

TAMPER PROOF CARD READER SYSTEM AND METHOD THEREOF

FIELD OF INVENTION

- 5 The invention relates to a card reader. More particularly, the invention relates to a system for testing and preventing tampering attacks on card reader and its method thereof.

BACKGROUND OF THE INVENTION

10

- A smart card reader is an electronic device that reads data from a card-shaped storage medium. The first were punched card readers, which read the paper or cardboard punched cards that were used during the first several decades of the computer industry to store information and programs for computer systems. Modern card readers are
- 15 electronic devices that can read smart cards embedded with either a barcode, magnetic strip, computer chip or another storage medium. There are two types of smart cards: contact and contactless. Both have an embedded microprocessor and memory. The smart card differs from a proximity card in that a microchip in the proximity card has only one function: to provide the reader with the card's identification number. The
- 20 microprocessor in the smart card has an embedded operating system and can handle multiple applications such as a cash card, a pre-paid membership card, or an access control card. The smart card readers have been targeted successfully by criminals, in which the smart card readers are being tampered by various methods with during manufacture or in the supply chain before delivery. These devices capture the
- 25 customer's card details before transmitting them to the criminals. Therefore, there is a need for a system that can prevent the tampering of the smart card readers.

There are a few patented technologies over the prior art relating to the tamper proof card reader system. Of interest in respect to the smart card reader with a secure

logging feature is US20130119130A1. The patent application discloses a secure smart card reader enabled to make reader signatures on data representative of events and actions which may be security related and which may include data representative of reader commands received from a host or remote application, smart card commands
5 exchanged with an inserted smart card, data presented to a user for approval, and/or configuration parameters applied when dealing with any of the foregoing. The smart card reader may be adapted to maintain logs of events and actions which may include exchanging reader commands, exchanging smart card commands, and/or interactions with a user. The logs may include data representative of the reader commands
10 received, the smart card commands exchanged, data presented to the user for approval, and/or configuration parameters applied when dealing with any of the foregoing. The secure smart card reader may be adapted to generate a reader signature over the logs.

15 Another is a personal biometric authentication and authorization device is disclosed in US6983882B2. This teaching, however, focuses primarily on the personal biometric authentication and authorization device (PAD) provides protection for portable tokens such as magnetic stripe cards and smart cards. The PAD enables portable tokens upon engagement with the PAD and comparison of a biometric input on the PAD with a
20 stored biometric data. The PAD can be used for biometrically authenticated transactions with or without a portable token. Multiple user account data can be stored in the PAD. The PAD can write the magnetic stripe of a magnetic stripe portable token. The PAD can be enrolled with an enrolment system to associate the PAD, an individual, and the portable tokens to be used with the PAD. The PAD can be used for
25 e-commerce transactions.

Accordingly, it would be desirable to provide a system that incorporate a means to detect invalid smart card and disconnect the communication between the smart card and the card reader. This invention provides such a system and method thereof.

SUMMARY OF INVENTION

- The present invention provides a method to test and prevent tampering attack on a
- 5 card reader, the method comprising the steps of: establish a communication link with a smart card, for communicating information between the card reader module and the smart card, by a card reader module; identify a pre-stored public key from the smart card, for comparison with a plurality of reference public keys stored in a data repository, by the card reader module; and determine validity of the smart card based
- 10 on the comparison between the pre-stored public key and the plurality of reference public keys, by a verification module, characterized in that, upon detection of an invalid smart card, disconnects the communication link of the card reader module with the smart card, by a means.
- 15 Further, the method comprises the steps clear memory stored in the data repository upon detection of an invalid smart card, by a memory clearance module.

Preferably, the card reading means includes a biometric sensor, a display, a card receiving slot and a processor.

20

- Further, the method comprises the steps: capture a biometric feature from a user as a biometric data, by the biometric sensor; compare the captured biometric data with corresponding reference data stored in the smart card, by a biometric identification module; and display a message only if there is a match between the captured
- 25 biometric data with corresponding reference biometric data stored in the smart card, by the display.

Further, the method comprises the steps to clear memory of the data repository upon completion of biometric comparison, by the memory clearance module.

The present invention also provides a tamper-proof card reading means comprises: a card reader having a card receiving slot, configured to receive a smart card comprises: a card reading module, configured to establish a communication link with the smart
5 card for communicating information between the card reading means and the smart card; a biometric sensor for capturing a biometric feature from a user as a biometric data; and a processor comprises: a verification module for determining validity of the smart card based on comparison between its pre-stored public key and a plurality of reference public keys from a data repository; a biometric identification module for
10 comparing the captured biometric data with corresponding reference biometric data stored in the smart card; and a means for disconnecting the communication link with the smart card upon detection of an invalid smart card.

Further, the tamper-proof card reading means comprising a memory clearance module
15 configured to clear memory stored in the data repository upon detection of an invalid smart card.

Preferably, the card reader includes a biometric sensor, a display, a card receiving slot and the processor.

20

Preferably, the data repository is accessible via offline or online communication.

One skilled in the art will readily appreciate that the invention is well adapted to carry out the objects and obtain the ends and advantages mentioned, as well as those
25 inherent therein. The embodiments described herein are not intended as limitations on the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

For the purpose of facilitating an understanding of the invention, there is illustrated in the accompanying drawing the preferred embodiments from an inspection of which when considered in connection with the following description, the invention, its construction and operation and many of its advantages would be readily understood and appreciated.

Figure 1 is a block diagram illustrating a tamper proof card reader system.

Figure 2 is a flow chart diagram illustrating the process flow to test and prevent tampering attack on the card reader.

DETAILED DESCRIPTION OF THE INVENTION

The invention will now be described in greater detail, by way of example, with reference to the drawings.

The present invention provides a system and method to prevent tampering attacks on a card reader. Preferably, the present invention also provides the system and method for security functionality and compatibility testing on a card reader carried out in both online mode and offline mode. In the offline mode, authentication and verification process of the smart card is carried in firmware of the card reader. In the online mode, the card reader is connected to a computing device installed with software to initiate and carry out the authentication and verification process.

Referring to Figure 1, tamper-proof card reading means (100) is the system comprises a card reader (110), a smart card (130) and a data repository (150). The card reader (110) is in communication with the data repository (150) via wired or wireless communication network. The data repository (150) is also known as a data library or data archive isolated to be mined for data reporting and analysis. The data repository

(150) is also a large database infrastructure that can collect, manage, and store data sets for data analysis, sharing and reporting. Preferably, the data repository (150) includes a plurality of pre-stored public keys for the smart card (130). The smart card (130) can be an identification card, bank related card or any other cards.

