PKCS#11 Testing

1 PKCS#11 Testing

1.1 PKCS#11: IWG Conformance Profile Specification

1.1.1 Introduction

The objective of this specification is to ensure that individual implementers of the PKCS#11 v2.11 standards can interoperate in Asia region. To achieve these objectives, subsets of the PKCS #11 specifications have been defined and are detailed in the form of profiles. The profiles specify which calls must or should be implemented in order to be considered compliant. These profiles can then be used in the production of conformance testing tools that allow vendors to certify their compliance.

References and related documents

- RSA Laboratories PKCS #1 v2.0: RSA Cryptography Standard.
- RSA Laboratories PKCS #11 v2.11: Cryptographic Token Interface Standard.
- RSA Laboratories PKCS #12 v1.0: Personal Information Exchange Syntax Standard.
- RSA Laboratories PKCS #15 v1.1: Cryptographic Token Information Format Standard

PKCS#11 version compatibilities

This document is originally supporting PKCS#11 v2.11, but none of advanced functionalities of this version are compulsory required. So, all versions above 2.01 are compatible for this profile.

1.1.2 Definitions

ANSI: American National Standards Institute. An American standards body.
Application: The implementation of a well-defined and related set of functions that perform useful work on behalf of the user. It may consist of software and or hardware elements and associated user interfaces.
Application provider: An entity that provides an application.
ASN.1 object: Abstract Syntax Notation object as defined in ISO/IEC 8824. A formal syntax for describing complex data objects.
Function: A process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction.
ICC: Integrated Circuit Card. Another name for a smart card.
ISO: International Organization for Standardization
Password: Data that may be required by the application to be presented to the card by its user before data can be processed.
PIN: Personal Identification Number. See CHV.
Provider: Authority who has or who obtained the rights to create the MF or a DF in the card.
Token: In this specification, a portable device capable of storing persistent data.

Tokenholder: Analogous to cardholder.
Uniform Resource Identifiers: a compact string of characters for identifying an abstract or physical resource. Described in RFC 2396.
The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in IETF RFC 2119.

1.1.3 Symbols and Abbreviations

BER Basic Encoding Rules
DER Distinguished Encoding Rules
OID Object Identifier
PKCS Public Key Cryptography Standard
URL Uniform Resource Locator (a class of uniform resource identifiers)

1.1.4 General Overview

This document defines profiles for the PKCS #11 v2.11 specification for the interoperability in Asia region. These profiles specify the function calls necessary and assumptions made for compliance. This section outlines the model used to specify a PKCS #11 profile. Two individual profiles are specified in later sections.

Profile Model

Scope: The scope will define the purpose and limitations of the profile.

Assumptions: Explicitly states any assumptions necessary for profile conformance.

Mechanisms: States the PKCS #11 v2.11 mechanism that must be available.

Additional APIs: Specifies which additional API's must be implemented for any application that claims conformance.

Sessions: Defines the session requirements.

Threading: Defines the thread requirements.

Key Issues: Defines any key size restrictions or requirements including specific key types that must be supported.

Base APIs

The following is a basic set of APIs for IWG PKCS#11 Conformance Profile. These APIs are detailed in the PKCS #11 V2.11 specification. And these base APIs are also compliant to the base APIs of "PKCS#11: Conformance Profile Specification" written by RSA Laboratories.

C_GetFunctionList
C_Initialize
C_Finalize
C_GetInfo
C_GetSlotList

C_GetSlotInfo
C_GetTokenInfo
C_GetMechanismList
C_GetMechanismInfo
C_OpenSession
C_CloseSession
C_CloseAllSessions
C_FindObjectsInit
C_FindObjects
C_FindObjectsFinal
C_GetAttributeValue

1.1.5 IWG Signing & Verification Profile

This section contains a detailed description of the IWG Signing & Verification Profile.

Scope
This profile specifies an application and token that supports signing, verification, certificate and basic private key storage.

Assumptions

- Key generation and certification is complete.
- Private key is a private object.

Mechanisms
CKM_RSA_PKCS must be supported

Algorithms
CKA_SIGN, CKA_VERIFY must be supported.

Additional APIs
The following additional APIs as defined in PKCS v2.11 must be supported.
C_CreateObject
C_SignInit
C_Sign
C_VerifyInit
C_Verify
C_DestroyObject
C_Login
C_Logout

Sessions
A single read only session must be supported.

Threading
Base library locking is not required.

Key Issues
Key sizes must be supported for the range of 512 to 2048 bits in increments restricted by the specifications.

1.1.6 IWG Experiment Profile

This section contains a detailed description of the minimum required profile for this-year-scope. It defines minimum specifications only for RSA signing and verification functionalities.

Scope
This profile specifies an application and token that supports signing, verification, certificate and basic private key storage as minimum requirements for the IWG experiment.

Assumptions

- Key generation and certification is complete.
- Private key is a private object.
- Client certificate is a public object.
- The location of intermediate and root certificate is undefined by the profile.

Mechanisms
CKM_RSA_PKCS must be supported.

Algorithms
CKA_SIGN, CKA_VERIFY must be supported.

APIs for Experiment
The following APIs as defined in PKCS v2.11 must be supported. These APIs are minimum requirements only for IWG Experiment.

C_GetFunctionList
C_Initialize
C_Finalize
C_GetSlotList
C_OpenSession
C_CloseSession
C_FindObjectsInit
C_FindObjects
C_FindObjectsFinal
C_CreateObject
C_DestroyObject
C_Login
C_Logout
C_GetAttributeValue

C_SignInit
C_Sign
C_VerifyInit
C_Verify

Sessions
A single read only session must be supported.

Threading
Base library locking is not required.

Key Issues
The client side MUST support a key size of 1024 bits. And the host application MUST support this key size.

1.2 PKCS#11 Local Test Check Sheets

Japan

No.	Function Name	Return Code	Operation	Argument	Result
1	C_GetFunctionList	CKR_OK			OK
2	C_Initialize	CKR_OK			OK
3	C_Finalize	CKR_OK			OK
4	C_GetInfo	CKR_OK			OK
5	C_GetSlotList	CKR_OK			OK
6	C_OpenSession	CKR_OK			OK
7		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
8		CKR_SLOT_ID_INVALID			OK
9	C_CloseSession	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
10		CKR_DEVICE_REMOVED			OK
11		CKR_OK			OK
12	C_Login	CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
13		CKR_PIN_INCORRECT			OK
14		CKR_PIN_INVALID			OK
15		CKR_PIN_LEN_RANGE			OK
16		CKR_PIN_LOCKED			OK
17		CKR_USER_ALREADY_LOGGED_IN			OK
18	C_Logout	CKR_OK			OK
19		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
20		CKR_USER_NOT_LOGGED_IN			OK
21	C_FindObjectsInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
22		CKR_DEVICE_REMOVED			OK
23	C_FindObjects	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
24		CKR_DEVICE_REMOVED			OK
25	C_FindObjectsFinal	CKR_OK			OK

		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
26		CKR_DEVICE_REMOVED			OK
27	C_CreateObject	CKR_OK			OK
28		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
29		CKR_USER_NOT_LOGGED_IN			OK
30	C_DestroyObject	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
31		CKR_DEVICE_REMOVED			OK
32	C_GetAttributeValue	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
33		CKR_DEVICE_REMOVED			OK
34	C_SignInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
35		CKR_DEVICE_REMOVED			OK
36		CKR_USER_NOT_LOGGED_IN (optional)			OK
41	C_Sign	CKR_OK			OK
42		CKR_DATA_INVALID			OK
43		CKR_DATA_LEN_RANGE			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
44		CKR_DEVICE_REMOVED			OK
45	C_VerifyInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
46		CKR_DEVICE_REMOVED			OK
47		CKR_USER_NOT_LOGGED_IN			OK
52	C_Verify	CKR_OK			OK
53		CKR_DATA_INVALID			OK
54		CKR_DATA_LEN_RANGE			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
		CKR_SIGNATURE_INVALID			NA
55		CKR_DEVICE_REMOVED			OK
56		CKR_SIGNATURE_LEN_RANGE			OK
	Encryption & Decryption Functions (Optional)				

57	C_EncryptInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
58		CKR_DEVICE_REMOVED			OK
59	C_Encrypt	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
60		CKR_DEVICE_REMOVED			OK
61	C_DecryptInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
62		CKR_DEVICE_REMOVED			OK
63	C_Decrypt	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
64		CKR_DEVICE_REMOVED			OK
65		CKR_ENCRYPTED_DATA_LEN_RANGE			OK
66	C_DigestInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
67		CKR_DEVICE_REMOVED			OK
68	C_Digest	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
69		CKR_DEVICE_REMOVED			OK

Singapore

No.	Function Name	Return Code	Operation	Argument	Result
1	C_GetFunctionList	CKR_OK			OK
2	C_Initialize	CKR_OK			OK
3	C_Finalize	CKR_OK			OK
4	C_GetInfo	CKR_OK			OK
5	C_GetSlotList	CKR_OK			OK
6	C_OpenSession	CKR_OK			OK
7		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
8		CKR_SLOT_ID_INVALID			OK
9	C_CloseSession	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA

		CKR_SESSION_HANDLE_INVALID			NA
10		CKR_DEVICE_REMOVED			OK
11	C_Login	CKR_OK			OK
12		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
13		CKR_PIN_INCORRECT			OK
14		CKR_PIN_INVALID			OK
15		CKR_PIN_LEN_RANGE			OK
16		CKR_PIN_LOCKED			OK
17		CKR_USER_ALREADY_LOGGED_IN			OK
18	C_Logout	CKR_OK			OK
19		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
20		CKR_USER_NOT_LOGGED_IN			OK
21	C_FindObjectsInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
22		CKR_DEVICE_REMOVED			OK
23	C_FindObjects C_FindObjectsFinal	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
24		CKR_DEVICE_REMOVED			OK
25		CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
26		CKR_DEVICE_REMOVED			OK
27	C_CreateObject	CKR_OK			OK
28		CKR_DEVICE_REMOVED			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
29		CKR_USER_NOT_LOGGED_IN			OK
30	C_DestroyObject	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
31		CKR_DEVICE_REMOVED			OK
32	C_GetAttributeValue	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
33		CKR_DEVICE_REMOVED			OK
34	C_SignInit	CKR_OK			OK

		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
35		CKR_DEVICE_REMOVED			OK
36		CKR_USER_NOT_LOGGED_IN (optional)			OK
41	C_Sign	CKR_OK			OK
42		CKR_DATA_INVALID			OK
43		CKR_DATA_LEN_RANGE			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
44		CKR_DEVICE_REMOVED			OK
45	C_VerifyInit	CKR_OK			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
46		CKR_DEVICE_REMOVED			OK
47		CKR_USER_NOT_LOGGED_IN			OK
52	C_Verify	CKR_OK			OK
53		CKR_DATA_INVALID			OK
54		CKR_DATA_LEN_RANGE			OK
		CKR_TOKEN_NOT_PRESENT			NA
		CKR_SESSION_HANDLE_INVALID			NA
		CKR_SIGNATURE_INVALID			NA
55		CKR_DEVICE_REMOVED			OK
56		CKR_SIGNATURE_LEN_RANGE			OK

1.3 PKCS#11 Application Interoperability Test Check sheets

Listed below is the test sheet template for the Application Interoperability test conducted for the PKCS#11 test Application developed by IWG member in Singapore.

