



PRECISION
GROUP

www.precisionit.co.in

User Manual Document

InnaIT PKCS11

User Manual Document



Precision Biometric India Pvt Ltd



Version history

Version	Date	Author	Comment
1.0	01-04-2024	Rajabharath S	Initial Changes
1.1	06-05-2024	Rajabharath S	Key type/Algorithm included for create keypair
1.2	16-07-2024	Rajabharath S	Decryption functionality added, dll name changed from InnaITPKCS11.dll to InnaITPKCS11Driver.dll



Contents

Introduction	4
Driver Information	4
PKCS11 Supported Functions	4
List Slots.....	5
Change Owner hierarchy Password	6
Create Keypair.....	7
List Credentials	8
Sign	9
Decrypt	10
Delete Credential.....	11
Get PublicKey	12
Get Certificate	13
Set Certificate	14
Delete Certificate	15
Import KeyPair	16



Introduction

This document is intended to give the user a complete understanding about the TPM PKCS11 functionalities. This document includes procedure to test InnalT PKCS11 Crptographic provider through OpenSC pkcs11-tool. User can use any PKCS11 supported application to load InnalTPKCS11Driver.dll to access PKCS11 functions.

Driver Information

PKCS11 Provider Name : InnalT Cryptographic Provider

DLL Location : C:\Windows\system32 \InnalTPKCS11Driver.dll

PKCS11 Supported Functions

C_Initialize
C_Finalize
C_GetInfo
C_GetFunctionList
C_GetSlotList
C_GetSlotInfo
C_GetTokenInfo
C_WaitForSlotEvent
C_GetMechanismList
C_GetMechanismInfo
C_SetPIN
C_OpenSession
C_CloseSession
C_CloseAllSessions
C_GetSessionInfo
C_Login
C_Logout
C_CreateObject
C_DestroyObject
C_GetAttributeValue
C_FindObjectsInit
C_FindObjects
C_FindObjectsFinal
C_EncryptInit
C_Encrypt
C_DecryptInit
C_Decrypt
C_SignInit
C_Sign
C_GenerateKeyPair



List Slots

Command: -

`pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --list-slots`

```
C:\Windows\System32\cmd.exe
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --list-slots
Available slots:
Slot 0 (0x0): InnaIT Slot Info
  token label      : InnaITKey
  token manufacturer : Precision Biometric
  token model      : PK110X-DSC
  token flags      : login required, rng, token initialized, PIN initialized
  hardware version  : 1.0
  firmware version  : 1.3
  serial num       : IF3A34B8F4
  pin min/max      : 4/63
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>
```



Change Owner hierarchy Password

Command: - pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --change-pin --so-pin <Old owner hierarchy password> --new-pin <New owner hierarchy password>

```
C:\Windows\System32\cmd.exe
D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo1>pkcs11-tool.exe --module .\InnaITPKCS11.dll --change-pin --so-pin 39X8Mvy3#74W6 --new-pin 12345
Using slot 0 with a present token (0x0)
PIN successfully changed
D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo1>
```



Create Keypair

Command: -

RSA KeyPair: -

```
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --keypairgen --pin <pin for new keypair> --label <label for keypair> --key-type <Key algorithm>:<key bit size>
```

EC KeyPair: -

```
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --keypairgen --pin <pin for new keypair> --label <label for keypair> --key-type <Key algorithm>:<curve name>
```

Supported EC Curves:

- prime256v1
- secp256r1
- ansiX9p256r1
- prime384v1
- secp384r1
- ansiX9p384r1

```
C:\Windows\System32\cmd.exe

C:\Program Files (x86)\Precision Biometric\InnaIT\InnaITPKCS11Driver>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --keypairgen --pin 123456 label rsakey2048 --key-type RSA:2048
error: invalid option(s) given
Aborting.

C:\Program Files (x86)\Precision Biometric\InnaIT\InnaITPKCS11Driver>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --keypairgen --pin 123456 --label rsakey2048 --key-type RSA:2048
Using slot 0 with a present token (0x0)
Key pair generated:
Private Key Object; RSA
  label:    rsakey2048
  ID:      81000005
  Usage:    sign
  Access:   none
Public Key Object; RSA 2048 bits
  label:    public_rsakey2048
  ID:      05000081
  Usage:    none
  Access:   none

C:\Program Files (x86)\Precision Biometric\InnaIT\InnaITPKCS11Driver>
```