5

The card reader (110) comprises of a card reader module (111), a biometric sensor (112), a display (113), a card receiving slot (114) and a processor (115). The card receiving slot (114) is configured to receive the smart card (120) inserted by the user. Upon insertion of the smart card (130) into the card reading slot (114), the card reader
 10 module (111) is configured to establish a communication link with the smart card (130) and configured to retrieve or identify a pre-stored public key in the smart card (130). The biometric sensor (112) is configured to obtain or retrieve the biometric data from the user. Preferably, the biometric sensor (112) can be a fingerprint sensor, iris detection, voice recognition or any other suitable biometric sensor (112) known in the
 15 art. The processor (115) is configured to control operations for the devices of the card reader (110). Further, the processor (115) is configured to perform identification, authentication and verification of the smart card (130). The card reader (110) preferably further comprises of a data retrieval module configured to retrieve the stored data from the smart card (130). The stored data includes biometric data and
 20 identification data of the user.

The processor (115) comprises of a processing module (116), a verification module (117), a biometric identification module (118) and a memory clearance module (119). The processing module (116) is configured to process the biometric data received
 25 from the biometric sensor (112) and the retrieved data. The verification module (117) is configured to determine validity of the smart card (130) by comparing the identified pre-stored public key with the plurality of reference public keys from the data repository (150). If the pre-stored public key matches with any of the plurality of the reference public keys then the smart card (130) is valid. Else, the smart card (130) is

invalid. Preferably, the data repository (150) is accessible via offline or online communication. The biometric identification module (118) is configured to compare the captured biometric data those stored biometric data in the smart card (130) for verification of the user's identity. The comparison result is displayed on the display
 5 (113). The memory clearance module (110) configured to clear the data memory from the data repository (150) upon detection of the invalid smart card (130). The processor (115) further comprises a means which is a communication disconnection module configured to disconnect the established communication link with the smart card (130) upon detection of the smart card (130) is invalid. This prevents the tampering of
 10 the card reader (110) using dummy card to fake the smart card (130).

In an embodiment, the tamper proof card reading means (100) comprises of the card reader (110), a computing device, the smart card (130) and the data repository (150). The computing device can be any device capable of data transmission is installed with
 15 an application module. The card reader (110) is communication with the computing device via wired or wireless communication network. The application module is configured to initiate the authentication and verification process of the smart card (130). Preferably, the application module includes the verification module (117), the biometric identification module (118), the memory clearance module (119) and the
 20 communication disconnection module. The verification module is configured to determine validity of the smart card (130) by comparing the identified pre-stored public key with the plurality of reference public keys from the data repository (150). If the pre-stored public key matches with any of the plurality of the reference public keys then the smart card (130) is valid else the smart card (130) is invalid. Preferably,
 25 the communication with the data repository (150) is accessible via offline or online communication. The biometric identification module (118) is configured to compare the captured biometric data those stored biometric data in the smart card (130) for verification of the user's identity. The comparison result is displayed on the display (113). The memory clearance module (110) configured to clear the data memory from

the data repository (150) upon detection of the invalid smart card (130). The processor (115) further comprises a communication disconnection module configured to disconnect the established communication link with the smart card (130) in the card reader (110) upon detection of the invalid smart card (130).

5

The present invention also provides the method to prevent tampering attack on the card reader (110); the method comprises the steps (210 to 250): insert the smart card (130) into the card receiving slot (114). (Step 210) establish a communication link with a smart card (120) for communicating information between the card reader
 10 module (111) and the smart card (120), by the card reader module (111). Then, (Step 220) identify the pre-stored public key from the smart card (120), by the card reader module (111). Next, (Step 230) compare the identified pre-stored public key with the plurality of reference public keys stored in the data repository (150), by the card reader module (111). Then, determine validity of the smart card based on the
 15 comparison between the pre-stored public key and the plurality of reference public keys, by the verification module (117). Next, disconnect the established communication link with the smart card (130) upon the detection of the invalid smart card (130) based on the comparison result, by the communication disconnection module. The method further comprises the steps to clear memory stored in the data
 20 repository (150) upon detection of the invalid smart card (130), by the memory clearance module (119).

Further, the method comprises the steps: capture the biometric feature from the user as the biometric data, by the biometric sensor (112). Then, compare the captured
 25 biometric data with corresponding reference data stored in the smart card (130), by a biometric identification module (118). Next, display a message only if there is a match between the captured biometric data with corresponding reference biometric data stored in the smart card (130), on the display (113). Then, clear the memory of the data repository (150) upon completion of the biometric comparison, by the

memory clearance module (119).

In an exemplary embodiment, an experiment for the security functionality and compatibility testing on the card reader carried out in both online mode and offline
 5 mode was carried out. The system and the method of the present invention is now explained with respect to the testing and its results obtained from the testing.

1. Introduction:

10 1.1 Overview:

Preferably, the card reader is a MyKad Enhancement Biometric Access (EBA) reader (MyKad EBA reader). The smart card is preferably a Malaysia Kad Akuan Diri (MyKad) smart card that contains owner's encrypted biometric fingerprint data and
 15 JPN's public key is for identification of the Malaysian citizen. The MyKad EBA reader is designed only for reading the MyKad or MyKad EBA that has the capability to identify, authenticate and verify the MyKad owner by accessing owner's encrypted biometric fingerprint data stored in the MyKad through mutual authentication using PKI implementation and biometric fingerprint verification. It also has the capability to
 20 access current MyKad contains chips (80k and 64k) types. There are two types of the MyKad EBA reader which are Type 1 and Type 2. Type 1 is the MyKad EBA reader that performs authentication and verification process within the firmware. Type 2 is the MyKad EBA reader that performs authentication and verification in the software installed in the computing device. The Target of Evaluation (TOE) is defined as the
 25 MyKad EBA Reader Type 1.

The test method comprises four components namely:

- i. Scope of testing;
- ii. Testing environment includes the configuration;
- 30 iii. Test execution; and

iv. Analysis of findings.

The scope of testing includes security functionality testing and compatibility testing on the TOE based on protection profile, Command Set and Requirements from the JPN.

The testing environment specifies the supporting software and hardware including the configuration details for the TOE deployment, the independent test tools and supporting test tools used for the testing.

The tests were executed by following the description defined in the pre-test steps and test steps. Thus, the expected test result is specified as guidance on the result of the test.

1.2 Objective:

The objective is to provide guidance to Researchers and Evaluators internally to perform testing on the TOE for the operations of online mode and offline mode.

1.3 Scope:

The scope of testing is security functionality testing and compatibility testing on the TOE. The TOE has the capabilities of performing mutual authentication using PKI implementation and biometric fingerprint verification. The details are as the following:

1.3.1 Security Functionality Testing:

Security functional testing is based on the following documents provided by JPN:

- a. Security functional requirements (SFRs) selected from Protection Profile for Secure Smart Card Reader with Biometric Protection v2.0 (PP). The selected SFRs

are stated below:

- i. User Data Protection: The biometric fingerprint data in MyKad must be protected by PKI implementation using mutual authentication between MyKad and TOE. Once mutual authentication is successfully executed, then only the TOE extracts the biometric fingerprint data;
- ii. Identification and Authentication: The TOE must compare the captured biometric fingerprint on TOE with the fingerprint extracted from MyKad to identify, authenticate and verify the MyKad owner; and
- iii. Cryptographic Support: The TOE must provide encryption, decryption, digital signing, and digital signature verification for PKI Implementation.
- b. Command set to invoke TOE functions based on the SFRs. The command sets are based on Command Set and Guideline of EBA MyKad Reading v1.2 (Command Set).