Test items (Singapore)

1. Test Table.

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
Short	Long					
ct01	ct-C11	ct	C. Taipei	1. normal	1. iwg_login	
ct02	ct-C12	ct	C. Taipei	1. normal	2. lwg_getcert	
ct03	ct-C13	ct	C. Taipei	1. normal	3. iwg_pubpubkey	
ct04	ct-C14	ct	C. Taipei	1. normal	4. iwg_sign	
ct05	ct-C15	ct	C. Taipei	1. normal	5. iwg_verify	
ct06	ct-C21	ct	C. Taipei	2. abnormal	1. iwg_login	
ct07					No scenario	
ct08					No scenario	
ct09	ct-C24	ct	C. Taipei	2. abnormal	4. iwg_sign	
ct10	ct-C25	ct	C. Taipei	2. abnormal	5. iwg_verify	
ct11	ct-J11	ct	J. Japan	1. normal	1. iwg_login	
ct12	ct-J12	ct	J. Japan	1. normal	2. lwg_getcert	
ct13	ct-J13	ct	J. Japan	1. normal	3. iwg_pubpubkey	
ct14	ct-J14	ct	J. Japan	1. normal	4. iwg_sign	
ct15	ct-J15	ct	J. Japan	1. normal	5. iwg_verify	
ct16	ct-J21	ct	J. Japan	2. abnormal	1. iwg_login	
ct17					No scenario	
ct18					No scenario	
ct19	ct-J24	ct	J. Japan	2. abnormal	4. iwg_sign	
ct20	ct-J25	ct	J. Japan	2. abnormal	5. iwg_verify	
ct21	ct-ct11	ct	K. Korea	1. normal	1. iwg_login	
ct22	ct-ct12	ct	K. Korea	1. normal	2. lwg_getcert	
ct23	ct-ct13	ct	K. Korea	1. normal	3. iwg_pubpubkey	
ct24	ct-ct14	ct	K. Korea	1. normal	4. iwg_sign	
ct25	ct-ct15	ct	K. Korea	1. normal	5. iwg_verify	
ct26	ct-ct21	ct	K. Korea	2. abnormal	1. iwg_login	
ct27					No scenario	
ct28					No scenario	
ct29	ct-ct24	ct	K. Korea	2. abnormal	4. iwg_sign	
ct30	ct-ct25	ct	K. Korea	2. abnormal	5. iwg_verify	
ct31	ct-S11	ct	S. Singapore	1. normal	1. iwg_login	
ct32	ct-S12	ct	S. Singapore	1. normal	2. lwg_getcert	
ct33	ct-S13	ct	S. Singapore	1. normal	3. iwg_pubpubkey	

ct34	ct-S14	ct	S. Singapore	1. normal	4. iwg_sign	
ct35	ct-S15	ct	S. Singapore	1. normal	5. iwg_verify	
ct36	ct-S21	ct	S. Singapore	2. abnormal	1. iwg_login	
ct37					No scenario	
ct38					No scenario	
ct39	ct-S24	ct	S. Singapore	2. abnormal	4. iwg_sign	
ct40	ct-S25	ct	S. Singapore	2. abnormal	5. iwg_verify	

2. Test Environments

Nation	Server	Client
Chinese Taipei	http://210.66.126.50/JKST/wrapper.html	gclib.dll
Japan	http://ap.pki-j-sim.jp/pkcs11/test2.html	F3EZscl2.dll
Korea	http://apptest.rootca.or.kr	Sgpkcs.dll
Singapore	http://203.126.248.102/iwg/pkcs11test_2.html	PKCS11WrapperJNI.dll.

3. Test Scenario for Abnormal Cases

1) iwg_login

a. scenario: input incorrect PIN

b. relating arguments or templates

- C_Login: Incorrect PIN (cf. “99999998”)

c. expected result: CKR_PIN_INCORRECT

2) iwg_sign

a. scenario: input data which has too big data exceed its own key size.

b. relating arguments or templates:

- C_FindObject: CK_private_key_template
- C_SignInit: CKM_PKCS_RSA
- C_Sign: Input a big data exceed its key size (cf. 300 bytes long data with 1024 bit key)

c. expected result: CKR_DATA_LEN_RANGE

3) iwg_verify

a. scenario: input signed data which generated from different key.

b. relating arguments or templates:

- C_CreateObject: CK_public_key_template
- C_VerifyInit: CKM_RSA_PKCS
- C_Verify: Input a invalid sign value (cf. random data)

c. expected result: CKR_SIGNATURE_INVALID

4. Used Templates

CK_public_key_template

- find public key object (client's RSA key pair)
- CKA_CLASS(CKO_PUBLIC_KEY), CKA_KEY_TYPE(CKK_RSA)

CK_private_key_template

- find private key object (client's RSA key pair)
- CKA_CLASS(CKO_PRIVATE_KEY), CKA_KEY_TYPE(CKK_RSA)

CK_certificate_template

- find certificate object (client's Certificate)
- CKA_CLASS(CKO_CERTIFICATE), CKA_KEY_TYPE(CKC_X_509)

CK_public_key2_template

- store public key object (server's public key)
- CKA_CLASS(CKO_PUBLIC_KEY), CKA_KEY_TYPE(CKK_RSA), CKA_TOKEN(FALSE), CKA_LABEL("IWG temporary public key object"), CKA_WRAP(FALSE), CKA_ENCRYPT(FALSE), CKA_ID(0x99), CKA_MODULUS(NULL), CKA_PUBLIC_EXPONENT(NULL)

Application Interoperability Test Sheet (SG01)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct01	ctC-11	ct	C. Taipei	1. normal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Instructions for Arguments

- (00000000) → CK_NULL_PTR
- (0012A420) → VOID_PTR (argument's address)
- TRUE, FALSE → CK_BBOOL
- (1), (2), (4) … → Slot, Object Number, input data length, ...
- 39:39:39:39:F3 → Helical binary data

Application Interoperability Test Sheet (SG02)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct02	ct-C12	ct	C. Taipei	1. normal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG03)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct03	ct-C13	ct	C. Taipei	1. normal	3. iwg_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG04)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct04	ct-C14	ct	C. Taipei	1. normal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG05)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct05	ct-C15	ct	C. Taipei	1. normal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG06)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct06	ct-C21	ct	C. Taipei	2.abnormal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG07)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct07	ct-C22	ct	C. Taipei	2.abnormal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Find_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG08)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct08	ct-C23	ct	C. Taipei	2.abnormal	3. iwg_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG09)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct04	ct-C14	ct	C. Taipei	1. normal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG10)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct05	ct-C15	ct	C. Taipei	1. normal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG11)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct11	ctJ-11	ct	J. Japan	1. normal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG12)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct12	ct-J12	ct	J. Japan	1. normal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG13)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct13	ct-J13	ct	J. Japan	1. normal	3. iwg_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG14)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct14	ct-J14	ct	J. Japan	1. normal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG15)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct15	ct-J15	ct	J. Japan	1. normal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG16)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct16	ctJ-21	ct	J. Japan	2.abnormal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
Iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG17)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct17	ct-J22	ct	J. Japan	2.abnormal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG18)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct18	ct-J23	ct	J. Japan	2.abnormal	3. iw g_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG19)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct19	ct-J24	ct	J. Japan	2.abnormal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG20)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct20	ct-J25	ct	J. Japan	2.abnormal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG21)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct21	ctK-11	ct	K. Korea	1. normal	1. iwg_login	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
Iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Instructions for Arguments

- (00000000) → CK_NULL_PTR
- (0012A420) → VOID_PTR (argument's address)
- TRUE, FALSE → CK_BBOOL
- (1), (2), (4) … → Slot, Object Number, input data length, ...
- 39:39:39:39:F3 → Helical binary data

Application Interoperability Test Sheet (SG22)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct22	ctK-12	ct	K. Korea	1. normal	2. iwg_getcert	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG23)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct23	ctK-13	ct	K. Korea	1. normal	3. iwg_putpubkey	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG24)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct24	ctK-14	ct	K. Korea	1. normal	4. iwg_sign	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG25)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct25	ctK-15	ct	K. Korea	1. normal	5. iwg_verify	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG26)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct26	ct-K21	ct	K. Korea	2.abnormal	1. iwg_login	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG27)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct27	ct-K22	ct	K. Korea	2.abnormal	2. iwg_getcert	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Find_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG28)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct28	ct-K23	ct	K. Korea	2.abnormal	3. iwg_putpubkey	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG29)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct29	ct-K24	ct	K. Korea	2.abnormal	4. iwg_sign	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG30)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct30	ct-K25	ct	K. Korea	2.abnormal	5. iwg_verify	Success

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG31)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct31	ctS-11	ct	S. Singapore	1. normal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Instructions for Arguments

- (00000000) → CK_NULL_PTR
- (0012A420) → VOID_PTR (argument's address)
- TRUE, FALSE → CK_BBOOL
- (1), (2), (4) … → Slot, Object Number, input data length, ...
- 39:39:39:39:F3 → Helical binary data

Application Interoperability Test Sheet (SG32)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct32	ctS-12	ct	S. Singapore	1. normal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG33)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct33	ctS-13	ct	S. Singapore	1. normal	3. iwg_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG34)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct34	ctS-14	ct	S. Singapore	1. normal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG35)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct35	ctS-15	ct	S. Singapore	1. normal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG36)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct36	ctS-21	ct	S. Singapore	2.abnormal	1. iwg_login	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_login	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG37)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct37	ctS-22	ct	S. Singapore	2.abnormal	2. iwg_getcert	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_getcert	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Find_ object	C_FindObjectInit			
		C_FindObjects			
		C_FindObjectFinal			
	Get_attr_ value	C_GetAttributeValue			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG38)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct38	ctS-23	ct	S. Singapore	2.abnormal	3. iwg_putpubkey	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG39)

Test Date:
Log File:
Signature:

Test No.		Test	Test	Case	Scenario	Test Result
No.	Long form	Authority	Server	(N:1. A:2)		
ct39	ctS-24	ct	S. Singapore	1. normal	4. iwg_sign	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_sign	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Fnd_ object	C_FindObjectInit			
		C_FindObjects			
	sign	C_FindObjectFinal C_SignInit			
		C_Sign			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

Application Interoperability Test Sheet (SG40)

Test Date:
Log File:
Signature:

Test No.		Test Authority	Test Server	Case (N:1. A:2)	Scenario	Test Result
No.	Long form					
ct40	ctS-25	ct	S. Singapore	1. normal	5. iwg_verify	

Scenario	Sequence	Function	Test Data		Notes
			Arguments	Result	
iwg_putpubkey	Login	C_GetFunctionList			
		C_Initialize			
		C_GetSlotList			
		C_OpenSession			
		C_Login			
	Create_ object	C_CreateObject			
	Verify	C_VerifyInit			
		C_Verify			
	Destroy_ object	C_DestroyObject			
	Logout	C_Logout			
		C_CloseSession			
		C_Finalize			

1.4 Operational Manuals for the PKCS#11 Interoperability Experiment

Operational Manual for the PKCS#11 Application from Japan

1. Preparation for client environment

1) Install JRE. Java2 Runtime Environment 1.3.1(06) is needed.

2) The PKCS#11 library is installed. The DLL file of the main body of the PKCS#11 library is stored in the Windows system folder of Windows (c:\winnt\syste32 etc.).

3) The following three files are copied in the Windows system folder (c:\winnt\system32 etc.).

- pkcs11.ini
- AsiaPKIEnv.dat
- PKCS11WrapperJNI.dll

4) Pkcs11.ini is edited, to include the PKCS#11 library file name "F3EZscl2.dll".

5) Java policy file (java.policy) is copied in the folder “lib \security" which is present in the folder where JRE is installed.

2. Start of application

1) The URL is http://ap.pki-j-sim.jp/pkcs11/test2.html

2) The following browsers are supported
Internet Explorer 5.5 SP2 and above
Netscape Communicator 6.01 and above

3) The screen as shown below in Fig-1 is displayed.

