interface, and is invoked by service software.
Module:	Program components of the software residing on the card.
Process:	A state of a module on card when it is running as a subject.

<Terms related to the AP management unit>

CA (certification authority):	A system that issues certificates for public keys.
AP loading administrator:	Manages overall AP loading in the AP management area.

Appendix B References

This appendix lists the reference materials referred to in this ST. Labels in brackets ([]) are reference identifiers of the material.

[JIS-1] JIS X 5070-1:2000 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[JIS-2] JIS X 5070-2:2000 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements

[JIS-3] JIS X 5070-3:2000 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements

[CC-1] Common Criteria for Information Technology Security Evaluation -- Part 1: Introduction and general model, August 2005, Version 2.3 CCMB-2005-08-001 (Translated by IPA, version 1.0)

[CC-2] Common Criteria for Information Technology Security Evaluation -- Part 2: Security functional requirements, August 2005, Version 2.3 CCMB-2005-08-002 (Translated by IPA, version 1.0)

[CC-3] Common Criteria for Information Technology Security Evaluation -- Part 3: Security assurance requirements, August 2005, Version 2.3 CCMB-2005-08-003 (Translated by IPA, version 1.0)

[CEM] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, August 2005, Version 2.30 CCMB-2005-08004 (Translated by IPA, version 1.0)

[Juki PP] Security Requirement Specifications (Protection Profile) for Basic Resident Registration IC Cards version 2.0 (in Japanese), Local Authorities Systems Development Center, April 16, 2003.

[Supplement-0512] Supplement-0512 (in Japanese), December 2005.

[Juki Specifications 23] Basic Resident Registration Network System Basic Resident Registration Card Specifications Version 2.3(in Japanese)
Local Authorities Systems Development Center, July 15, 2003.

[CC-1E] Common Criteria for Information Technology Security Evaluation
Part1:Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[CC-2E] Common Criteria for Information Technology Security Evaluation
Part2:Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[CC-3E] Common Criteria for Information Technology Security Evaluation
Part3:Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[CEM-E] Common Methodology for Information Technology Security Evaluation (CEM)
Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[CCMB-0512] Interpretations-0512

[JIL] Application of Attack Potential to Smartcards, Version 2.5, Revision 1,
April 2008 CCDB-2008-04-001

[AIS] Application Notes and Interpretation of the Scheme, 01 June 2004, Version 1.00