1.3.2 Compatibility Testing:

The following is the compatibility testing requirements defined by JPN, as stated below:

- a. Compatibility testing with different ATR (Answer to Reset): The TOE should have the capabilities to read MyKad EBA through variation of ATR. ATR is defined in this document as Slow, Medium and Fast by card supplier in form of sample cards. The sample cards with different ATR may produce different timing response during the tests.
- b. Backward Compatibility Testing using MyKad with 64K chip and 80K chip: The TOE should have the capabilities to read MyKad ESA and its predecessor, such as MyKad with 64K chipset and MyKad 80K chipset through backward compatibility features that allows the TOE to read MyKad predecessors based on previous defined APDU commands.

In order for the TOE to pass the evaluation, it has to fulfill all the testing requirements as set by JPN as in sub-sections 1.3.1 and 1.3.2.

2. Test Scenario

5

This section describes the test scenario details which consist of the test rationale and test cases for both security functional testing and compatibility testing.

2.1 Test Rationale:

10

The following is the description of the test rationale which is an assumption made towards the TOE with specific objective and identified threat. Table 2.1 is test rationale for security functional testing and Table 2.2 is test rationale for compatibility testing.

15

No	Items	Description
1	Assumption	It is assumed that the TOE manufactured by the developer has the capabilities of reading biometric fingerprint data which is protected inside the MyKad EBA using JPN public key (PKI process).
2	Objectives	To ensure the TOE being tested comply toward the security functional requirements (SFRs) based on the PP document and Command Set. Refer section 1.3.1 for more details on the document PP and Command Set.
3	Threat	An attacker may have access to TOE internal memory and steal the biometric fingerprint information.

Table 2.1: Test Rationale for Security Functional Testing

No	Items	Description
1	Assumption	It is assumed that the TOE manufactured by the developer has the capabilities of reading data inside 64K and 80K version of MyKad. It should also be capable to read MyKad EBA set with different set of ATR.
2	Objectives	To ensure the TOE being tested based on requirements provided by JPN. Refer section 1.3.2 for more details.
3	Threat	The attacker or TOE user may damage the TOE including its predecessor smart card due to unable to read using correct APDU commands.

Table 2.2: Test Rationale for Compatibility Testing

2.2 Test Cases:

- 5 Based on the above rationale, the identified SFRs are mapped to the Test Case Group as below (Table 2.3 for Security Functional Testing and Table 2.4 for Compatibility Testing):

No	Security Functional Requirement (SFRs)	Test Case Group	Test Case Description
1	User Data Protection Identification and Authentication	A.1	Test Group A .1 and A.2 comprises series of offline mode test cases on TOE security functions. Refer to section 4.1 for more details.
		A.2	
2	User Data Protection Identification and Authentication	B.1	Test Group B.1 to 8.2 comprises series of online mode test cases on TOE security functions. Refer to section 4.2 (4.2.1 and 4.2.2) for more details.
		B.2	
	Cryptographic support	B.3	Test Group B.3 to B.4 comprises series of online mode test cases on TOE security functions. Refer to section 4.2 (4.2.3 and 4.2.4) for more details.
		B.4	

Table 2.3: Test cases for Security Functional Testing.

No	Test Case Group	Test Case Description
1	C.1	Test C.1. is test case on backward compatibility with 64K and 80K Mykad version on offline mode. Refer to section 4.3 for more details.
2	C.2	Test C.2, C.3 and C4 are test cases on compatibility testing for reading MyKad EBA set with different ATR. Refer to section 4.3 for more details.
	C.3	
	C.4	
3	C.5	Test C.5 is test case on backward compatibility with existing MyKad on online mode. Refer to section 4.3 for more details.

Table 2.4: Test cases for Compatibility Testing.

3. Test Environment

5

This section describes test environment which consist of the test item, test equipment, supporting test equipment and independent test tool.

3.1 Test Item, Test Equipment and Supporting Test Equipment

10

List of test items (Refer to Table 3.1), test equipment (Refer to Table 3.2) and supporting test equipment (Refer to Table 3.3) used in the testing.

Components/ Identifier	Hardware Information	Software Information	Network Configuration	Purpose/Remarks
MyKad EBA Reader	Supported Card: 1507810 and ISO/IEC 7816 standard	Supported Operating System: Windows XP, Windows 7, Windows 10 and other OS that support the CCIDID or PC/SC protocol.	Does not require any network configuration.	The TOE performs mutual authentication identity verification (biometric fingerprint verification) using a secure channel with other operational components within the TOE and produces an identity verification through P11 implementation (encryption, decryption and signing processes) inside the TOE itself. The deployment is Type 1 which is hardware (firmware) deployment.

Table 3.1: Test item(s)

CCID (Chip card interference device) protocol is a USB protocol that allows the smart card to be connected to the computer via a card reader using a standard USB interface, without the need for each manufacturer of smart cards to provide its own reader or protocol.

PC/SC is a specification for the smart card integration into computing environment.

No	Components/ Identifier	Hardware Information	Software Information	Network Configuration	Purpose/Remarks
1	LaptopWin8	Dell Latitude E5470 Intel(R) Core (TM) i7-6600U 2.8GHz 8GB RAM	Operating System: Windows 8.1 Pro.	Does not require any network configuration. The tests execute in the laptop did not require any network connectivity.	Machine where the Test Tool and Spring Card has been executed. Check compatibility TOE running on Windows 8.
2	DesktopWin10	Dell Optiplex 360 Intel(R) Core (TM) 2 Duo CPU 3.33GHz 4GB RAM	Operating System: Windows 10 Pro.	Does not require any network configuration. The tests execute in the laptop did not require any network connectivity.	Machine where the Test Tool and Spring Card has been executed. Check compatibility TOE running on Windows 10.
3	Power Bank	PINENG 3.7V 20000mAh	Not applicable	Not applicable	Attached to TOE for offline mode test.
4	Spring Card	Latitude E5470 Intel(R) Core (TM) i7-6600U 2.8GHz 8GB RAM	Operating System: Windows 8.1 Pro.	The Spring Card operated without any requirement of network connectivity.	Machine where Spring card is installed.
		Dell Optiplex 360	Operating System: Intel (R) Core (TM) 2 Duo CPU	Does not require any network configuration. The spring card operated	Machine where Spring card is installed.

			3.33 GHz 4GB RAM	without any requirement of network connectivity.	
--	--	--	---------------------	---	--

Table 3.2: Test Equipment

The Supporting Test Equipment table consists of supporting card information provided by JPN in order to perform the test. An Item No. 1 to 7 represents the authorized MyKad EBA and item 8 represents the unauthorized MyKad EBA. While, item No.9 to 10 represents the current MyKad.