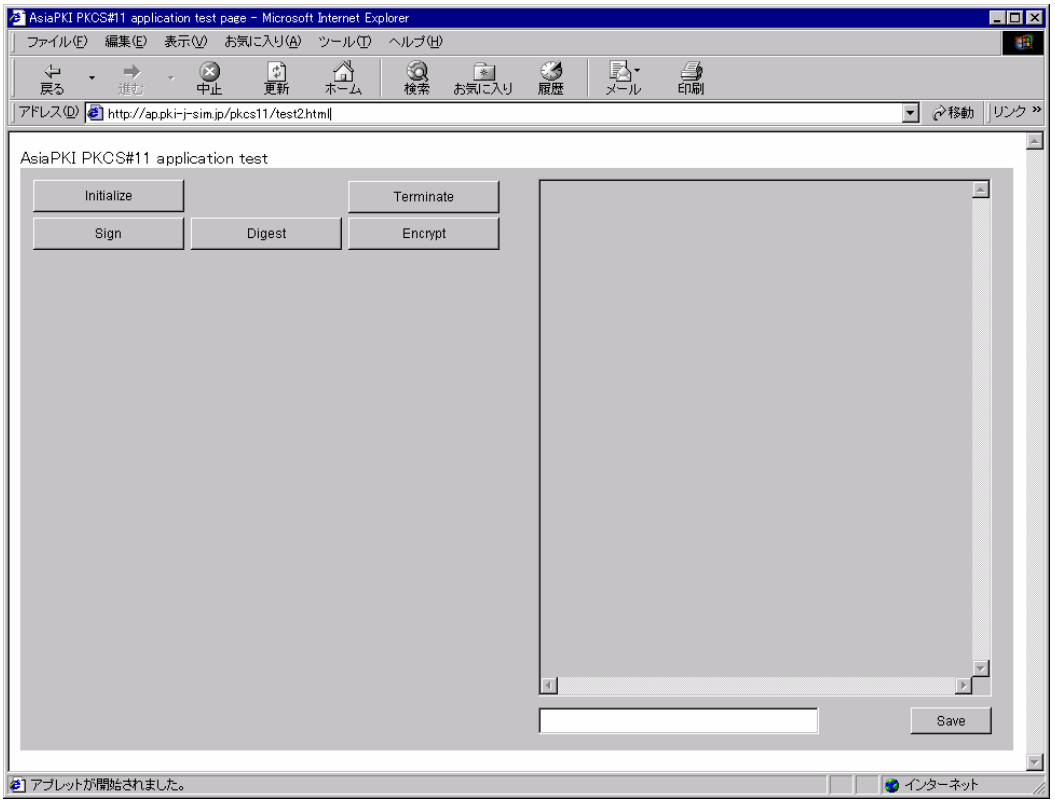


Fig 1 start screen

3. Login

1) Click on the "Initialize" button.
2) The screen as shown below in Fig-2 is displayed.

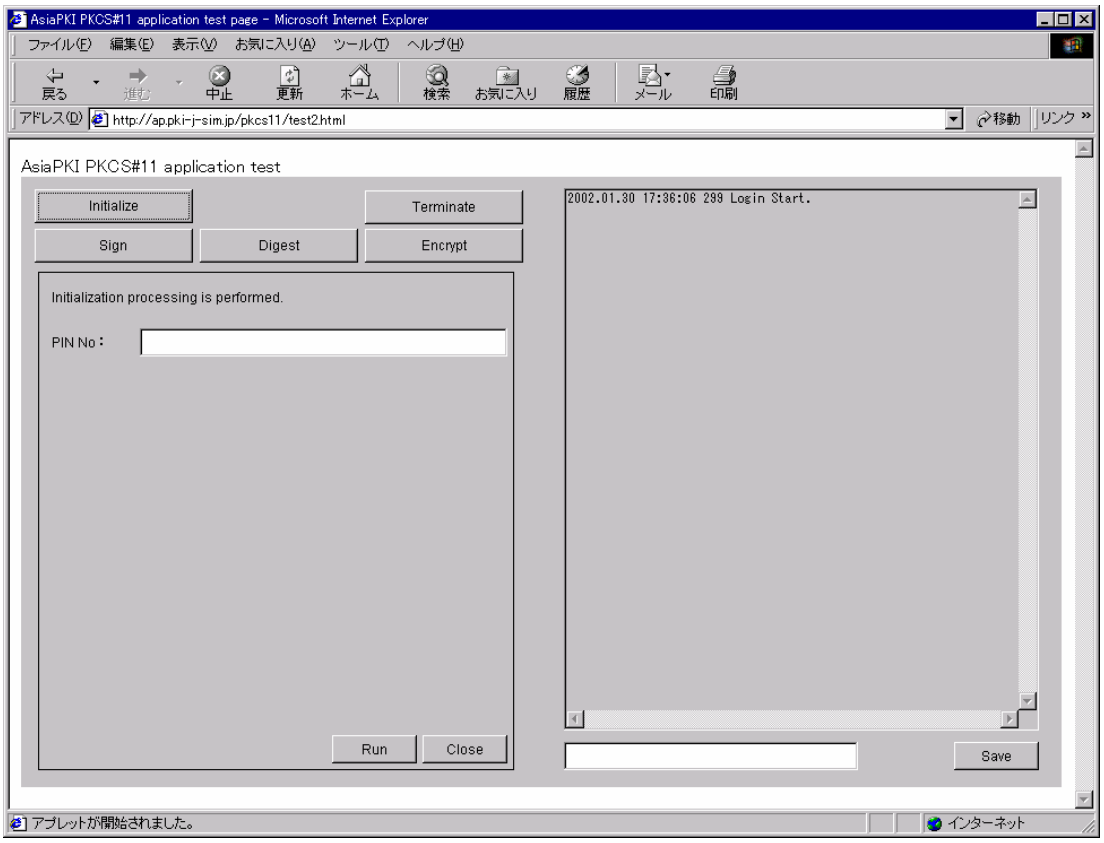


Fig 2 initialize screen

3) Input the PIN and click on the “Run” button.

4. Get_Object

1) After Initialize function is successful, Click on the “Sign” button.
2) The screen as shown below in Fig-3 is displayed.

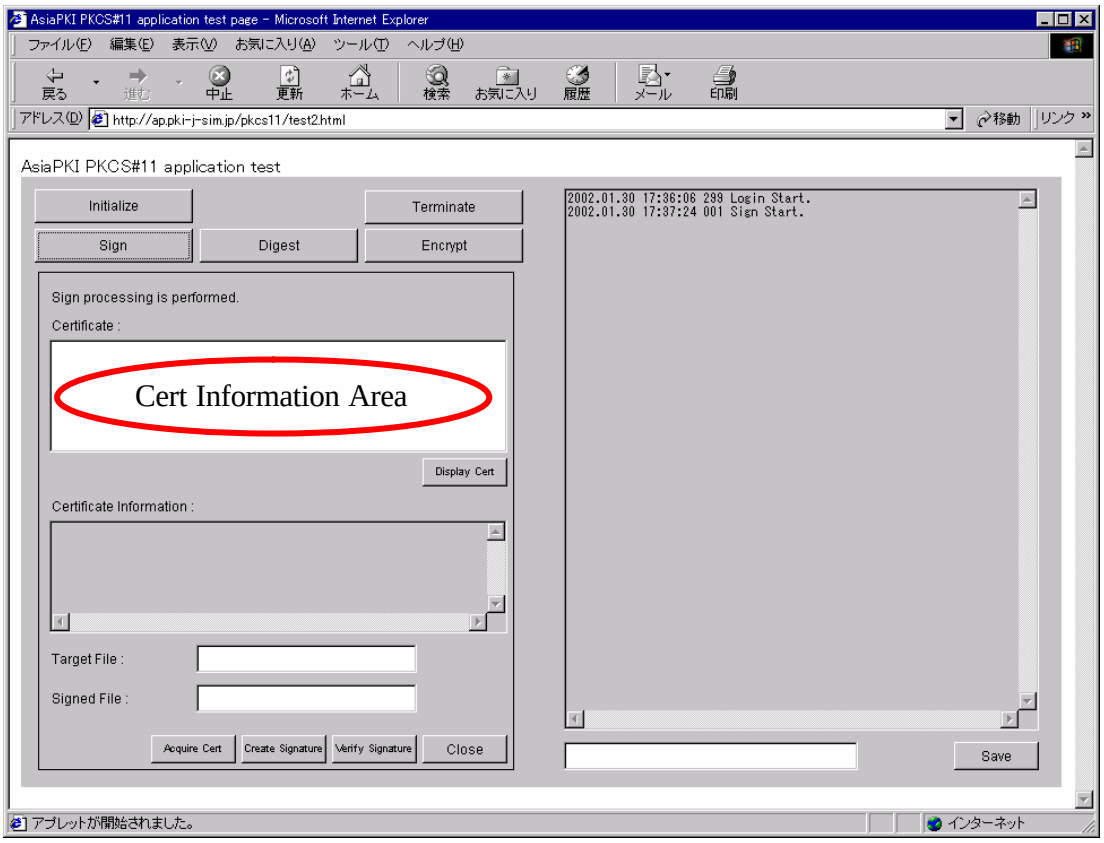


Fig 3 Sign screen

3) Click on the "Acquire Cert" button.
4) The Certificate information in the token is displayed in Fig-3 "Cert Information Area".

5. Sign

1) Enter the file name that should be signed in the "Target File" text box as seen in Fig 3 after completing the Login function and the Get_Object function.
2) Enter the output file name in the Fig-3 "Signed File" test box as seen in Fig 3.
3) Click the certificate in the list displayed in the "Cert Information Area" as seen in Fig 3.
4) Then click on the "Create Signature" button.
5) After a while, the "Close" button is clicked.

6. Verify

1) Enter the file name that should be signed "Target File" text box as seen in Fig 3 area after completing the Login function and the Get_Object function.
2) Enter the output file name in the Fig-3 "Signed File" test box as seen in Fig 3.
3) Click the certificate in the list displayed in the "Cert Information Area" as seen in Fig 3.
4) Then click on the "Verify Signature" button.
5) After a while, the "Close" button is clicked.

7. Logout

1) Click on the "Terminate" button as shown in Fig 1.
2) The screen as shown below in the Fig-4 is displayed.

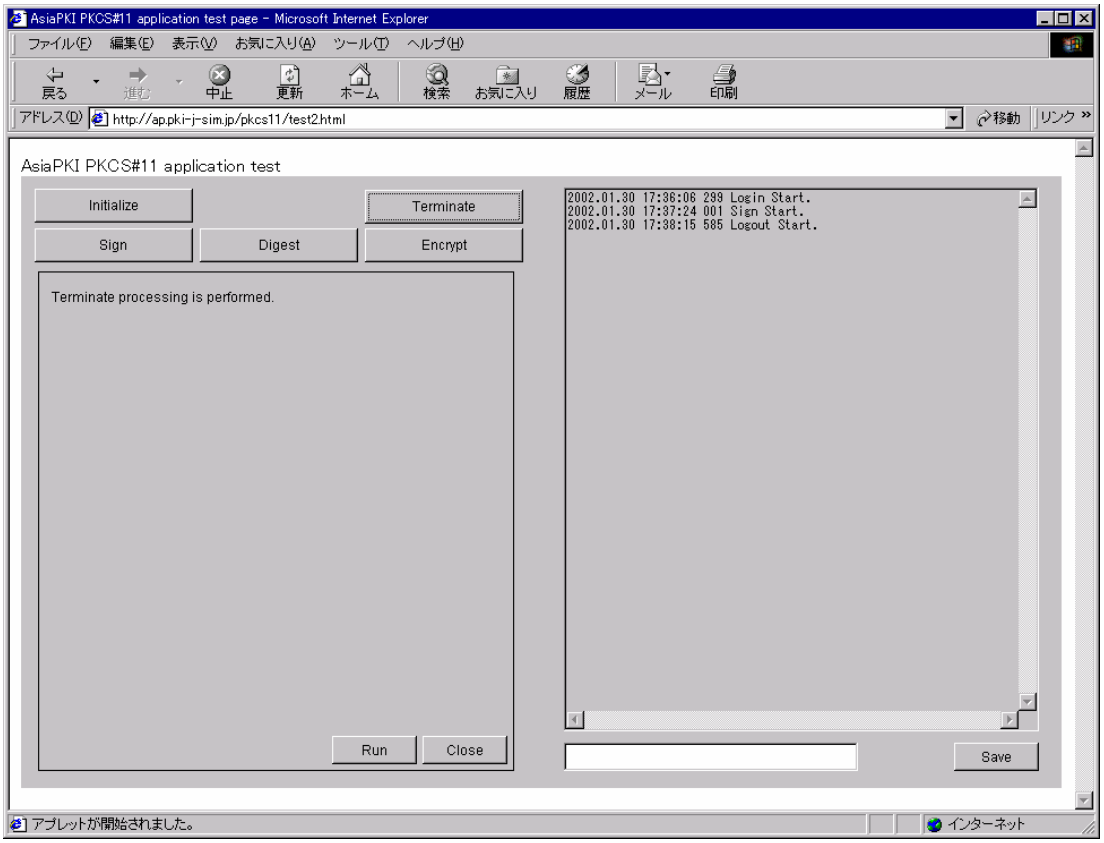


Fig 4 Terminate Screen

3) Click on the "Run" button.
4) Click on the "Close" button.

8. Encryption (optional)

1) Click on the "Encrypt" button as seen in Fig 1.
2) The screen as shown below in Fig 5 is displayed.

