Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-08-06 (ITC-7162)
Certification No.	C0191
Sponsor	NTT Communications Corporation
Name of TOE	Adapter Compatible High-Speed Juki Card Software
Version of TOE	2.00
PP Conformance	None
Conformed Claim	EAL4 Augmented with AVA_MSU.3
Developer	Nippon Telegraph and Telephone Corporation Sharp Corporation
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc.

This is to report that the evaluation result for the above TOE is certified as follows.
2008-10-30

Hideji Suzuki, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"Adapter Compatible High-Speed Juki Card Software" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of " Adapter Compatible High-Speed Juki Card Software Version 2.00" (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, NTT Communications Corporation.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product: Adapter Compatible High-Speed Juki Card Software
Version: 2.0
Developer: Nippon Telegraph and Telephone Corporation,Sharp Corporation

1.2.2 Product Overview

The TOE 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.
The objectives of the TOE loaded onto the 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 card. Juki cards are used for such services 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.

1.2.3 Scope of TOE and Overview of Operation

The relationship between the software that comprise the TOE and the peripheral hardware and software are as shown in Figure 1-1.

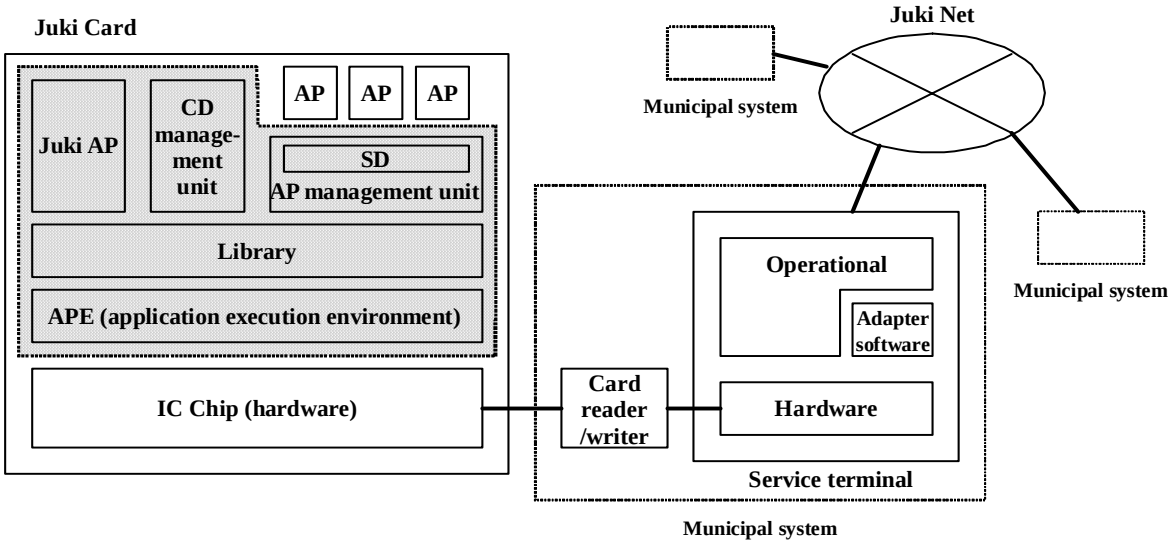

Figure 1-1 TOE Configuration

The TOE is the software represented by the shaded area, and is loaded onto the memory of the IC chip embedded in the Juki card. 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. While an area called “SD” is created in the AP management unit, and applications can be loaded into that area, the loaded APs are beyond the scope of this TOE.

1.2.4 TOE Functionality

Functions of the TOE which are implemented by the APE, library, CD management unit, AP management unit, and Juki AP module shown in Figure 1-1 are described in the following two sections below: “Security Functions of TOE” and “TOE Functions Other than Security.”

<<Security Functions of TOE>>
1. Identification and Authentication Functions
(1) Identification Functions
The TOE indentifies modules that are selected with the Select command. The selected

module running on the card is called a “process,” and runs on behalf of that user. And any 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 become a CD management process, a Juki AP process, and an AP management process, respectively.
(2) PIN Verification Functions
The TOE compares PINs transmitted from outside with the cards' pre-set data to authenticate TOE-related parties (card holders, card issuers).
(3) External Authentication Functions
The TOE sends out a random number it generates to a service terminal which sends back the random number encrypted with a corresponding secret key. The TOE decrypts the returned encrypted data using the cards' pre-set public key or a public key included in a verified public key certificate in order to authenticate the service terminal.