No	Components/Identifier	Hardware Information	Software Information	Network Configuration	Purpose/Remarks
1	CFast1	Proposed ATR for MyKad EBA by card provider	Not applicable	Not applicable	Dummy card of subject 1, used to test TOE functionality. Information of subject 1 will be loaded to the dummy card including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003E0
2	CSlow1	Current ATR used by JPN	Not applicable	Not applicable	Dummy card of subject 1, used to test TOE functionality. Information of subject 1 will be loaded to the dummy card

					including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003E1
3	CFast2	Proposed ATR for MyKad EBA by card provider	Not applicable	Not applicable	Dummy card of subject 2, used to test TOE functionality. Information of subject 2 will be loaded to the dummy card including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003E6
4	CSlow2	Current ATR used by JPN	Not applicable	Not applicable	Dummy card of subject 2, used to test TOE functionality. Information of subject 2 will be loaded to the dummy card including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003D5

5	CDifferentSlow	Set with Slow ATR	Not applicable	Not applicable	Dummy card of subject 1 used to test TOE functionality and performance. Information of subject 1 will be loaded to the dummy card including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003D3
6	CDifferentMedium	Set with Medium ATR	Not applicable	Not applicable	Dummy card of subject 1 used to test TOE functionality and performance, Information of subject 1 will be loaded to the dummy card including fingerprint. Card injected with JPN public key. This is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003D2
7	CDifferentFast	Set with Fast ATR	Not applicable	Not applicable	Dummy card of subject 1 used to test TOE functionality and performance. Card injected with JPN public key. This

					is applicable to Security Functional Testing and Compatibility Testing. SN: 00000003E2
8	CUnknownKey	Set with Not invalid Non-JPN Public Key.	Not applicable	Not applicable	Dummy card of subject I used to test TOE functionality. Card injected with unknown public key. This is applicable to Security Functional Testing and Compatibility Testing. SN:00000003E3
9	MyKad1	80K Chip	Not applicable	Not applicable	Original MyKad has been issued by JPN of subject I. This is applicable to Compatibility Testing.
10	MyKad2	64K Chip	Not applicable	Not applicable	Original MyKad has been issued by JPN of subject 2. This is applicable to Compatibility Testing.

Table 3.3: Supporting Test Equipment

3.2 Independent Test Tool:

- The following is the list of independent test tool (hardware and/or software) used in the testing. The usage of test tool was reviewed by CSM MySEF Research Lead and approved by CSM MySEF Lab Manager.

Software	Version	Obtained From	Description
MyKadReaderApp	1.0	In house developed Test Tools by CSM MySEF	MyKadReaderApp is an in-house by CSM MySEF testing tool developed by CSM MySEF to test TOE security function on how TOE reading MyKad EBA and checking on Public Key used for mutual authentication. The tool also used for compatibility testing.

Table 3.4: Independent Test Tool (s)

4. Test Execution

5

This section describes the test steps and expected test results of the potential findings based on the test executed on the TOE.

Successful pre-test steps and test steps will be indicated as "OK" and the failure/unexpected results of those steps will be indicated by "X". For pre-test steps or test steps indicated as "X", the results of the test step(s) do not meet the expected results defined by the developer or evaluators.

10

4.1 Test Case Group A

The following is the list of test cases that consist of test case for offline mode and security functional testing.

5

4.1.1 Test Group A.1

AIM: To test whether TOE:

- i. Able to read MyKad EBA (injected with JPN Public Key) and perform mutual authentication and verification on offline mode.
- ii. Shall clear data displayed on LCD upon the card have been removed from the TOE.

SFR(s): User Data Protection and Identification and Authentication.

ENVIRONMENT DETAILS: As per stated in Section 3.

15 PRE-TEST STEP:

Description:

1. Connect TOE to power bank. 'Welcome to use Smart Card Device' will display at LCD TOE.
2. LCD device will display 'Please insert card'

20 TEST STEP:

Description:

1. Insert CFastl to TOE.
2. LCD TOE will display 'Reading Card' and next will display Check: Right Thumb.
- 25 3. Owner of CFastl need to place right thumb in finger in thumb reader when it displays red light. For smooth test, please ensure thumb print of card owner does not dry or sweat.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 30 5. LCD TOE will display 'Reading Card....' and next will display Check: Left Thumb.

6. Owner of CFast1 need to place left thumb in finger thumb reader when it displays red light.
7. LCD TOE will display 'Comparison Finished. Verified Successfully.'
8. LCD TOE will display 'Reading Card....' and next will display 'Success!
5 "Name', "MyKad Number", "Date of Birth" and "Sex".
9. Reading CFast1 and mutual authentication on offline mode is success.
10. Repeat test step 1 to 9 with replacing CFasti to CSlow1.
11. Repeat test step 1 to 9 with replacing CFastl to CFast2.
12. Repeat test step 1 to 9 with replacing CFastl to CSlow2.
- 10 13. Repeat test step 1 to 2.
14. Pull out the CFastl from TOE.
15. LCD TOE should display 'Please insert card' message.

EXPECTED TEST RESULTS:

PASSED:

- 15 i. TOE is able read MyKad EBA injected with JPN Public Key (using selected card mentioned: CFast1, CSlow1, CFast2 and CSlow2) and perform mutual authentication and verification on offline mode; and
- ii. TOE shall clear data once the card has been removed from the TOE and 'Please insert card' message should be displayed.

FAILED:

- 20 i. TOE is unable to read MyKad EBA injected with JPN Public Key (using selected card mention: CFastl, CSlowl, CFast2 and CSlow2) and perform mutual authentication and verification on offline mode; and
- ii. TOE is unable to clear data once the card has been removed from the
25 TOE and 'Please insert card' message should be displayed.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: The results of testing may differ for other TOE produced by different Developer. Thus, kindly consult the Developer for further understanding of

the TOE operations and responses produced during the test.

4.1.2 Test Group A.2

- 5 **AIM:** To test whether TOE is able to differentiate the authorized MyKad EBA injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key), performs mutual authentication and verification on offline mode.

SFR(s): User Data Protection and Identification and Authentication.

- 10 **ENVIRONMENT DETAILS:** As per stated in Section 3.

PRE-TEST STEP:

Description:

1. Connect TOE to power bank. 'Welcome to use Smart Card Device' will display at LCD TOE.
- 15 2. LCD device will display 'Please insert card'

TEST STEP:

Description:

1. Insert CUnknownKey to TOE.
2. LCD TOE will display 'Reading Card'.
- 20 3. LCD TOE will display:
 FAILED
 Cannot gen pub key
 Error ID = 0007
 Please pull out card.
- 25 4. Reading MyKad EBA (injected with unknown public key) and perform mutual authentication on offline mode is failed.

EXPECTED TEST RESULTS:

PASSED:

TOE able to differentiate authorized MyKad EBA (injected with JPN public

key) with unauthorized MyKad EBA (injected with unknown public key), and denied from reading the card content.

FAILED: TOE unable to differentiate authorized MyKad EBA (injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key), and successfully read the card content.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: The results of testing may differ for other TOE produced by different Developer. Thus, kindly consult the Developer for further understanding of the TOE operations and responses produced during the test.