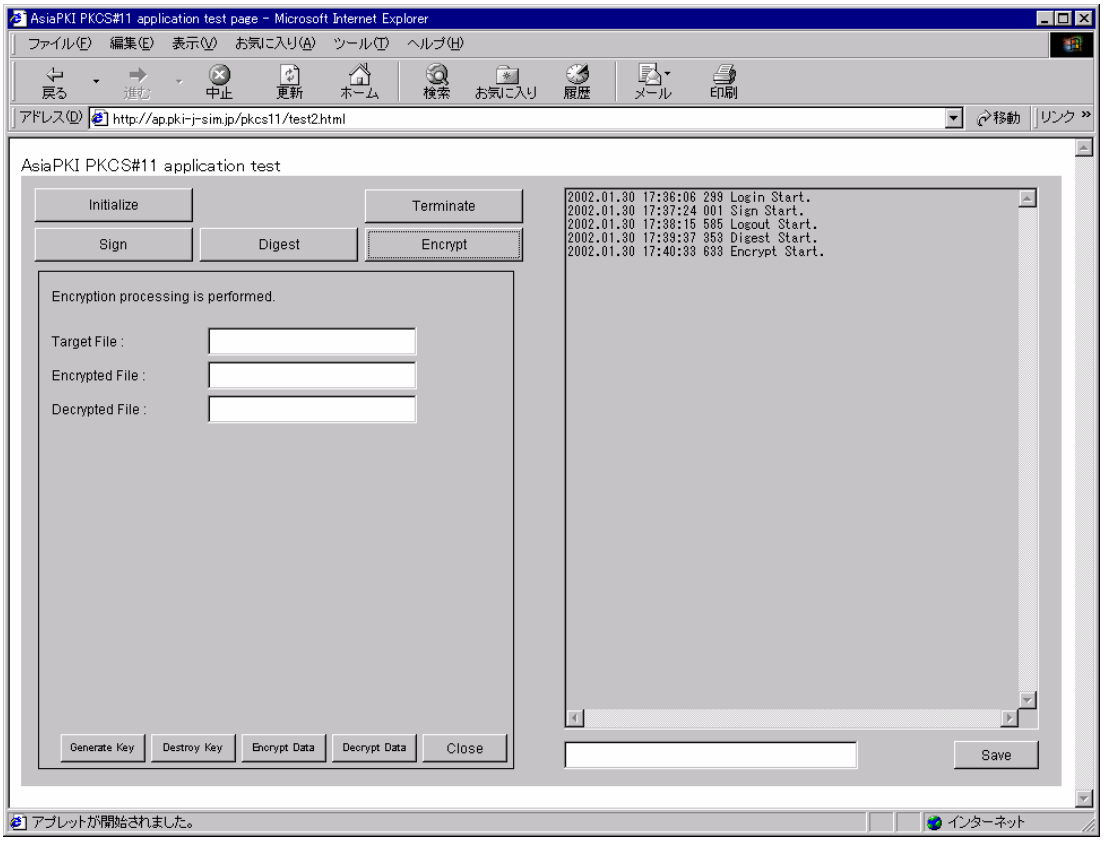


Fig 5 Encrypt Screen

3) Enter the target file name and the encrypted file name in the respective text boxes.
4) Click the "Generate Key" button.
5) Then click on the "Encrypt Data" button.
6) After the process is over, click on the "Destroy Key" button.
7) Click on the "Close" button.

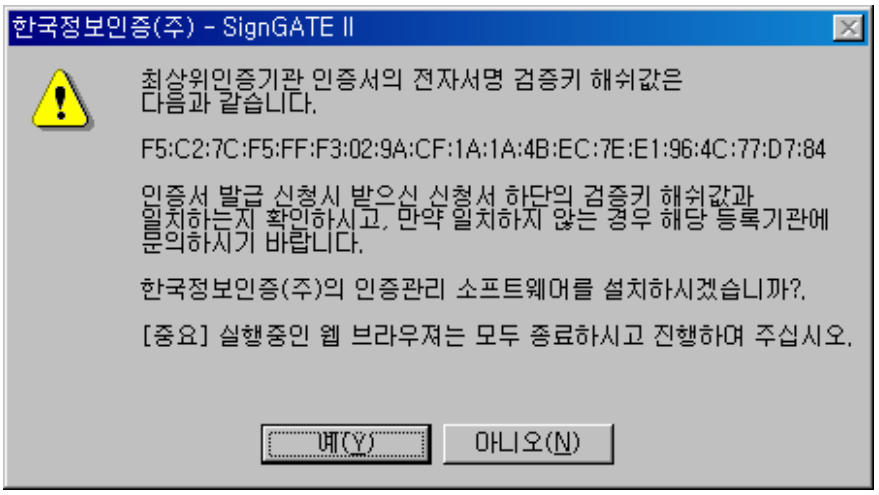
9. Decryption (optional)

1) Click on the "Encrypt" button as seen in Fig 1.
2) The screen as shown below in Fig 5 is displayed.
3) Enter the encrypted file name and the decrypted file name the respective text boxes.
4) Click on the "Decrypt Data" button.
5) Click on the "Close" button.

Operational Manual for the PKCS#11 Application from Korea

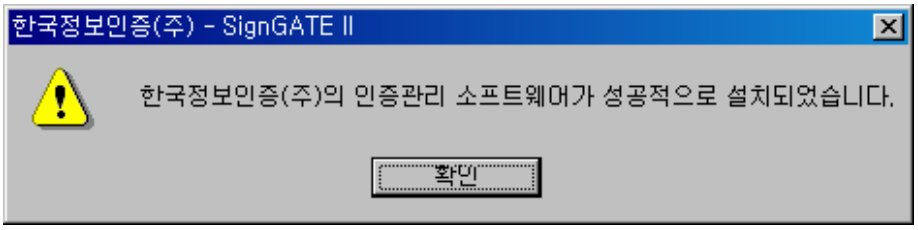
Available OS: Windows XP.
Browser: Internet Explorer 5.5 above

1. The pop-up window shown below is for checking the ROOT CA's Certificate hash. You can press the left button (Y), which means Yes.



2. If you press the left button, the installation starts.

3. The Pop-Up window as shown below denotes that the installation has finished successfully.



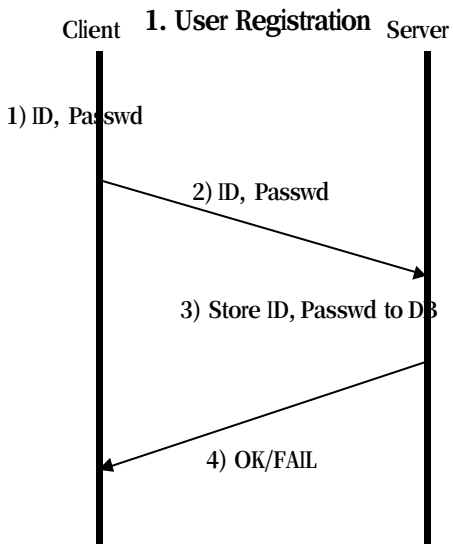
4. Unzip the Kor_PSE.zip file (containing SignCert.der and SignPriv.key) into the Windows System directory(e.g. "C:\WINDOWS\System32").

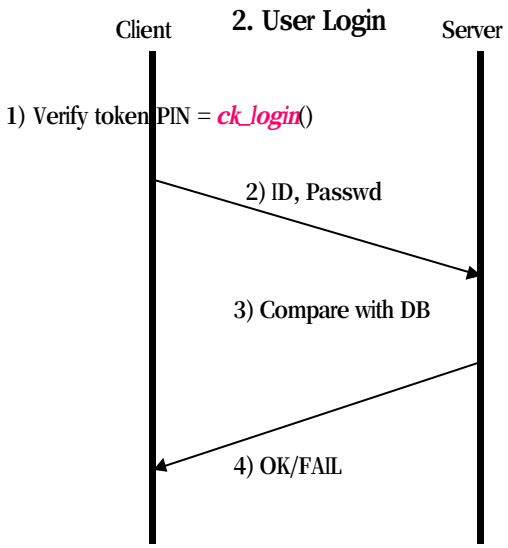
The PIN for the token is "99999999" and the PrivateKey password is "99999999".

Korea Business Application Scenario(1)

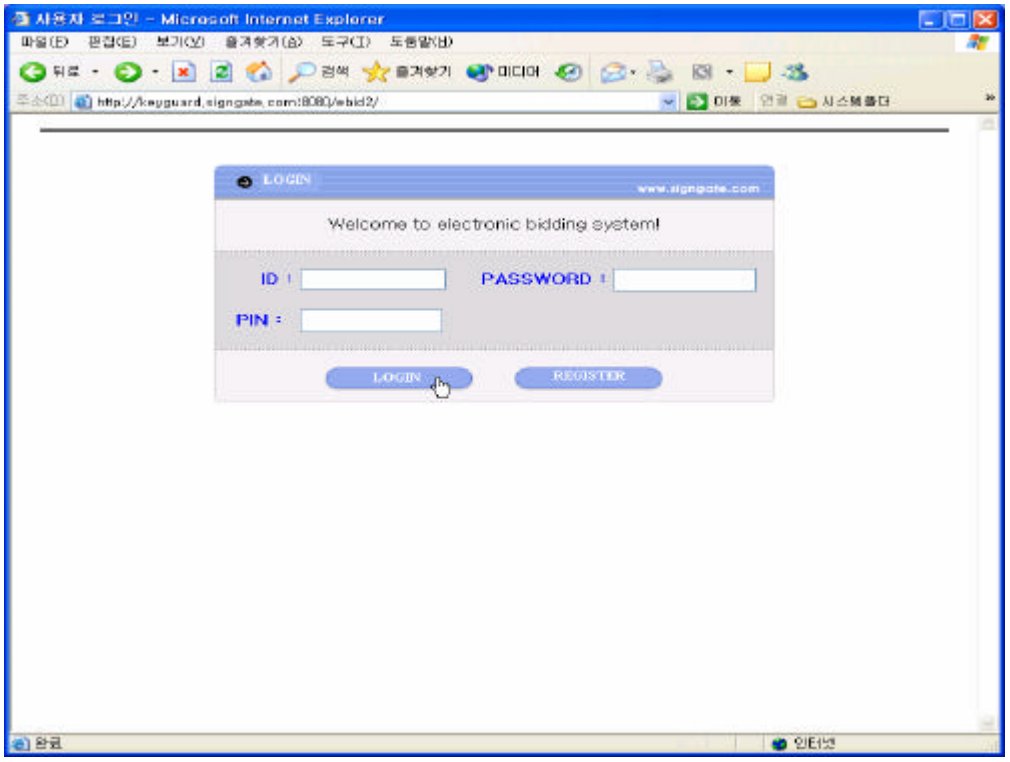
- **E-bidding application**

(red : test item) : Abstract Functions

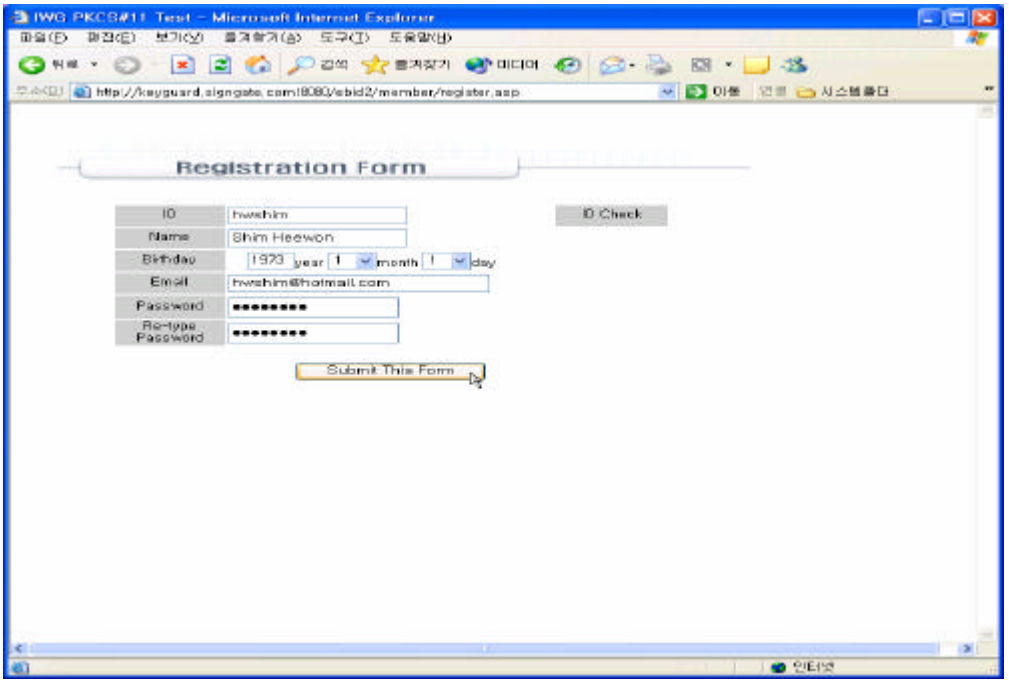




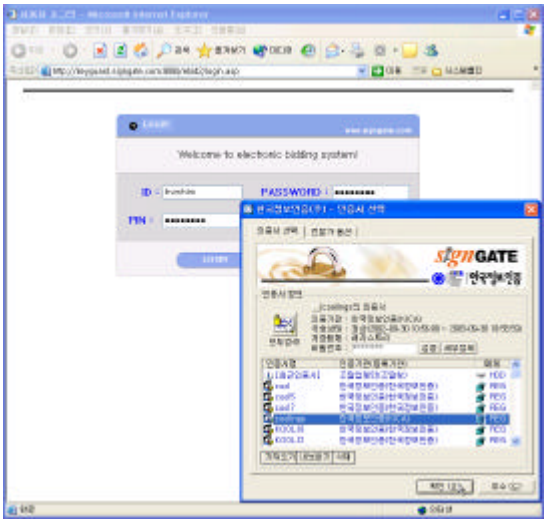
URL : http://211.252.135.223/ or http://apptest.rootca.or.kr