2. Access Management Functions
(1) File Management Functions
The TOE secures and manages file areas where data are stored in the flash memory of the IC chip, and controls accesses to the data stored in the files.
(2) Application Management Functions
The TOE has an area called “SD,” which is an area for managing APs and where APs are loaded. The TOE manages APs in the SD, and based on its access control, manages the loading, selection, and deletion of the APs.
(3) Key Management Functions
The TOE stores and updates key data stored in the key storage files it manages on the IC chip.

3. Cryptograhic Communications Functions
(1) Secure Messaging Functions
In communications 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.

4. Execution Management Functions
(1) Authentication Status Management Functions
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 Juke 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.
(2) 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 effects state transition of each module using commands.
Note: Each module is in a different state depending on the current phase (manufacture phase, deliver phase, grant phase, and operation phase), and the commands allowed for each state are different. 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.
(3) 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.

5. Domain Separation Functions
(1) 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.

6. Data Restoration Functions
(1) Power Failure Detection Functions
When starting up, the TOE examines whether any power failure had occurred during a data write or data deletion. If a power failure had occurred during a write operation or a delete operation, the data is restored using the failure recovery function described in (2) below.
(2) Failure Recovery Functions
The TOE begins a transaction prior to write or delete processing, and if the processing ends successfully, the TOE effectuates the contents written during the processing and completes the transactions. If the processing ends unsuccessfully, the contents written during the processing are discarded and the card is returned to a connect state.

<<TOE Functions Other than Security>>
1. Communications 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.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Adapter Compatible High-Speed Juki Card Software Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3

(either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "Adapter Compatible High-Speed Juki Card Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2008-10 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

The Evaluation Assurance Level of the TOE specified by the ST is EAL4 augmented. The augmented assurance component is AVA_MSU.3.

1.5.3 SOF

The ST claims “SOF-Basic” as the minimum strength of function. This TOE 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.

1.5.4 Security Functions

The security functions of this TOE is as described in “Security Functions of TOE” in section 1.2.4 “Functions of TOE.”

1.5.5 Threat

The TOE assumes the threats listed in Table 1-1, and provides functions to counter

these threats.

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.

Table 1-1 Assumed Threats

Identifier	Threat
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.
T.Illegal_Term_Use	Attackers other than authorized municipal government officials 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.
T.Disturb_APL	A Juki card has many applications installed; i.e., user identification applications and municipality 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.
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.

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.
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

1.5.6 Organisational Security Policy

The organisational security policies required for the use of the TOE is described in Table 1-2.
The Basic Resident Registration Card Specification Ver.2.3 is a specification for Juki cards but include descriptions that should be considered as organisational security policies. These requirements are as quoted below:

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
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) * Personal Identification Number. Equivalent to a password.
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.
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.
P.Secure_Path	Section 3.4 “Secure Messaging Functions” in Chapter 7 “Juki Card Application Specifications” includes a provision that specifies 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.”

1.5.7 Configuration Requirements

Specifications of the TOE operational environment and TOE peripheral devices are as described below. These are all placed and installed within the municipal system.

<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.

1.5.8 Assumptions for Operational Environment

The assumptions with regard to the operational environment where the TOE used are desribed in Table 1-3.
If these assumptions are not met, the effective operation of the security functions of the TOE will not be guaranteed.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
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.

1.5.9 Documents Attached to Product

The documents accompanying this TOE are listed below.

Table 0-4 List of Guidance Documents

Title	Identification	Version
Adapter-Compatible Juki Card Software General Guidance Document	GD_ALL	1.10
Adapter-Compatible Juki Card Software AP Loading Manager Guidance Document	GD_APM	1.10
Adapter-Compatible Juki Card Software CM Unit Operation Manual	GD_CM	1.12
Adapter-Compatible Juki Card Software Card Issuer Guidance Document	GD_ISS	1.12
Adapter-Compatible Juki Card Software Juki AP Operation Manual	GD_JAP	1.11
Adapter-Compatible Juki Card Software Juki CD Unit Operation Manual	GD_JCD	1.11
IC Card Internal Software AP Execution Environment Operation Manual (Concerning AP Execution Environment Ver. 2.517dR, for system developers)	APE_GD	1.2.0
SM4148 AP Execution Environment (APE) Security Guidance	APE_GD_S	1.3.0

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2007-08 and concluded by completion the Evaluation Technical Report dated 2008-10. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites six times from 2007-10 to 2008-07 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2008-05 and 2008-08.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

An overview of the developer tests evaluated by the evaluator and the evaluator tests performed by the evaluator is given below.