4.2 Test Case Group B

The following consist of test case for online mode and Security Functionality Testing.

4.2.1 Test Group B.1

AIM: To test whether TOE is able to read MyKad EBA (injected with JPN Public Key) and perform mutual authentication and verification on online mode.

SFR(s): User Data Protection and Identification and Authentication.

ENVIRONMENT DETAILS: As per stated in Section 3.

PRE-TEST STEP:

Description:

1. Download and install SpringCard software in a laptop.
2. Connect TOE to LaptopWin8 USB port.
3. Insert CFast1 into TOE.
4. Run installed SpringCard by going to installation path, click on SpringCard folder and then click on SQ2075 folder. Inside the folder double click on PcscDiag2.exe

TEST STEP:**Description:**

1. On the open SpringCard software, double click on 'Vendor ICC 0'.
2. Directs to a new page.
- 5 3. Default Mode for SpringCard software is PCSC mode. To check the mode device, Enter the Command APDU 'FF 72 DA 03 00' in Hexadecimal entry and click on Transmit.
4. Check Hexadecimal value on Response APDU from the card to get the result. Result will be 9000.
- 10 Note: 9000 - PCSC mode
19000 - Assistant mode
5. Next, to check reading MyKad ERA on online mode, reader should be in assistant mode. Enter the Command APDU 'FF 72 DA 00 00' in Hexadecimal entry and click on Transmit to change device mode to Assistant mode.
- 15 6. Hexadecimal value on Response APDU from the card is 009000.
7. Enter the Command APDU 'FF 72 DA 03 00' in Hexadecimal entry and click on Transmit to re-check device mode.
8. Check Hexadecimal value on Response APDU from the card to get the result. Result will be 19000.
- 20 9. Enter the Command APDU 'DA 82 00 00 00' in Hexadecimal entry and click on Transmit to perform Mutual Auth.
10. Check Hexadecimal value on Response APDU from the card to get the result. Result will be 009000. TOE LCD will be displayed 'Success!'.
- 25 11. Enter the command APDU 'DA 7C 00 00' in Hexadecimal entry and click on Transmit.
12. Re-click on Transmit to perform Verify Right thumb. Check Hexadecimal value on Response APDU from the card to get the result.
13. Owner of CFastI need to place right thumb in finger thumb reader when

light.

14. LCD TOE will display 'Comparison Finished. Verified Successfully.'
15. Enter the Command APDU 'DA 7C 00 00' in Hexadecimal entry and click on Transmit.
- 5 16. Re-click on Transmit to perform Verify Left thumb. Check Hexadecimal value on Response APDU from the card to get the result.
17. Owner of CFast1 need to place left thumb in finger thumb reader when it in red light.
18. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 10 19. Reading CFast1 and mutual authentication on assistant mode is success. LCD TOE will be displayed 'Success!' message.
20. Repeat test step 1 to 14 with replacing CFast1 to CSlow1.
21. Repeat test step 1 to 14 with replacing CFast1 to CFast2.
22. Repeat test step 1 to 14 with replacing CFast1, to CSlow2.
- 15 23. Repeat Pre-test step 1 to 4 but change in point 2 LaptopWin8 to DesktopWin10.

EXPECTED TEST RESULTS:

PASSED:

- 20 TOE is able read MyKad EBA injected with JPN Public Key (CFast1, CSlow1, CFast2 and CSlow2) and perform mutual authentication and verification on online mode.

FAILED:

- 25 TOE is unable to read MyKad EBA injected with JPN Public Key (CFast1, CSlow1, CFast2 and CSlow2) and perform mutual authentication and verification on online mode.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: the results produced are different when performing the test steps above.

4.2.2 Test Group B.2

AIM: To test whether TOE is able to read MyKad EBA (injected with JPN Public Key) with unauthorized MyKad EBA (injected with unknown public key), and failed to perform mutual authentication and verification on online mode.

SFR(s): User Data Protection and Identification and Authentication.

ENVIRONMENT DETAILS: As per stated in Section 3.

PRE-TEST STEP:

10 Description:

1. Download and install SpringCard software in a laptop.
2. Connect TOE to LaptopWin8 USB port.
3. Insert CUnKnownKey.
4. Run installed SpringCard by going to installation path, click on SpringCard
- 15 folder and then click on SQ2075 folder. Inside the folder double click on PcscDiag2.exe

TEST STEP:

Description:

1. On the open SpringCard software, double click on 'Vendor ICC 0'.
- 20 2. Directs to a new page.
3. Enter the Command APDU 'FF 72 DA 03 00' in Hexadecimal entry and click on Transmit to check device mode. Check Hexadecimal value on Response APDU from the card to get the result.
4. To check reading MyKad ERA on assistant mode, reader should be in
- 25 assistant mode. Enter the Command APDU 'FF 72 DA 00 00' in Hexadecimal entry and click on Transmit to change device mode to Assistant mode. Check Hexadecimal value on Response APDU from the card to get the result.
5. Enter the Command APDU 'FF 72 DA 03 00' in Hexadecimal entry and

click on Transmit to re-check device mode. Check Hexadecimal value on Response APDU from the card to get the result.

6. Enter the Command APDU 'DA 82 00 00 00' in Hexadecimal entry and click on Transmit to perform Mutual Auth. Check Hexadecimal value on Response APDU from the card to get the result.
7. Enter the command APDU 'DA 7C 00 00' in Hexadecimal entry and click on Transmit. Check Hexadecimal value on Response APDU from the card to get the result.
8. Reading CUnKnowKey and perform mutual authentication on assistant mode is failed.
9. Repeat Pre-test step 1 to 4 but change in pcint2 LaptopWin8 to DesktopWin10. Repeat test step 1 to 9.

EXPECTED TEST RESULTS:

PASSED:

- 15 TOE able to differentiate authorized MyKad EBA (injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key), and failed to perform mutual authentication and verification on offline mode.

FAILED:

- 20 TOE unable to differentiate authorized MyKad EBA (injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key), and failed to perform mutual authentication and verification on online mode.

- 25 **ACTUAL TEST RESULTS:** For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: Repeat step from 1 to 9 to ensure test result is correct.

4.2.3 Test Group B.3

AIM: To test whether TOE is able to perform key generation, key destruction, operation on trusted channel and digital signing.

SFR: Cryptographic support

ENVIRONMENT DETAILS: As per stated in Section 3.