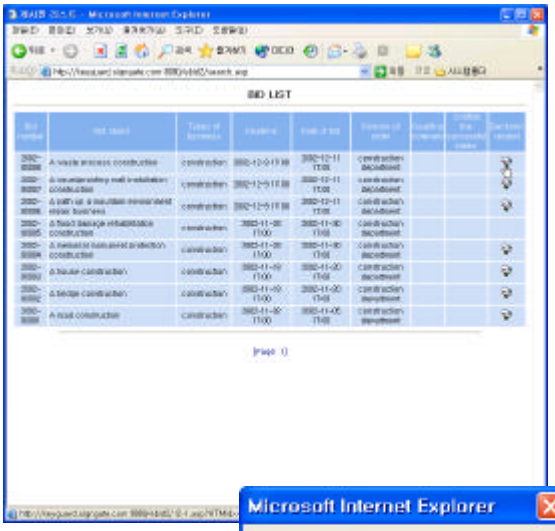


In order to register, Press [Register] Button



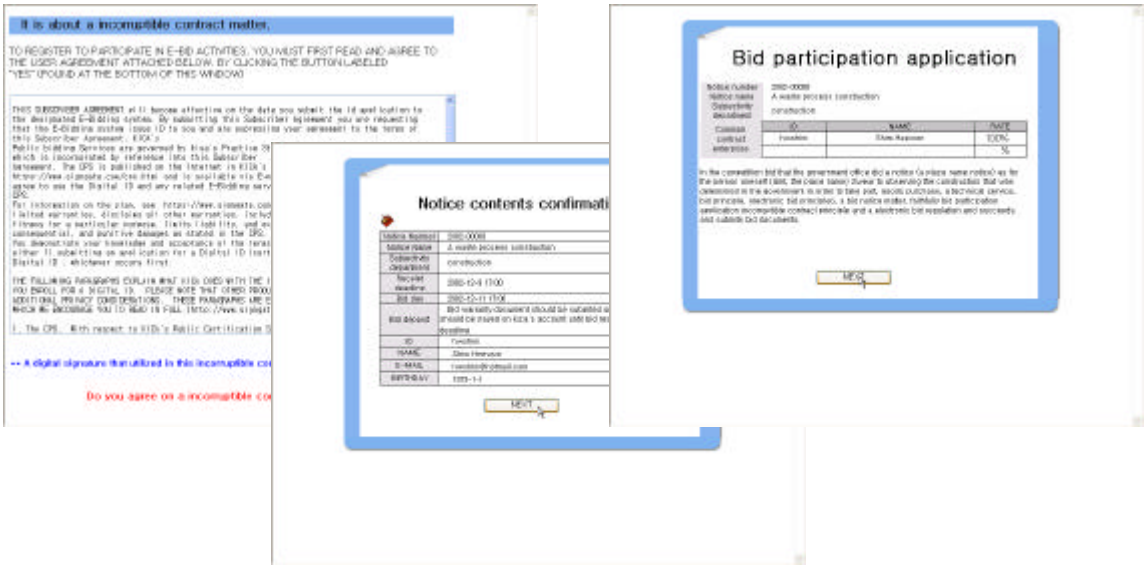
Fill in the Registration Form and Press [Submit This Form] Button





- ck_login() : Checks PIN validity

You can login with the previously registered information.

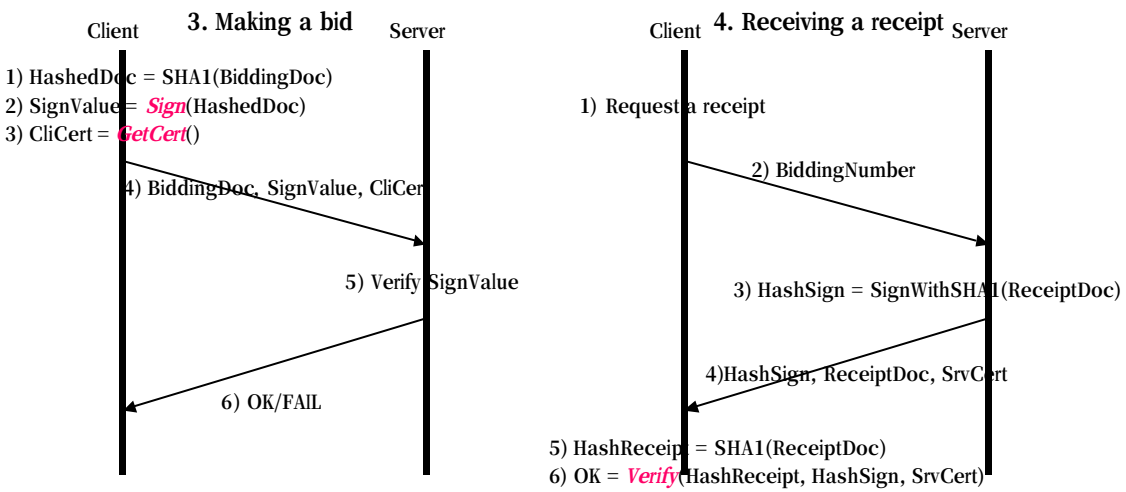


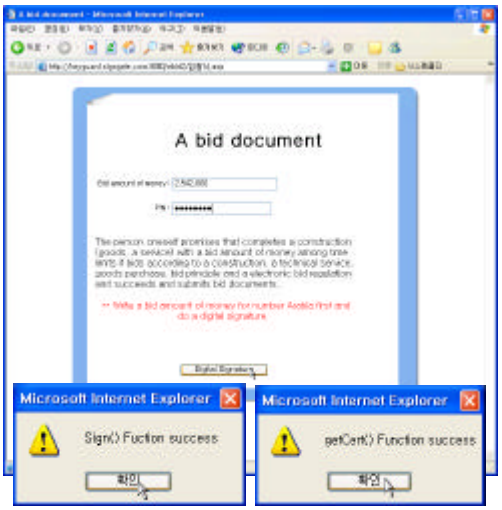
This is the Bid participation application form that you ordered.

Korea Business Application Scenario(2)

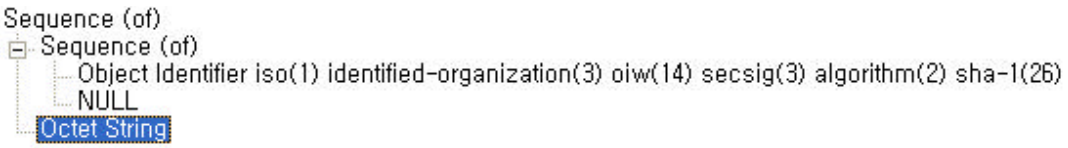
- E-bidding application (cont.)

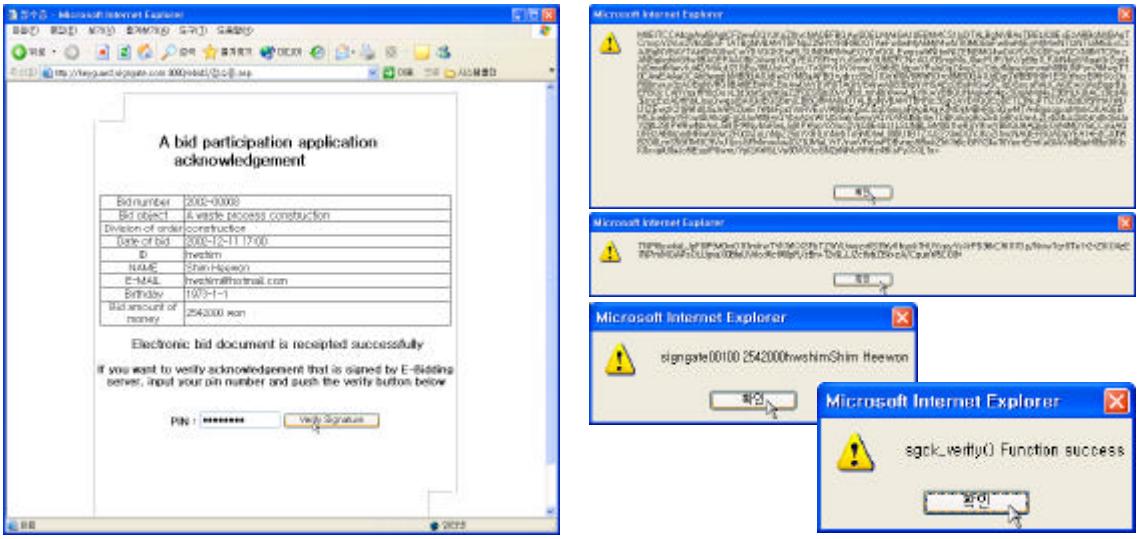
(red test) : Abstract Functions





- ck_sign()
  - PKCS#11 Token make a signature using client's private key.
- ck_get_cert()
  - Wrapper fetches a client's certificate to give to the server for verifying a client's signature.
- Signing value must be DER formed hashed data





- ck_verify() : verify a receipt generated by server.
  - ck_put_pubkey() needed internally to make a server's public key object using server's certificate.