List Credentials

Command: -

`pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --list-objects --slot=0`

```
C:\Windows\System32\cmd.exe
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --list-objects --slot 0
Public Key Object; RSA 2048 bits
  label:    public_importrsakey
  ID:       04000081
  Usage:    encrypt
  Access:   none
Private Key Object; RSA
  label:    importrsakey
  ID:       81000004
  Usage:    decrypt, sign
  Access:   none
Certificate Object; type = X.509 cert
  label:    cert_genkey1
  ID:       03000081
Private Key Object; RSA
  label:    genkey1
  ID:       81000003
  Usage:    decrypt, sign
  Access:   none
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>
```




Sign

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --sign --slot 0 --id <ID of private key object> --mechanism SHA256-RSA-PKCS --signature-format=sequence --input-file <input file contains the data to sign> --output-file <output file to write the signature>

Mechanism for EC Key:

- ECDSA-SHA256

```
C:\Windows\System32\cmd.exe - pkcs11-tool.exe --module .\InnaITPKCS11.dll --sign --slot=0 --id="81000005" --mechanism=SHA256-RSA-PKCS --signature-format=sequence --input-file=.data_to_sign.txt -o .signed_data.txt

D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo\pkcs11-tool.exe --module .\InnaITPKCS11.dll -O
Using slot 0 with a present token (0x0)
Certificate Object; type = X.509 cert
Label: cert_cred7
ID: 05000081
Private Key Object; RSA
Label: cred7
ID: 81000005
Usage: none
Access: none
Certificate Object; type = X.509 cert
Label: cert_cred9
ID: 04000081
Private Key Object; RSA
Label: cred9
ID: 81000004
Usage: none
Access: none
Certificate Object; type = X.509 cert
Label: cert_cred5
ID: 03000081
Private Key Object; RSA
Label: cred5
ID: 81000003
Usage: none
Access: none

D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo\pkcs11-tool.exe --module .\InnaITPKCS11.dll --sign --slot=0 --id="81000005" --mechanism=SHA256-RSA-PKCS --signature-format=sequence --input-file=.data_to_sign.txt -o .signed_data.txt
Logging in to "InnaITKey".
Please enter User PIN:
```

Enter PIN of the credential

```
C:\Windows\System32\cmd.exe

D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo\pkcs11-tool.exe --module .\InnaITPKCS11.dll -O
Using slot 0 with a present token (0x0)
Certificate Object; type = X.509 cert
Label: cert_cred7
ID: 05000081
Private Key Object; RSA
Label: cred7
ID: 81000005
Usage: none
Access: none
Certificate Object; type = X.509 cert
Label: cert_cred9
ID: 04000081
Private Key Object; RSA
Label: cred9
ID: 81000004
Usage: none
Access: none
Certificate Object; type = X.509 cert
Label: cert_cred5
ID: 03000081
Private Key Object; RSA
Label: cred5
ID: 81000003
Usage: none
Access: none

D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo\pkcs11-tool.exe --module .\InnaITPKCS11.dll --sign --slot=0 --id="81000005" --mechanism=SHA256-RSA-PKCS --signature-format=sequence --input-file=.data_to_sign.txt -o .signed_data.txt
Logging in to "InnaITKey".
Please enter User PIN: Using signature algorithm SHA256-RSA-PKCS

D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo\>
```



Decrypt

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --decrypt --slot 0 --id <ID of private key object> --mechanism RSA-PKCS --input-file=<input file contains the encrypted data> --output-file <output file to write the decrypted data>

```
C:\Windows\System32\cmd.exe

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll -0
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
  label:    public_Key1
  ID:       03000081
  Usage:    encrypt
  Access:   none
Private Key Object; RSA
  label:    Key1
  ID:       81000003
  Usage:    decrypt, sign
  Access:   none

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --decrypt --slot=0 --pin="1234" --id="81000003" --mechanism=RSA-PKCS --input-file=data_to_encrypt.txt -o encryptedData.txt
```