5 PRE-TEST STEP:

Description:

1. The test will be running in same machine with MyKadReaderApp application server.
2. Connect TOE to LaptopWin8 USB port.
- 10 3. Insert CFast1 to TOE.
4. Start or restart apache server at Windows Service (services.msc).
5. Open a browser and enter the url of the application.
6. Login to application using
 - Login ID: admin
 - 15 Password: testtool

TEST STEP:

Description:

1. Click on 'PCSC Mode'.
 2. Click on 'Start Authenticate'.
 - 20 3. New page will be displayed, To check whether the cryptographic process is performing correctly, the result will be displayed in single page.
- Part 1
- Device Driver is PC/SC terminal Vendor ICC 0
 - Select JPN Application: Passed - 6F03444D019000
 - 25 • Select MyKad Public Key EF: Passed - 9000
 - Read MyKad Public Key EF 1st: Passed -- 128 bytes -- «128bytes data (random number)>>9000
 - Read MyKad Public Key EF 2nd: Passed -- 128 bytes -- «128bytes data (random number)>>9000

- Verify RSA Signature: Passed -- Verified Success

Part 2

- [illegible]

Part 3

- [illegible]

Part 4

- S2: Passed – 192 bytes -<<192 bytes data>>
- D7: Passed – 01 <<D0 15bytes data>>02<<31 bytes random

number as D6>>

[illegible]

- D6: Passed -- <<31 bytes data>>
- TK: Passed – 16 bytes -- <<16 bytes data. Value from D1{01} D6{0} D1{2} D6{2} D1{4} D6{4} D1{6} D6{6} D1{8} D1{10} D6{10} D1{12} D6{12} D1{14} D6{14}>>

Note: Y[X]; Y refer to D<<number>>; X refer to byte coordinate

- Select JPN EF3: Passed – 9000
- Read JPN EF3: Passed – 136bytes - <<136bytes data>>9000

Part 5

- Read JPN EF3 2nd: Passed – 136bytes - <<136bytes data>>9000

Part 6

- Select MyKad Length: Passed – 9000
- Read EF1 Length: Passed – 01CB9000
- Read EF2 Length: Passed – <<2bytes data>>9000
- Read EF3 Length: Passed – <<2bytes data>>9000
- Read EF4 Length: Passed – <<2bytes data>>9000
- Read EF5 Length: Passed – <<2bytes data>>9000
- Read EF6 Length: Passed – <<2bytes data>>9000

- Select MyKad Sign: Passed – <<2bytes data>>9000
- Read sign EF1: Passed – <<2bytes data>>9000
- Read sign EF2: Passed – <<2bytes data>>9000
- Read sign EF3: Passed – <<2bytes data>>9000

4. Reading CFast1 and mutual authentication on PCSC mode is success.

5. Click on 'Home' icon.
6. Remove Insert CFast1 from TOE and insert CSlow1. Repeat test step 1 to 5 with replacing CFast1 to CSlow1.
7. Remove Insert CSlow1 from TOE and insert CFast2. Repeat test step 1 to 5 with replacing CFast1 to CFast2.
8. Remove Insert CFast2 from TOE and insert CSlow2. Repeat test step 1 to 5 with replacing CFast1 to CSlow2.
9. Repeat Pre-test step 1 to 6 but change in point 2 LaptopWin8 to DesktopWin10. Repeat test step 1 to 8.

10 EXPECTED TEST RESULTS:

PASSED:

TOE is able to perform key generation, key destruction, operation on trusted channel and digital signing.

FAILED:

- 15 TOE is unable to perform key generation, key destruction, operation on trusted channel and digital signing.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: Repeat step from 1 to 9 to ensure test result is correct

20

4.2.4 Test Group B.4

- AIM:** To test whether TOE is able differentiate authorized MyKad EBA (injected with JPN Public Key) with unauthorized MyKad EBA (injected with unknown public key), and performs key generation, key destruction, operation on trusted channel and digital signing.

SFR(s): Cryptographic support

ENVIRONMENT DETAILS: As per stated in Section 3.

PRE-TEST STEP:

Description:

1. The test will be running in same machine with MyKadReaderApp application.
2. Connect TOE to LaptopWin8.
- 5 3. Insert CUnKnownKey to TOE.
4. Start or restart apache server at Windows Service (services.msc).
5. Open a browser and enter the url of the application.
6. Login to application using
 - Login ID: admin
 - 10 Password: testtool

TEST STEP:**Description:**

1. Click on 'PCSC Mode'.
 2. Click on 'Start Authenticate'.
 - 15 3. New page will be displayed. To check whether the cryptographic process is performing correctly, the result will be displayed in single page.
- Part 1
- Device Driver is PC/SC terminal Vendor ICC 0
 - Select JPN Application: Passed - 6F03444D019000
 - 20 • Select MyKad Public Key EF: Passed - 9000
 - Read MyKad Public Key EF 1st: Passed -- 128 bytes — «128bytes data>>9000
 - Read MyKad Public Key EF 2nd: Passed -- 128 bytes -- «128bytes data>>9000
 - 25 • Verify RSA Signature: Passed -- Verified Failed
- Part 2
- Decode Public Key: Passed
 - MyKad Modules - Public Key: Passed -- 192 bytes - «192bytes data»

- MyKad Public Exponent - Public Key: Passed – 8c40d5
 - Sha1: Passed -- 20 bytes -- <<20bytes Sha1(Public Key »
 - Get Challenge MyKad: Passed -- «8bytes data>>9000
 - D0: Passed -- 15 bytes -- «15bytes data»
 - 5 • D1: Passed -- 16 bytes — «16bytes data»
- Part 3
- D2: Passed -- 32 bytes <<32bytes data>>
 - D3: Passed -- 8 bytes -- «8bytes data»
 - D4: Passed -- 192 bytes -- «192bytes data>>
 - 10 • S1: <<data>>
 - Mutual Authentication: Failed - 6983
- Part 4
- S2: --NA--
 - D7: --NA--
 - 15 • D6: --NA--
 - TK: --NA--
 - Select JPN EF3: --NA--
 - Read JPN EF3: --NA--
- Part 5
- 20 • Read JPN EF3 2nd: --NA--
4. Reading CFast1 and mutual authentication on PCSC mode is success.
 5. Repeat Pre-test step 1 to 6 but change in point 2 LaptopWin8 to DesktopWin10. Repeat test step 1 to 4.

EXPECTED TEST RESULTS:

- 25 **PASSED:**
- TOE is able differentiate authorized MyKad EBA (injected with JPN Public Key) with unauthorized MyKad EBA (injected with unknown public key) and performs key generation, key destruction, operation on trusted channel and digital signing.

FAILED:

- TOE is unable differentiate authorized MyKad EBA (injected with JPN Public Key) with unauthorized MyKad EBA (injected with unknown public key) and able to perform key generation, key destruction, operation on trusted channel and digital signing.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: Repeat step from 1 to 5 to ensure test result is correct

10 4.3 Test Case Group C

Consist of test case for offline mode (C.1) and online mode (C.2, C.3, C.4 and C.50). This is a Compatibility Testing.

15 4.3.1 Test Group C.1

AIM: To test whether TOE is able to read different MyKad chips issued by JPN on offline mode.

ENVIRONMENT DETAILS: As per stated in Section 3.

20 PRE-TEST STEP:

Description:

1. Connect TOE to power bank. 'Welcome to use Smart Card Device' will display at LCD TOE.
2. LCD device will display 'Please insert card'

25 TEST STEP:

Description:

- A. MyKad (80K Chip)
 1. Insert MyKad to TOE.
 2. LCD TOE will display 'Reading Card' and next will display Check: Right

Thumb.