Operational Manual for the PKCS#11 Application from Chinese Taipei

Start Application

1. Copy the file "gclib.dll" in the Windows System folder
2. The URL is http://210.66.126.50/JKST/wrapper.html

The screen as shown below is displayed in the browser

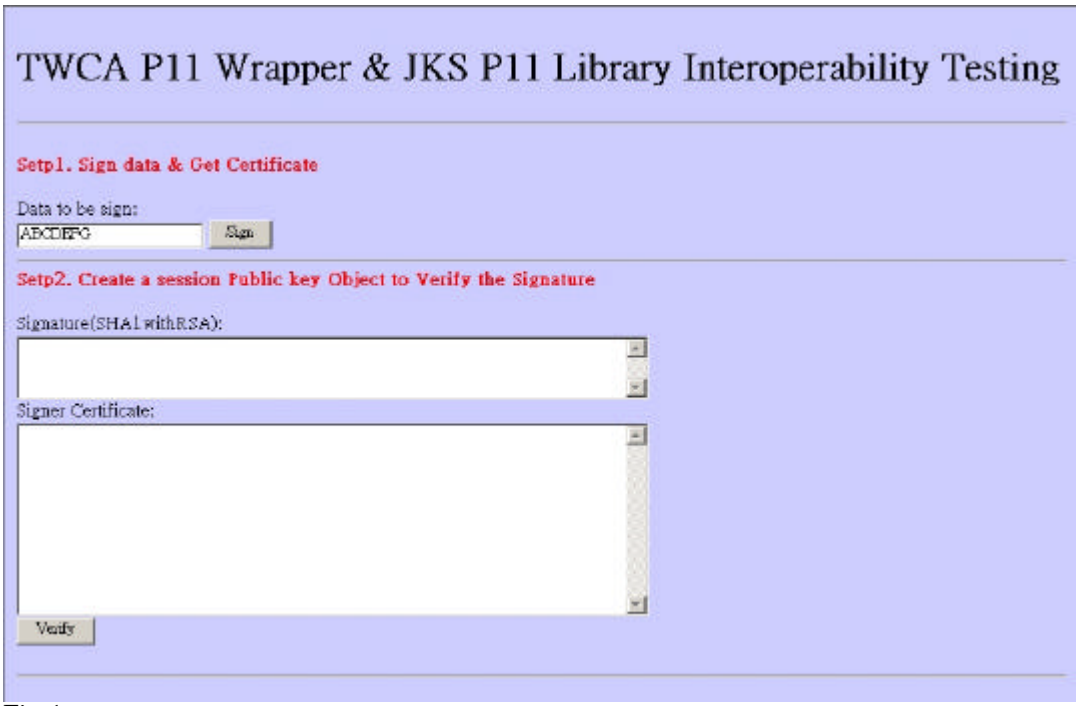


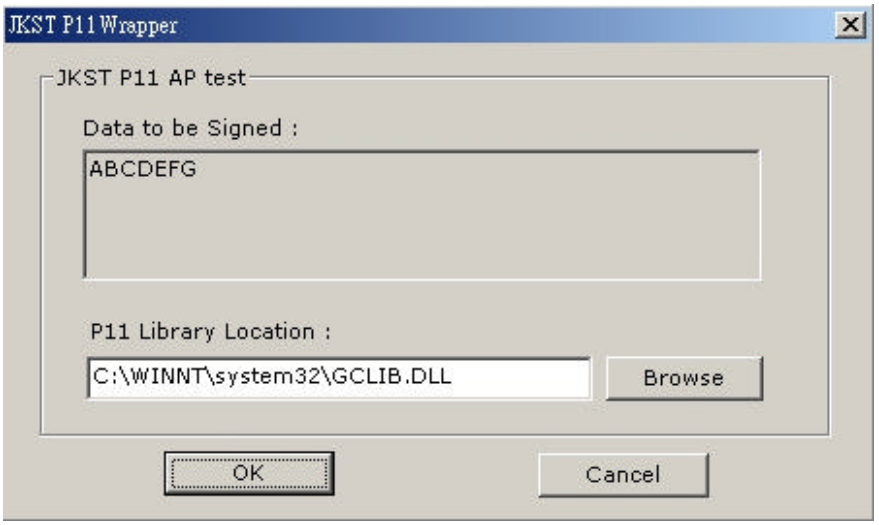
Fig 1

Step1: Sign data & Get Certificate

The following is the sequence of PKCS#11 function calls
LoadLibrary()
GetProcAddress("C_GetFunctionList")
C_GetFunctionList()
C_Initialize()
C_GetSlotList()
C_OpenSession()
C_Login()
C_SignInit()
C_Sign()
C_FindObjectsInit()
C_FindObjects()
C_FindObjectsFinal()
C_GetAttributeValue()

Testing Procedure

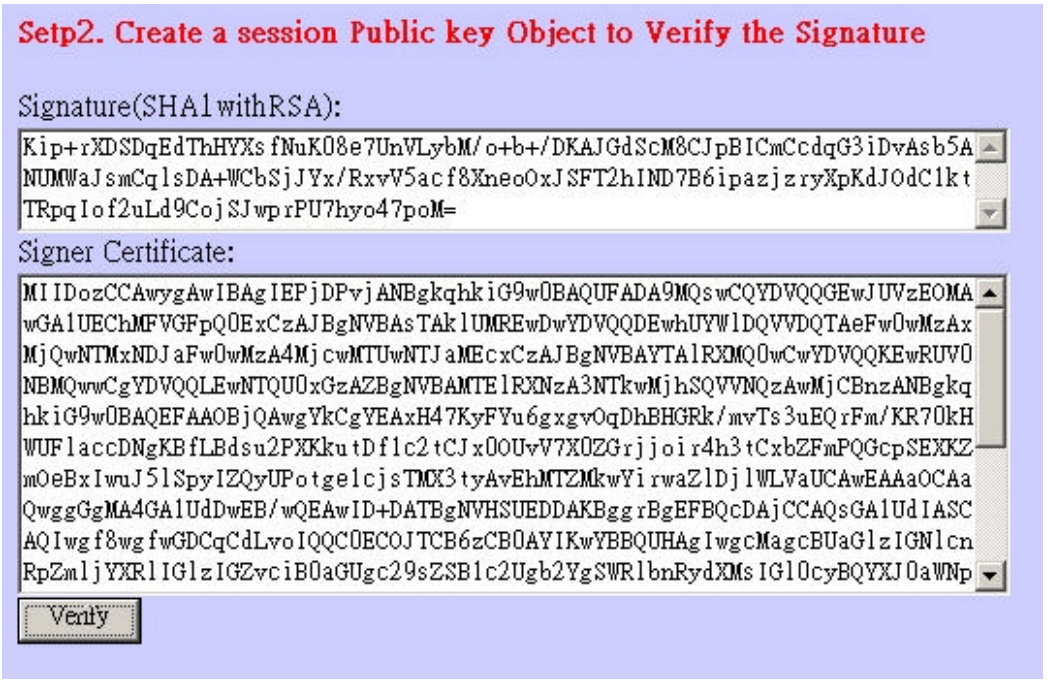
1. Click on the “Sign” button as seen in Fig 1. Then Enter the PKCS# 11 Library location as shown in the figure below. Click on the OK button.



2. The pop-up window as shown below is displayed stating that ”Sign data” procedure is completed.

3. The pop-up window as shown below is displayed stating that”Get Certificate” Procedure is completed

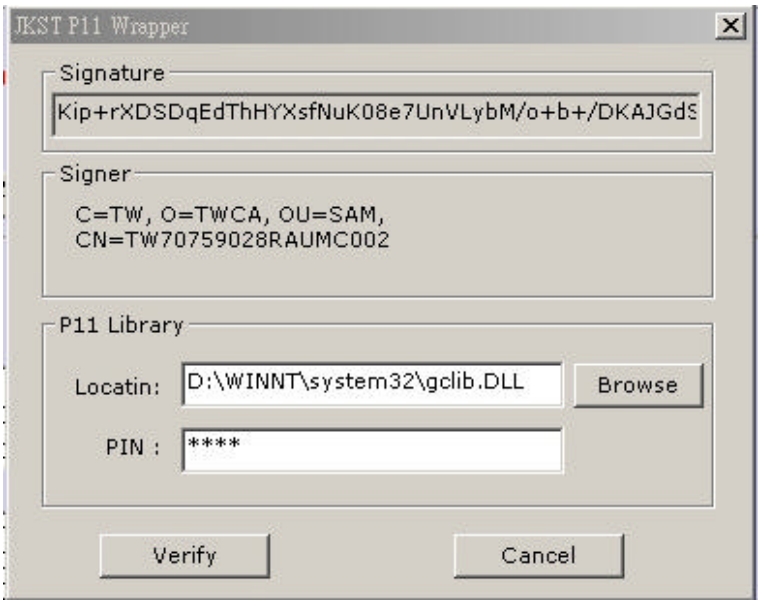
Step2. Create a session Public key Object to Verify the Signature



The following is the sequence of PKCS#11 function calls
LoadLibrary()
GetProcAddress("C_GetFunctionList")
C_GetFunctionList()
C_Initialize()
C_GetSlotList()
C_OpenSession()
C_Login()
C_CreateObject(Session Public Key Object)
C_VerifyInit()
C_Verify()

Testing Procedure

1. After Step2 is completed, click on the “Verify” button as seen in the figure above to verify the Signature
2. Enter the PKCS#11 Library location & PIN Code as seen in the figure below.



3. The pop-up window as shown below is displayed stating that “Create a session Public Key Object” procedure is completed.

4. The pop-up window as shown below is displayed stating that “Verify the Signature” procedure is completed

Operational Manual for the PKCS#11 Application from Singapore

1. Prepare the client environment

1) Install JRE.

Java2 Runtime Environment **1.4.1 (02)** is needed.

2) Install the PKCS#11 library.

The driver for your smart card is installed and the DLL file of the main body of the PKCS#11 library is stored in the system folder of Windows (e.g. **c:\winnt\system32** etc.).

3) Copy the config file.

Create a new directory **c:\iwg\,** copy **pkcs11.ini** to this directory.

4) Edit the config file.

Changes the parameter under the section [PKCS11.Driver.Name] to the PKCS#11 library file name in each country.

In the pkcs11.ini file provided by SPTC, it is "dkck201.dll".

5) Copy the **PKCS11WrapperJNI.dll.**

Copy it to system folder of Windows (e.g. **c:\winnt\system32**).