2.3.1 Developer Testing

1) Developer Test Environment

The TOE is developed by Sharp Corporation and Nippon Telegraph and Telephone Corporation (the APE is developed by Sharp Corporation, the library, CD management unit, AP management unit, and the Juki AP are developed by Nippon Telegraph and Telephone Corporation), and tests are performed by both parties on their respective area of development. The configuration of the tests performed by Nippon Telegraph and Telephone Corporation is as follows:

Table 2-1 Test Configuration (Nippon Telegraph and Telephone Corporation)

Device	Main Specifications
Contactless IC Card Reader/Writer – USB type	SCR331DI-NTTCom NTT Communications Corporation
PC for Testing	Windows 2000 or Windows XP
IC Card (including chip)	IC Chip model: SM4148 IC Card LSI
Software	**Main Specifications**
Smart Card Simulator	Version 4.0.1 Sharp Corporation.
Fsp	1.7.8 NTT Electronics Corporation

The configuration of the tests performed by Sharp Corporation is as follows:

Table 2-2 Test Configuration (Sharp Corporation)

Device	Main Specifications
Terminal PC	AT compatible
Evaluation Board	Evaluation board (by Sharp Corporation)
ICE	ROMICE64 (by COMPUTEX CO., LTD.)
Protocol Analyzer	LE-7200 (by LINEEYE CO., LTD.)
Protocol Evaluation Tool	MP300 (by MICROPROSS)
Contactless Reader/Writer	EVPCD7010 (for IC card debugging)
	PD8080 (by Yamato Denki Kogyo), PD2002 (by Yamato Denki Kogyo)
Contact type Reader/Writer	RW4040 (by Sharp Corporation)
	SCR331 (by NTT Communications Corporation)
IC Card LSI	SM4148
Software	**Main Specifications**
OS for Terminal PC	Windows 2000, Windows XP
Software for ROMICE	CSIDE for ROMICE64 MK5 v3.31 (by COMPUTEX CO., LTD.)
AP/LIB Downloader	2.0.0.0 (by Sharp Corporation)
Software for MP300	MPScope v1.12.0 (by MICROPROSS)

1) Developer Tests Overview
An overview of the tests performed by the developers are shown below.

a. Test Configuration
The configuration for the tests performed by the developers is as already shown in Table 2-1 and 2-2. The developer tests have been conducted in a TOE test environment that is partially different from the TOE configuration identified in the ST (for example, since power failure cannot be performed on demand on an IC chip, a Smart Card Simulator was used to accomplish the power failure test).However, such differences have been analyzed by the evaluator, and have been confirmed that they do not affect the outcome of the tests.

b. Testing Method
Nippon Telegraph and Telephone Corporation and Sharp Corporation have adopted different testing methods. Table 2-3 and 2-4 below describe the details respectively.

Table 2-3 Testing Method (Nippon Telegraph and Telephone Corporation)

Type	Overview of Method
Testing of Actual Cards	Using a tool, issue a C-APDU to the card and then compare the returned R-APDU with the expected R-APDU. If the returned R-APDU is encrypted, decrypt the R-APDU and compare it with the expected R-APDU.
Simulator	Using a tool, allow a power failure to occur and then using the step execution feature or breakpoint feature of the tool, verify that the process to recover from a power failure is driven correctly. Using a tool, perform attacks that affect the security (memory dump, tampering etc.) and then using the step execution feature or breakpoint feature of the tool, verify that the attacks are properly detected, and security countermeasure processes are driven correctly.