3. Owner of MyKad1 need to place right thumb in finger in thumb reader when it displays red light.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 5 5. LCD TOE will display 'Reading Card....' and next will display Check: Left Thumb.
6. Owner of MyKad1 need to place left thumb in finger thumb reader when it displays red light.
7. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 10 8. LCD TOE will display 'Reading Card....' and next will display 'Success! "Name", "MyKad Number", "Date of Birth" and "Sex"'.
9. Reading MyKad1 on offline mode is success.
- B. MyKad (64K Chip)
1. Insert MyKad2 to TOE.
- 15 2. LCD TOE will display 'Reading Card' and next will display Check: Right Thumb.
3. Owner of MyKad2 need to place right thumb in finger in thumb reader when it displays red light.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 20 5. LCD TOE will display 'Reading Card....' and next will display Check: Left Thumb.
6. Owner of MyKad2 need to place left thumb in finger thumb reader when it displays red light.
7. LCD TOE will display 'Comparison Finished. Verified Successfully.'
- 25 8. LCD TOE will display 'Reading Card....' and next will display 'Success! "Name", "MyKad Number", "Date of Birth" and "Sex"'.
9. Reading MyKad2 on offline mode is success.

EXPECTED TEST RESULTS:

PASSED:

TOE is able to read different MyKad chip (80K and 64K) issued by JPN on offline mode.

FAILED:

5 TOE is unable to read different MyKad chip (80K and 64K) issued by JPN on offline mode.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: It is recommended to use several sample cards of MyKad 64K and MyKad 80K chips for results comparison.

10

4.3.2 Test Group C.2

AIM: To test whether TOE is able to read MyKad EBA set with slow ATR and to measure the speed of reading the MyKad EBA data.

15 **ENVIRONMENT DETAILS:** As per stated in Section 3.

Description:

1. The test will be running in same machine with MyKadReaderApp application server.
2. Connect TOE to LaptopWin8 USB port.
- 20 3. Insert CDifferentSlow to TOE.
4. Start or restart apache server at Windows Service (services.msc).
5. Open a browser and enter the url of the application.
6. Login to application using
 - Login ID: admin
 - 25 Password: testtool
7. Click on 'Performance'.

TEST STEP:

Description:

1. Click on 'Start Reading'.

2. Owner of CDifferentSlow need to place right thumb in finger in thumb reader when it displays red light.
3. LCD TOE will display 'Comparison Finished. Verified Successfully.'
4. Owner of CDifferentSlow need to place left thumb in finger thumb reader when it displays red light.
5. LCD TOE will display 'Comparison Finished. Verified Successfully.'
6. New page will be displayed.
7. Record the results.
8. Repeat the test for 3 times.
9. Repeat Pre-test step 1 to 7 but change in point 2 LaptopWin8 to DesktopWin10. Repeat test step 1 to 8.

EXPECTED TEST RESULTS:

PASSED:

TOE is able to read MyKad EBA set with slow ATR.

- I. Record 1: xx seconds
 - II. Record 2: xx seconds
 - III. Record 3: xx seconds
- Average: xx seconds

FAILED:

- TOE is unable to read MyKad EBA set with slow ATR.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

- RECOMMENDATION:** Owner of card need to place the thumb print immediately after the red light appear at TOE to get actual time to record. The average should be around 24 seconds.

4.3.3 Test Group C.3

AIM: To test whether TOE is able to read MyKad EBA set with medium ATR and to

measure the speed of reading the MyKad EBA data.

ENVIRONMENT DETAILS: As per stated in Section 3.

Description:

1. The test will be running in same machine with MyKadReaderApp application server.
2. Connect TOE to LaptopWin8 USB port.
3. Insert CDifferentMedium to TOE.
4. Start or restart apache server at Windows Service (services.msc).
5. Open a browser and enter the url of the application.
6. Login to application using
 - Login ID: admin
 - Password: testtool

TEST STEP:

Description:

1. Click on 'Performance'.
2. Click on 'Start Reading'.
3. Owner of CDifferentMedium need to place right thumb in finger in thumb reader when it displays red light.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
5. Owner of CDifferentMedium need to place left thumb in finger thumb reader when it displays red light.
6. LCD TOE will display 'Comparison Finished. Verified Successfully.'
7. New page will be displayed.
8. Record the results.
9. Repeat the test for 3 times.
10. Repeat Pre-test step 1 to 6 but change in point 2 LaptopWin8 to DesktopWin10. Repeat test step 1 to 9.

EXPECTED TEST RESULTS:

PASSED:

TOE is able to read MyKad EBA set with medium ATR.

- I. Record 1: xx seconds
- II. Record 2: xx seconds
- III. Record 3: xx seconds

5 Average: xx seconds

FAILED:

TOE is unable to read MyKad EBA set with medium ATR.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

- 10 **RECOMMENDATION:** Owner of card need to place the thumb print immediately after the red light appear at TOE to get actual time to record. The average should be around 12 seconds.

4.3.4 Test Group C.4

15

AIM: To test whether TOE is able to read MyKad EBA set with fast ATR and to measure the speed of reading the MyKad EBA data.

ENVIRONMENT DETAILS: As per stated in Section 3.

Description:

- 20 1. The test will be running in same machine with MyKadReaderApp application server.
2. Connect TOE to LaptopWin8 USB port.
3. Insert CDifferentFast to TOE.
4. Start or restart apache server at Windows Service (services.msc).
- 25 5. Open a browser and enter the url of the application.
6. Login to application using
- Login ID: admin
- Password: testtool

TEST STEP:

Description:

1. Click on 'Performance'.
2. Click on 'Start Reading'.
3. Owner of CDifferentFast need to place right thumb in finger in thumb
5 reader when it displays red light.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
5. Owner of CDifferentFast need to place left thumb in finger thumb reader
when it displays red light.
6. LCD TOE will display 'Comparison Finished. Verified Successfully.'
7. New page will be displayed.
10
8. Record the results.
9. Repeat the test for 3 times.
10. Repeat Pre-test step 1 to 6 but change in point 2 LaptopWin8 to
DesktopWin10. Repeat test step 1 to 9.

15 EXPECTED TEST RESULTS:**PASSED:**

TOE is able to read MyKad EBA set with fast ATR.

- I. Record 1: xx seconds
 - II. Record 2: xx seconds
 - 20 III. Record 3: xx seconds
- Average: xx seconds

FAILED:

TOE is unable to read MyKad EBA set with fast ATR.

ACTUAL TEST RESULTS: For evaluator and researcher: Kindly select the
25 expected result as stated above based on your testing finding.

RECOMMENDATION: Owner of card need to place the thumb print immediately
after the red light appear at TOE to get actual time to record. The average should be
around 9 seconds.

4.3.5 Test Group C.5

AIM: To test whether TOE is able to read different MyKad chips issued by JPN on online mode.

5 **ENVIRONMENT DETAILS:** As per stated in Section 3.