2. Start the Application

1. The URL is: http://203.126.248.102/iwg/pkcs11test_2.html

2. The browser is: Microsoft Internet Explore 5.5 & above.

3. When prompted to trust or not, please click “Yes” button.

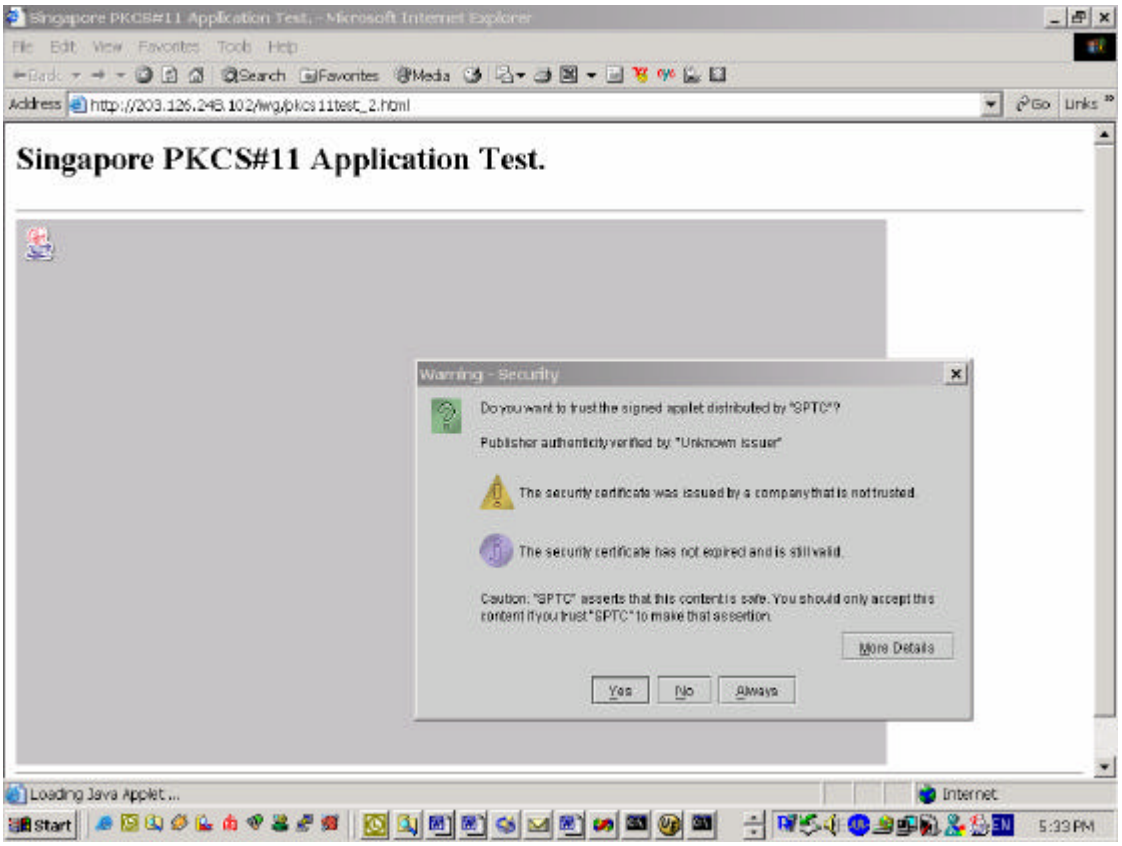


Figure 1: Start the application

4. Main Screen

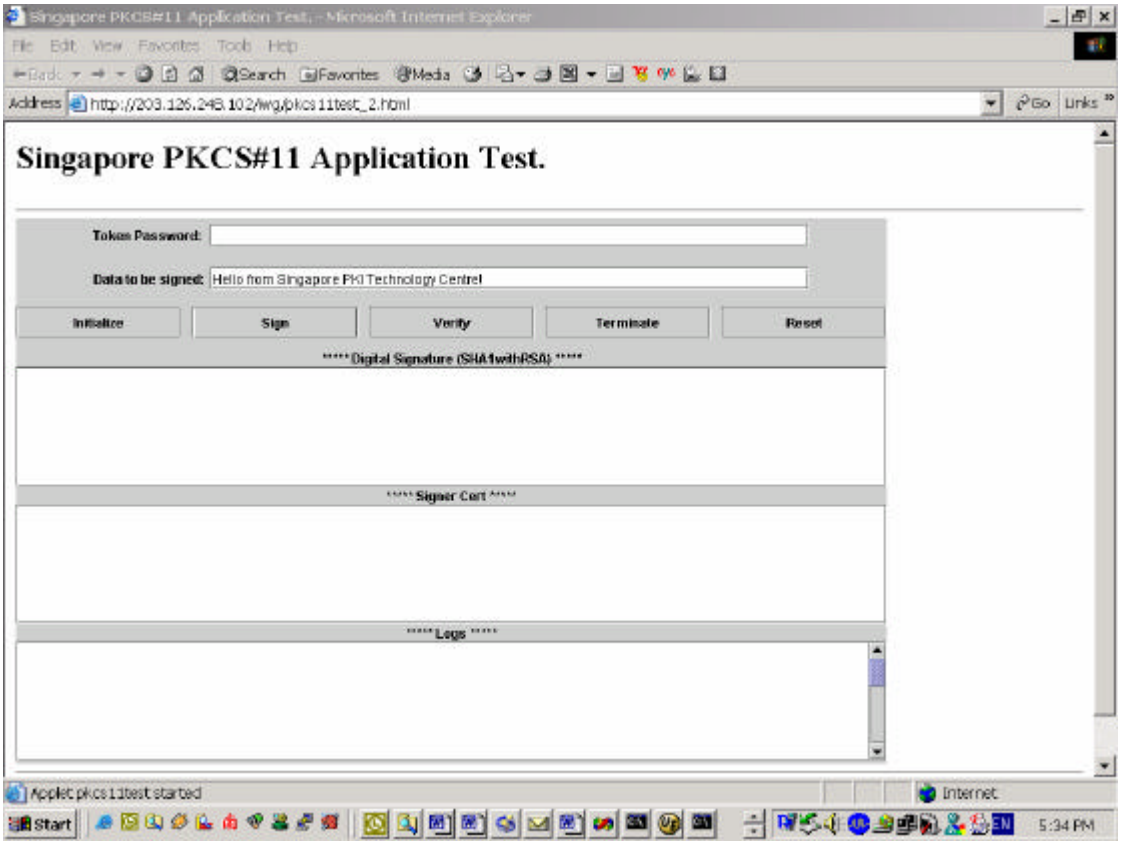


Figure 2: Main Screen

3. Functional Testing

1.5 1. Test for opening a smart card login session:

1) Enter the token password.
2) Click the “Initialize” button.
Expected Result is displayed in the “Logs “ text box (Appended after the previous result).

**********Begin initializing**********
You smart card is successfully initialized.

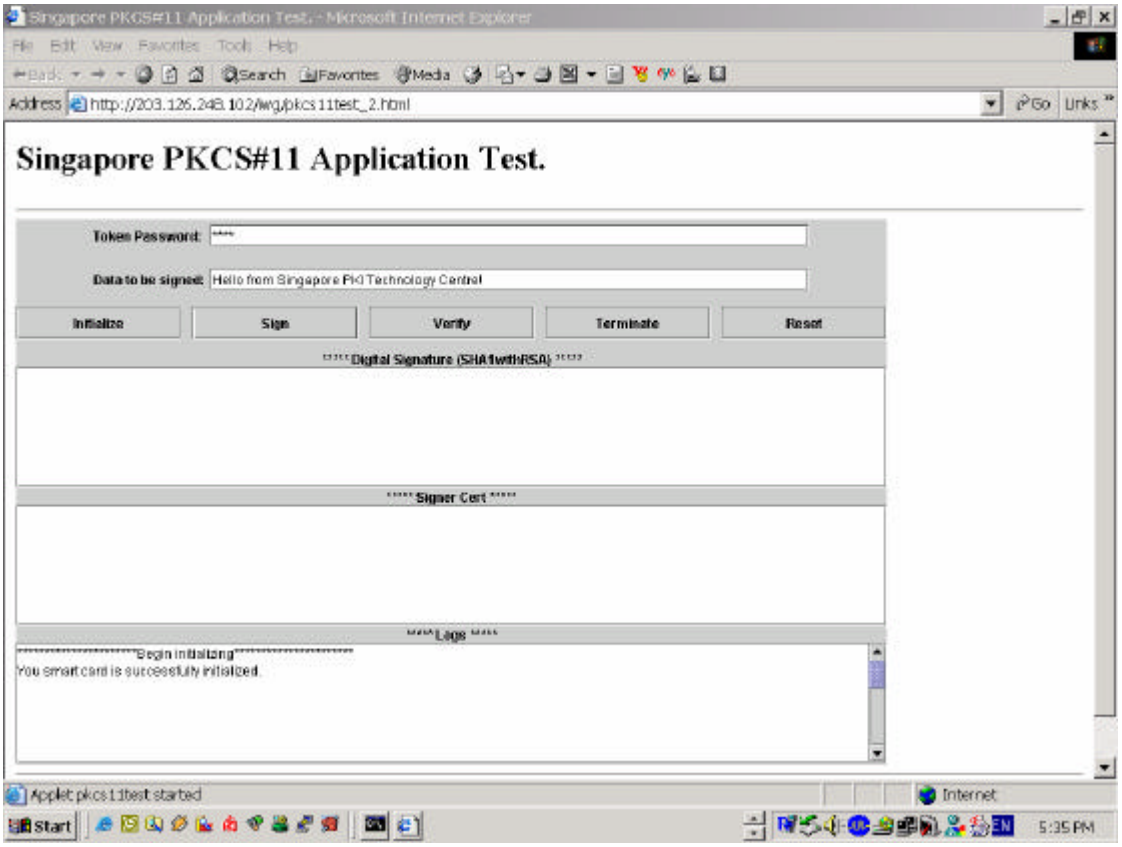


Figure 3: Initialize the Smart Card

1.6 2. Test for Digital Signing:

1) Enter the data to be signed.
2) Click the “Sign” button.
Expected Result is displayed in the “Logs “ text box (Appended after the previous result).

**********Begin Signing**********
Get the privateKey Successfully.
Sign Successfully.
Get the cert Successfully.

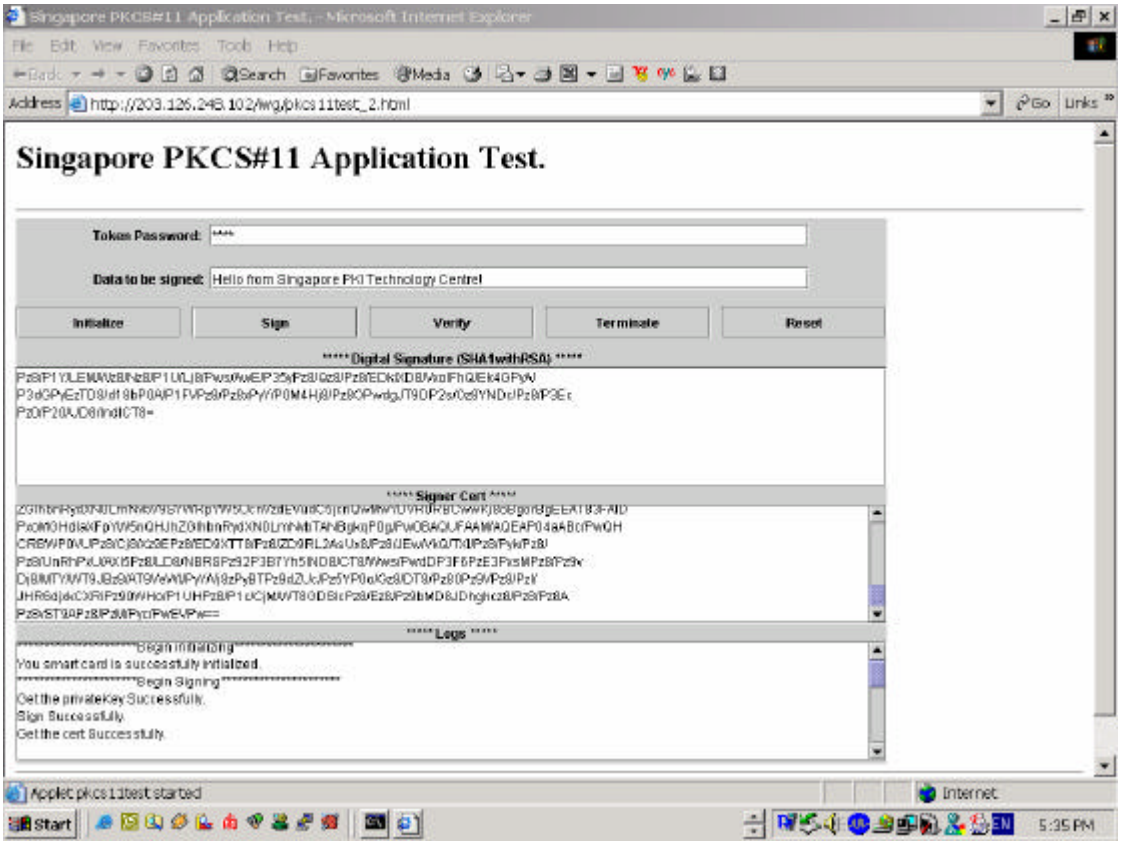


Figure 4: Sign the text

1.7 3. Test for verifying Signature:

1) Click the “Verify” button.
Expected Result is displayed in the “Logs “ text box (Appended after the previous result).

**********Begin Verifying**********
Get the public key successfully!
Verify Successfully!
The message is from the sender!

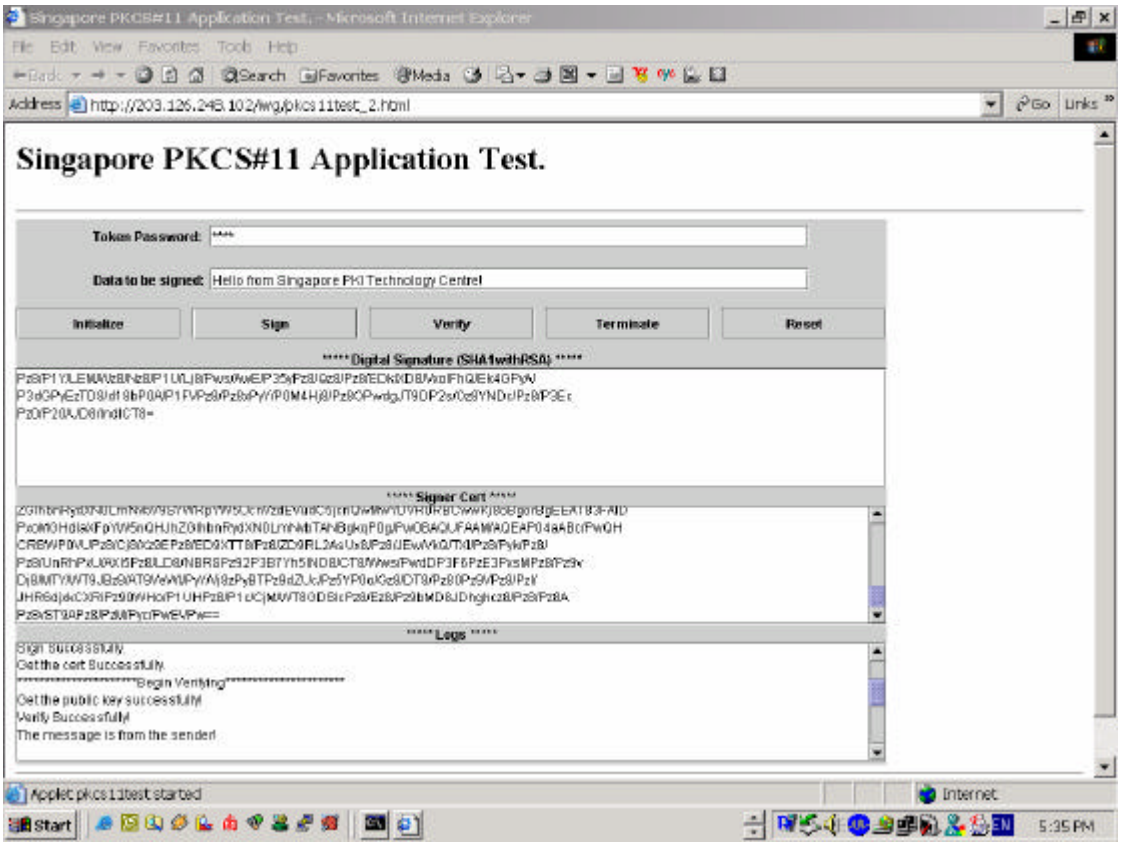


Figure 5: Verify the Signature

1.8 4. Test for terminating a smart card session:

1) Click the "Terminate" Button.
Expected Result is displayed in the "Logs " text box (Appended after the previous result).