Table 2-4 Testing Method (Sharp Corporation)

Type	Overview of Method
Test Environment using the Evaluation Board in Contact Mode	Using an automated evaluation software running on a terminal PC, send a C-APDU through the contact-type reader/writer to ROMICE and evaluation board that simulates the IC card LSI, and perform tests.Visually verify the values stored in memory. The evaluation board provides the IC card functionality. By accessing the internal memory of the evaluation board through ROMICE, internal RAM information which is not accessible on IC cards becomes accessible.
Test	Using an automated evaluation software running on a terminal

Type	Overview of Method
Environment using the Evaluation Board in Contactless Mode	PC, send a C-APDU through the contactless IC card debugging reader/writer to ROMICE and evaluation board that simulates the IC card LSI, and perform tests.Visually verify the values stored in memory. The evaluation board provides the IC card functionality. By accessing the internal memory of the evaluation board through ROMICE, internal RAM information which is not accessible on IC cards becomes accessible.
Test Environment using the Actual IC Cards in Contact Mode	Using an automated evaluation software running on a terminal PC, send a C-APDU through the contact-type reader/writer to the IC card, and perform tests. Using the automated evaluation software, send a C-APDU and then automatically compare the received R-APDU with the expected value to see whether they match. Furthermore, obtain the comparison results log and verify there are no errors. This testing environment performs tests on normally connected IC cards and reader/writers. The commands from the terminal PC are sent to the IC card via the contact-type reader/writer.
Test Environment using the Actual IC Cards in Contactless Mode	Using an automated evaluation software running on a terminal PC, send a C-APDU through the contactless reader/writer to the IC card, and perform tests. Using the automated evaluation software, send a C-APDU and then automatically compare the received R-APDU with the expected value to see whether they match. Furthermore, obtain the comparison results log and verify there are no errors. This testing environment performs tests on normally connected IC cards and reader/writers. The commands from the terminal PC are sent to the IC card via the contactless reader/writer.

c. Scope of the Tests Performed
A total of 907 test items have been covered by Nippon Telegraph and Telephone Corporation and 2158 by Sharp Corporation.
Coverage analysis has been performed, and it has been verified that the security functions and external interfaces described in the functional specifications have been tested sufficiently. Depth analysis has been performed, and it has been verified that all subsystems and subsystem interfaces described in the high-level design have been tested sufficiently.

d. Results
The actual results of the tests performed by the developers have been confirmed to match the expected test results. The evaluator has confirmed the validity of the

methods and items of the developer tests, and has confirmed that the methods and results match those described in the test plan document.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The configuration for the tests performed by the evaluator for the evaluator independent testing was equivalent to that of the developer tests. For penetration tests, tests have been performed using additional testing devices such as oscilloscopes. For details, refer to 2) below.

2) Outlining of Evaluator Testing

An overview of the tests performed by the evaluator (evaluator independent tests, penetration tests) are shown below.

a-1. Configuration of Evaluator Independent Tests
As described in item “a. Test Configuration” of section 2.3.1 2) “Developer Tests Overview,” while the configuration of the tests performed by the evaluator is partially different from the configuration of the ST, the evaluator has verified that the differences do not affect the tests.

a-2. Configuration of Penetration Tests
In addition to the configuration for the evaluator independent tests, the following three types of testing devices have been employed for power analysis.

Table 2-5 Testing Device 1

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center V2.30 & Signalyer V2.09
Software	Brightsight	EMV Tool
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	DPA Card Reader V1.1

Table 2-6 Testing Device 2

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center v2.30& Signalyser v.2.09
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	Reset Board V1.1
Puls generator	Agilent	81110A

Table 2-3 Testing Device 3

Instrument	Manufacturer	Model
Digital Storage Oscilloscope	LeCroy	WP7300A
PC		
Software	Brightsight	DPA Center V2.30 & Sideways 3
Software	Brightsight	EMV Tool
Function generator	Agilent	33120A
Power supply	Agilent	3631A
Card Interface & Trigger Circuit	Brightsight	DPA Card Reader V1.1

b-1. Evaluator Independent Test Testing Method
The same as described in item “a. Test Configuration” of section 2.3.1 2) “Developer Tests Overview.”

b-2. Penetration Test Testing Method
In addition to using the same methods as the evaluator independent tests, employing the devices described in item “a-2. Configuration of Penetration Tests” of section 2.3.2 2) “Evaluator Tests Overview,” power analysis (SPA/DPA) have been performed in an attempt to decipher the PINs and encryption keys of the TOE.