Delete Credential

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --delete-object --type privkey --id <id of private key object to delete> --login --login-type so --so-pin <Owner hierarchy password>

```
C:\Windows\System32\cmd.exe

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll -0
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
Label:      public_rsakey1
ID:         04000001
Usage:      encrypt
Access:     none
Private Key Object; RSA
Label:      rsakey1
ID:         81000004
Usage:      decrypt, sign
Access:     none
Public Key Object; RSA 2048 bits
Label:      public_rsakey1
ID:         03000001
Usage:      encrypt
Access:     none
Private Key Object; RSA
Label:      rsakey1
ID:         81000003
Usage:      decrypt, sign
Access:     none

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --delete-object --type privkey --id 81000003 --login --login-type so --so-pin Password123
Using slot 0 with a present token (0x0)

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll -0
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
Label:      public_rsakey1
ID:         04000001
Usage:      encrypt
Access:     none
Private Key Object; RSA
Label:      rsakey1
ID:         81000004
Usage:      decrypt, sign
Access:     none

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>
```



Get PublicKey

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --read-object --type pubkey --id <id of public key object to read> --output-file <path for the public key to write>

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

D:\Projects\OpenSource\openssl\openssl-1.1.0f-vs2017\bin>openssl rsa -pubin -in pubkey.key -inform DER -outform PEM -out
pubkey.pem
writing RSA key

D:\Projects\OpenSource\openssl\openssl-1.1.0f-vs2017\bin>
```



Get Certificate

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --read-object --type cert --id <id of certificate object to read> --output-file <path for the read certificate to write>

```
C:\Windows\System32\cmd.exe
D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo1>pkcs11-tool.exe --module .\InnaITPKCS11.dll --read-object --type cert --label=cert_cred8 -o .\cert_cred8.der
Using slot 0 with a present token (0x0)
D:\Projects\InnaITKey\gitstore\tools\3.5\CCA_Demo1>
```



Set Certificate

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --write-object <path of the certificate to write> --type cert --id <ID of the private key object for which certificate need to set> --label <label for certificate(optional)> --login --login-type so --so-pin <Owner hierarchy password>

```
C:\Windows\System32\cmd.exe

d:\CCA_Demo>pkcs11-tool.exe --module InnaITPKCS11\InnaITPKCS11.dll -0
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
label:
ID:      05000081
Usage:   none
Access:  none

d:\CCA_Demo>pkcs11-tool.exe --module InnaITPKCS11\InnaITPKCS11.dll --write-object cert_to_write.cer --type cert --id 81000005
Using slot 0 with a present token (0x0)
Created certificate:
Certificate Object; type = X.509 cert
label:
ID:      81000005

d:\CCA_Demo>
```



Delete Certificate

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --delete-object --type cert --id <id of certificate object to delete> --login --login-type so --so-pin <Owner hierarchy password>

```
C:\Windows\System32\cmd.exe

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11.d
ll -o
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
  label:      Signing_Key_04
  ID:         81000004
  Usage:      none
  Access:     none
Certificate Object; type = X.509 cert
  label:      cert_Signing_Key_03
  ID:         03000081
Public Key Object; RSA 2048 bits
  label:      Signing_Key_03
  ID:         81000003
  Usage:      none
  Access:     none

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11.d
ll --delete-object --type cert --label="cert_Signing_Key_03"
Using slot 0 with a present token (0x0)

D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>
```



Import KeyPair

Command: -

pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --write-object <path of the Private key to write> --type privkey --label <label for keypair> --pin <pin for the keypair importing>

A screenshot of a Windows command prompt window. The title bar shows "C:\Windows\System32\cmd.exe". The command entered is: `D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --write-object private.key --type privkey --label importrsa2048 --pin 12345`. The output shows: `Using slot 0 with a present token (0x0)`. The prompt then returns to the same directory.

```
C:\Windows\System32\cmd.exe
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>pkcs11-tool.exe --module InnaITPKCS11Driver.dll --write-object private.key --type privkey --label importrsa2048 --pin 12345
Using slot 0 with a present token (0x0)
D:\Projects\InnaITKey\gitstore\tools\3.5\innait-pkcs11-interface\src\x64\Release>
```