**********Begin Terminating**********
Your smart card session is terminated successfully.

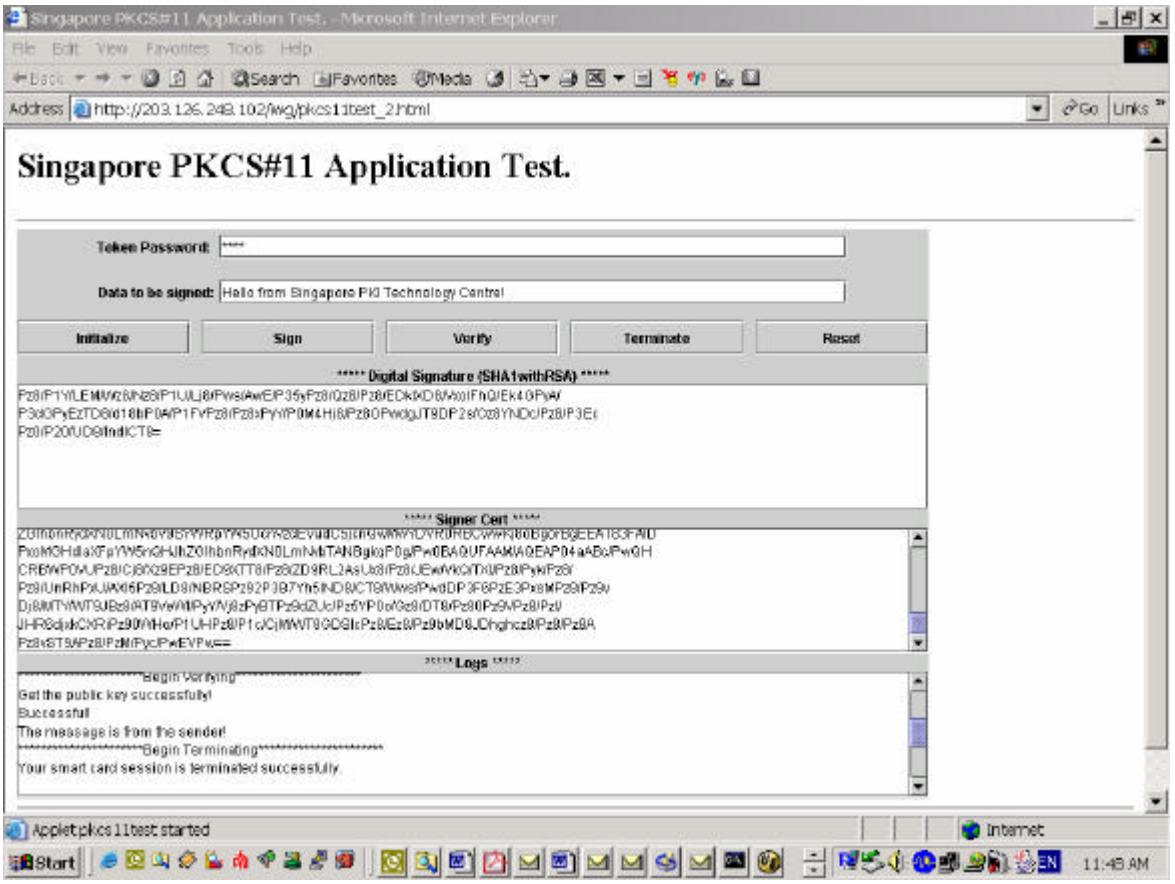


Figure 6: Terminate the Smart Card session

1.9 5. Reset the text area:

1. Click the "Reset" Button.
Expected Result is displayed in the Logs area (Appended after the precious result).
The three text areas on the screen viz. Digital Signature, Cert and Logs are cleared.

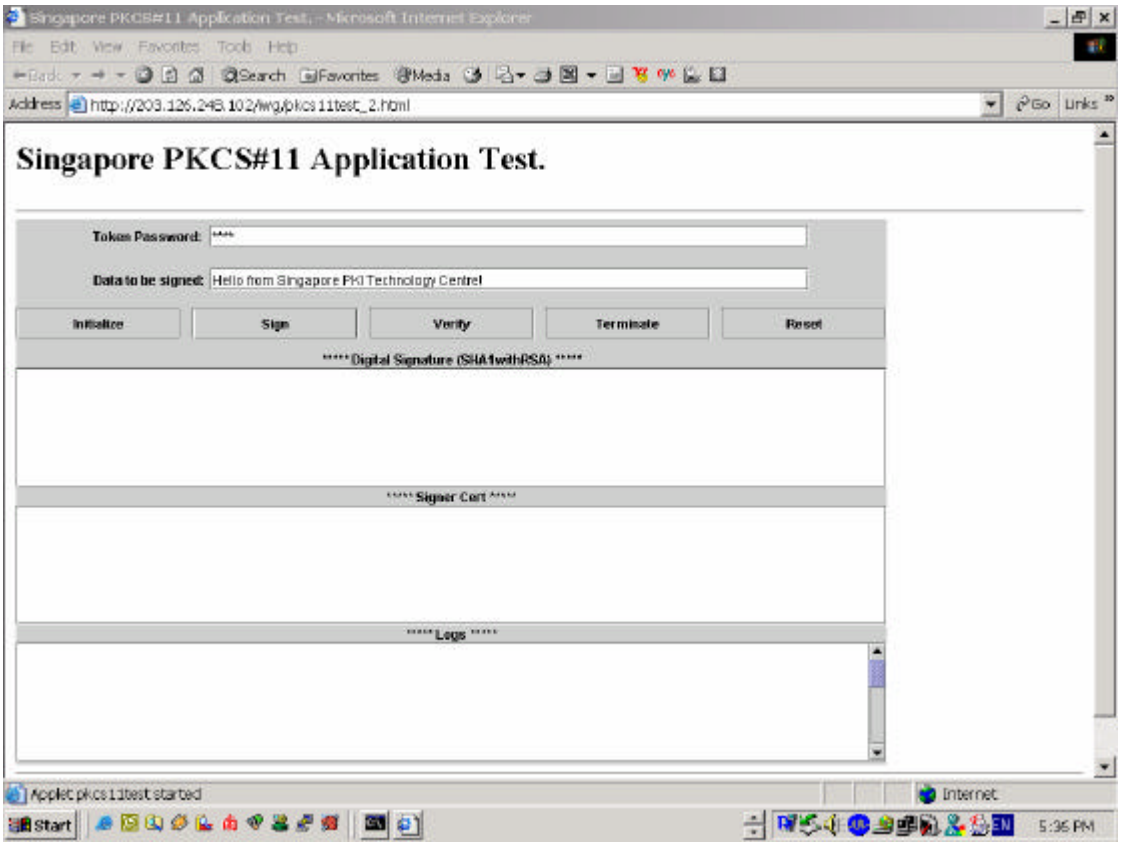


Figure 7: Reset the screen

4. Test Plan

Function	Normal Case (Expected Result)	Abnormal Case (Expected Result)
Initialize	On entering the correct token password, the user logs in to the smart card.	If incorrect password is entered or if the smart card is not inserted into the reader, the user cannot login to the smart card.
Sign	Get the private key object from the token. Sign the digest using the user's private key.	Cannot perform the sign operation
Verify	Get the Cert object from the token. Verify the signature using user's public key.	Cannot verify the signature
Terminate	Close the smart card session.	Cannot Terminate the smart card session.

5. Notes

1. If any errors, please let us know in which action you hit the error and what is the error message.

2. After you installed JRE 1.4.1, please make sure that the following IE setting is set (otherwise the applet can not be loaded correctly).
Click on Tools->Internet Options->Advanced to set the particular option.

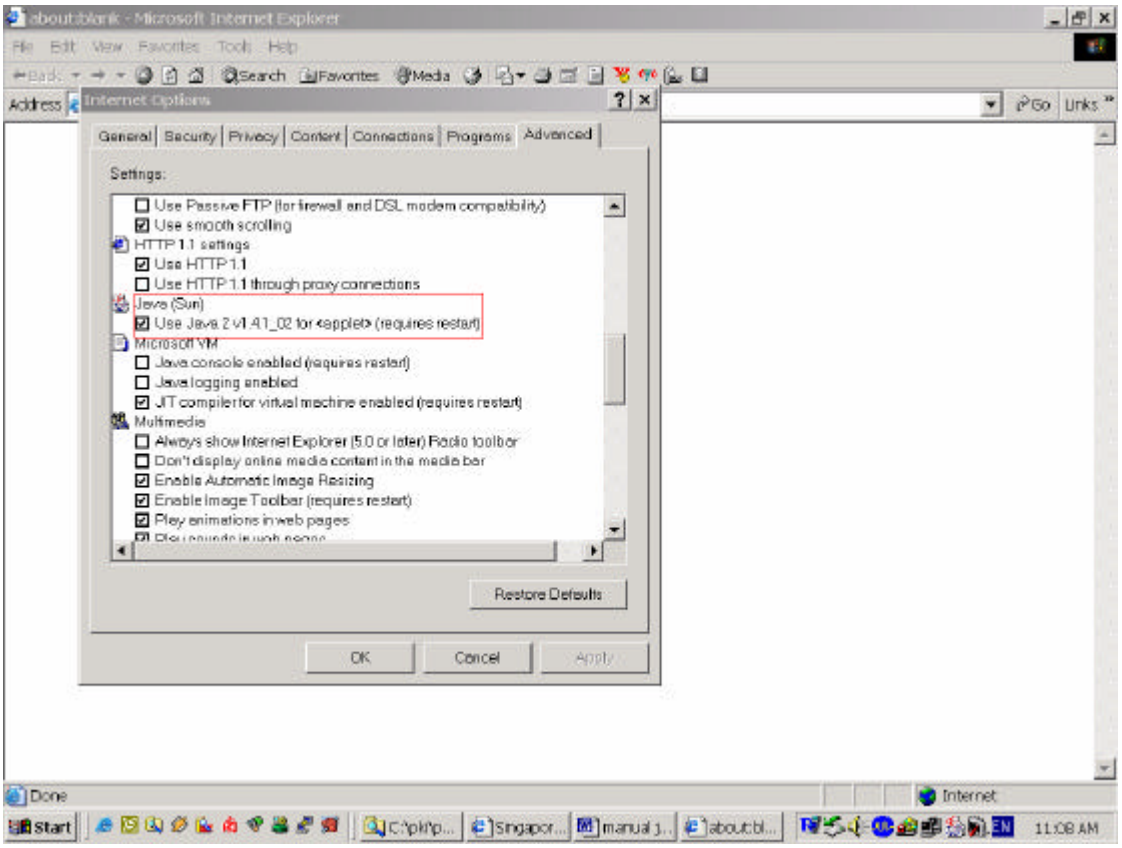


Figure 8: IE Configuration

1.10 Future Plans

- **Encryption/Decryption and Wrap/Unwrap.**
  IWG members agreed to include the Encryption/Decryption and the Wrap/Unwrap functions in the next phase of the PKCS#11 Interoperability test.

- **Multiple Slot APIs and Multiple Key.**
  IWG members in Korea are interested in including the concerned APIs and considering the multiple keys on one token in the next phase of the PKCS#11 experiment.

- **XML Signature & Encryption Message for E2E Security.**
  IWG members in Korea agree that it is necessary to have a standard message format for the XML Signature and Encryption. Since it is not yet determined between IWG members, Korea thinks it is better to consider as a future plan of the PKCS#11 Interoperability test.

- **PIN Code Change API**
  IWG members in Korea also raised a suggestion on whether there is really a need to include the function for PIN code change in the next phase of PKCS#11 interoperability test.

- **Integrity Issues and Certificate Path Processing API**
  IWG members in Korea believe that the current PKCS#11 application model can't be practical and applicable to the real businesses without addressing the integrity issues and the functions of certificate path processing.