Description:

1. The test will be running in same machine with MyKadReaderApp application server.
2. Connect TOE to LaptopWin8 USB port.
- 10 3. Insert MyKad1 to TOE.
4. Start or restart apache server at Windows Service (services.msc).
5. Open a browser and enter the url of the application.
6. Login to application using
 - Login ID: admin
 - 15 Password: testtool

TEST STEP:

Description:

1. Click on 'Compatibility'.
2. Click on 'Start Reading'.
- 20 3. Owner of MyKad1 need to place right thumb in finger in thumb reader when it displays red light.
4. LCD TOE will display 'Comparison Finished. Verified Successfully.'
5. Owner of MyKad1 need to place left thumb in finger thumb reader when it displays red light.
- 25 6. LCD TOE will display 'Comparison Finished. Verified Successfully.'
7. New page will be displayed with compatibility field 'Compatibility Success'.
8. Repeat the steps 1-7 using MyKad2.
9. Repeat Pre-test step 1 to 6 but change in point 2 LaptopWin8 to

DesktopWin10. Repeat test step 1 to 8.

EXPECTED TEST RESULTS:

PASSED:

5 TOE is able to read MyKad (80K and 64K) chip issued by JPN on online mode.

FAILED:

TOE is unable to read MyKad (80K and 64K) chip issued by JPN on online mode.

10 **ACTUAL TEST RESULTS:** For evaluator and researcher: Kindly select the expected result as stated above based on your testing finding.

RECOMMENDATION: It is recommended to use several sample cards of MyKad 64K and MyKad 80K chips for results comparison.

5. Analysis

15

This section describes the analysis of findings based on test executed in Section 4.

For evaluator and researcher, kindly select the analysis as stated below (section 5.1 and 5.2) based on the testing finding.

20

5.1 Analysis of the Test Findings for Test Cases with PASSED results.

Below is the analysis representation for the PASSED test findings for the purpose of guiding Researcher and Evaluator on Test Group A, B and C:

25

a) Test Group A: consists series of test cases on TOE with offline mode functionality, while Test Group B consist series of test cases on TOE with online mode functionality. Based on both the series of tests it is defined that:

- i. The TOE is able to read MyKad EBA.
- ii. The TOE is able to clear the data immediately inside the TOE

memory once the card has been removed.

iii. The TOE is able to differentiate authorized MyKad EBA (injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key) to avoid identity theft.

5 b) Test Group C consists series of test cases on Compatibility functionality.

Based on the series of test:

i. The TOE is able to read different MyKad chips (80k and 64k) on offline or online mode.

ii. The TOE is able to read slow, medium and fast ATR MyKad EBA.

10

The TOE is working correctly showing that the developer has followed the command set document provided by JPN.

5.2 Analysis of Test Findings for Test Cases with FAILED results.

15

Below is the analysis representation for the FAILED test findings for the purpose of guiding Researcher and Evaluator on Test Group A, B and C:

a) Test Group A consists series of test cases on TOE offline mode functionality, while Test Group B consist series of test cases on TOE online mode

20 functionality. Based on both the series of tests:

i. The TOE unable to read MyKad EBA. Developer need to fix the TOE by following the command set document provided by JPN.

ii. The TOE unable to clear the data immediately inside the TOE memory once the card has been removed. Developer need to fix the TOE to avoid an attacker to access the TOE memory and steal the biometric information.

25

iii. The TOE unable to differentiate authorized MyKad EBA (injected with JPN public key) with unauthorized MyKad EBA (injected with unknown public key) to avoid identity theft. JPN need to change the algorithms for

cryptographic process to ensure TOE able to differentiate authorized and unauthorized MyKad EBA.

b) Test Group C consists series of test cases on Compatibility functionality.

Based on the series of test:

- 5 i. The TOE which is not able to read different MyKad chips (80k and 64k) on offline or online mode will interrupt the process of retrieving user info from MyKad.
- ii. The TOE is not able to read slow, medium and fast ATR MyKad EBA will interrupt the process of retrieving user info from MyKad.

10

It is recommended to the developer to fix the TOE by meeting the requirements in the PP and Command Set document provided by JPN.

The present disclosure includes as contained in the appended claims, as well as that of
15 the foregoing description. Although this invention has been described in its preferred form with a degree of particularity, it is understood that the present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction and the combination and arrangements of parts may be resorted to without departing from the scope of the invention.

20

CLAIMS

1. A method for testing and preventing tampering attack on a card reader (110), the method comprising the steps of:
 - 5 establishing, by a card reader module (111), a communication link with a smart card (130) for communicating information between the card reader module (111) and the smart card (130);
 - identifying, by the card reader module (111), a pre-stored public key from the smart card (130) for comparison with a plurality of reference public keys stored in a data
 - 10 repository (150); and
 - determining, by a verification module (117), validity of the smart card based on the comparison between the pre-stored public key and the plurality of reference public keys,
 - characterized in that, upon detection of an invalid smart card, disconnects the
 - 15 communication link of the card reader module (111) with the smart card (130), by a means.
2. The method according to claim 1 further comprising the steps of clearing, by a memory clearance module (119), memory stored in the data repository upon detection
- 20 of an invalid smart card (130).
3. The method according to any preceding claims, wherein the card reading means (110) includes a biometric sensor (112), a display (113), a card receiving slot (114) and a processor (115).
- 25 4. The method according to claim 1, further comprising the steps of:
 - capturing, by the biometric sensor (112), a biometric feature from a user as a biometric data;
 - comparing, by a biometric identification module (118), the captured biometric data

with corresponding reference data stored in the smart card (130); and
 displaying, by the display (113), a message only if there is a match between the
 captured biometric data with corresponding reference biometric data stored in the
 smart card (130).

5

5. The method according to any of the preceding claims further comprising the steps
 of clearing, by the memory clearance module (119), memory of the data repository
 (150) upon completion of biometric comparison.

10 6. The method according to claim 1, wherein the data repository (150) is accessible
 via offline or online communication.

7. A tamper-proof card reading means (100) comprising:

a card reader (110) having a card receiving slot (114), configured to receive a smart
 15 card (130) comprises;

a card reading module (111), configured to establish a communication link
 with the smart card (130) for communicating information between the card reading
 means and the smart card (130);

20 a biometric sensor (112) for capturing a biometric feature from a user as a
 biometric data; and

a processor (115) comprising:

a verification module (117) for determining validity of the smart card
 based on comparison between its pre-stored public key and a plurality of
 reference public keys from a data repository (150);

25 a biometric identification module (118) for comparing the captured
 biometric data with corresponding reference biometric data stored in the smart
 card (130); and

a means for disconnecting the communication link with the smart card
 upon detection of an invalid smart card.

8. The tamper-proof card reading means according to claim 7, further comprising a memory clearance module (119) configured to clear memory stored in the data repository upon detection of an invalid smart card.

5

9. The tamper-proof card reading means according to claim 7, wherein the card reader (110) includes a biometric sensor (112), a display (113), a card receiving slot (114) and the processor (115).

10 10. The tamper-proof card reading means according to claim 7, wherein the data repository (150) is accessible via offline or online communication.