c. Scope of the Tests Performed
For the areas developed by Nippon Telegraph and Telephone Corporation, 106 items have been covered with evaluator independent tests and 15 items with penetration tests, as well as 313 items through sampling of developer tests, totaling 434 items tested. For sampling tests, in order to cover all security functions, approximately 34.4% of the developer tests were sampled and followed-up with verification. In considering the selection criteria of the evaluator independent test items, since the developer has performed threshold analysis and executed all pair tests with those thresholds, there is not much room for the evaluator to lay out effective test items.However, since the testers of the AP management unit and the CD management unit/Juki AP had been different, and the test items had been prepared separately, no tests that encompass both the AP management unit and the CD management unit/Juki AP was performed by the developers. Therefore, the evaluator has focused on this area, and has performed independent tests related to the status transitions that encompass the AP management unit and the CD management unit/Juki AP. Furthermore, the evaluator has also performed independent tests for parameter values that have not been performed by the developers. For penetration tests, command scans that attackers generally perform, as well as penetration tests in terms of vulnerabilities specified in the CC supporting documents (such as penetration tests on SPA of RSA) have been performed in order to confirm the validity of the vulnerability analysis conducted by the developer.Prior to testing, the evaluator has investigated theses, publications, publicly known smartcard vulnerability information on the Internet, and has verified that these information have been aggregated into the CC supporting documents, therefore concluding that all current smart card vulnerability perspectives have been considered.
For the areas developed by Sharp Corporation, 12 items have been covered with evaluator independent tests and 5 items with penetration tests, as well as 505 items through sampling of developer tests, totaling 522 items tested. For sampling

tests, in order to cover all security functions, approximately 23.4% of the developer tests were sampled and followed-up with verification. In considering the selection criteria of the evaluator independent test items, as with the area developed by Nippon Telegraph and Telephone Corporation, since the developer has performed comprehensive tests, there is not much room for the evaluator to lay out effective test items. Therefore, the evaluator has focused on parameter values that the developer had not performed, and conducted the evaluator independent tests while covering all security functions of the APE. For penetration tests, command scans that attackers generally perform, as well as penetration tests in terms of vulnerabilities specified in the CC supporting documents (in APE, only buffer overflow) have been performed in order to confirm the validity of the vulnerability analysis conducted by the developer. Other considerations have been covered in the area developed by Nippon Telegraph and Telephone Corporation.Prior to testing, the evaluator has investigated theses, publications, publicly known smartcard vulnerability information on the Internet, and has verified that these information have been aggregated into the CC supporting documents, therefore concluding that all current smart card vulnerability perspectives have been considered.

d. Results
All evaluator tests have completed successfully, confirming the operation of the TOE. The evaluator has confirmed that all test results match with the expected behaviors.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the Augmented with AVA_MSU.3 prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

Below are the acronyms used in this report.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
APDU	Application Protocol Data Unit

Below are the TOE specific terms and abbreviations used in this report.

Juki Card	Basic Resident Registration IC Card
Juki Network	Basic Resident Registration Network System
CD	Card Domain. Only one exists on 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 in the card.
Manufacturer	A role that loads the TOE onto the cards and delivers them to the municipality. Corresponds with manufacturing vendors.
Issuer	A role that issues 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 management unit	Manages the security configuration of CD.
AP management unit	Manages the APs loaded onto the card.
Juki AP	Juki card AP. AP for Juki cards used with municipal services.
Adapter	Software that operates on the service terminals. Based on the interfaces specified in the Juki specifications, it generates 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 a card when it is running as a subject.

APDU	Data exchanged between a terminal and an IC card (commands and responses)
C-APDU	Command APDU. An APDU issued by a terminal to an IC card.
R-APDU	Response APDU. An APDU by the IC card in response to a C-APDU.
ROMICE	In-circuit emulator. A product as an alternative to a ROM on a board and used for debugging and other tasks.
Evaluation Board	A circuit board for evaluation purposes.

6. Bibliography

[1] Adapter Compatible High-Speed Juki Card Software Security Target Version 1.92 (Oct 10, 2008) Nippon Telegraph and Telephone Corporation

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

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

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

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

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] Supplement-0512 December 2005

[18] Adapter Compatible High-Speed Juki Card Software Evaluation Technical Report Version 2.1, Oct 17th, 2008, Electronic Commerce Security Technology Laboratory Inc.

[19] Application Notes and Interpretation of the Scheme, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.0, 01 June 2004, Certification body of the BSI

[20] Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards Version 2.3