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 InnaIT PKCS11 Crptographic provider through OpenSC pkcs11-tool. User can use any PKCS11 supported application to load InnaITPKCS11Driver.dll to access PKCS11 functions.

Driver Information

PKCS11 Provider Name : InnaIT Cryptographic Provider

DLL Location : C:\Windows\system32 \InnaITPKCS11Driver.dll

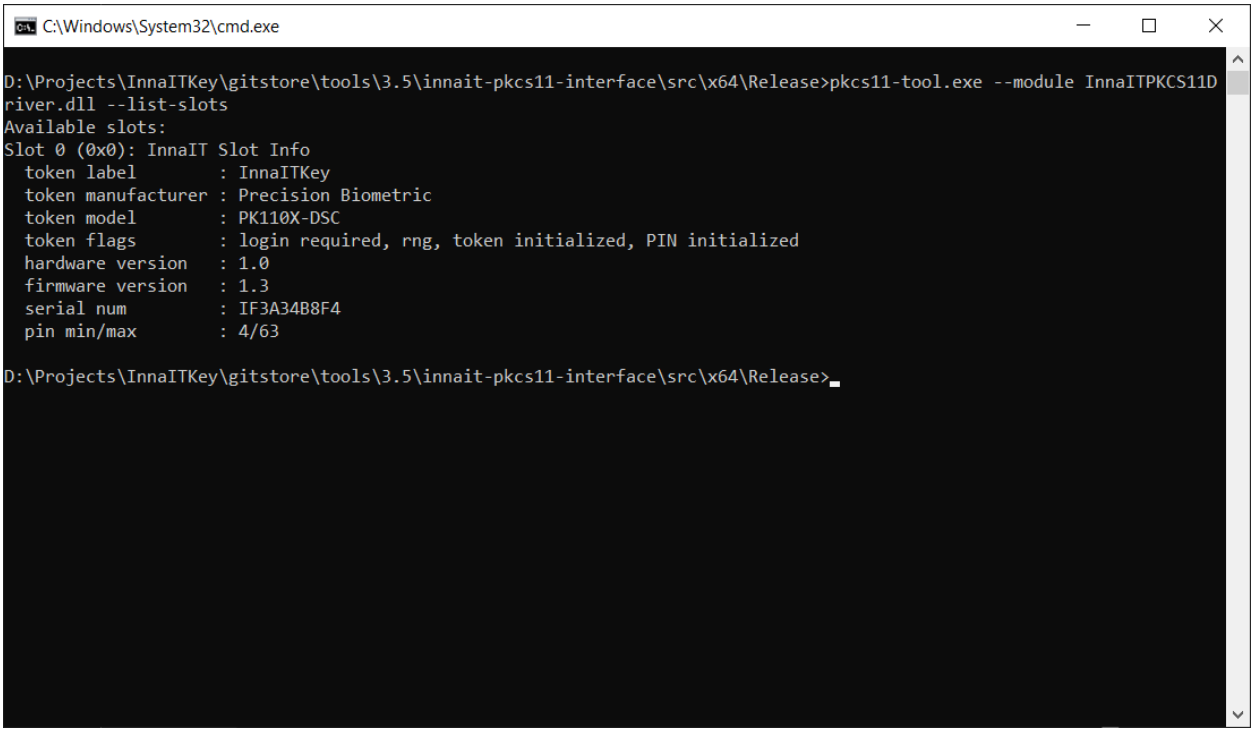
PKCS11 Supported Functions

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

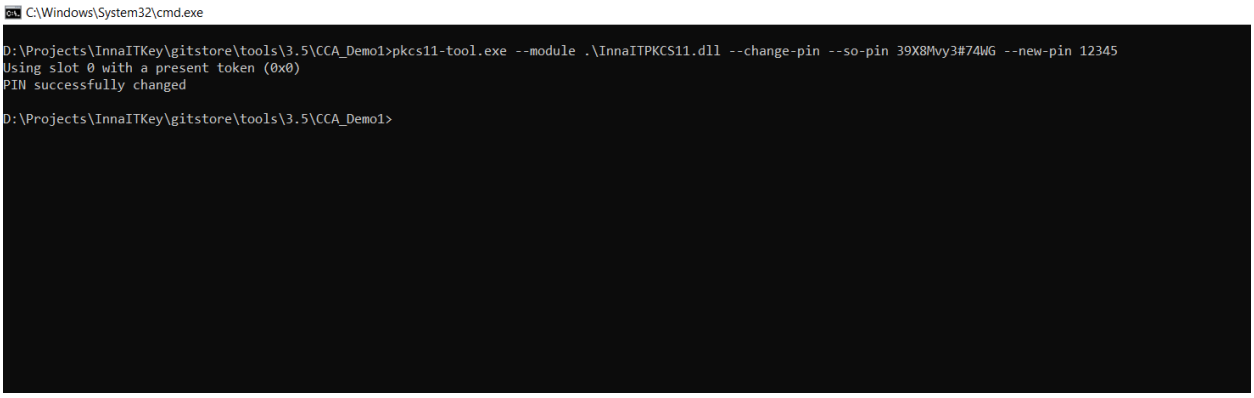
Command: -

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



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>



Create Keypair

Command: -

RSA KeyPair: -

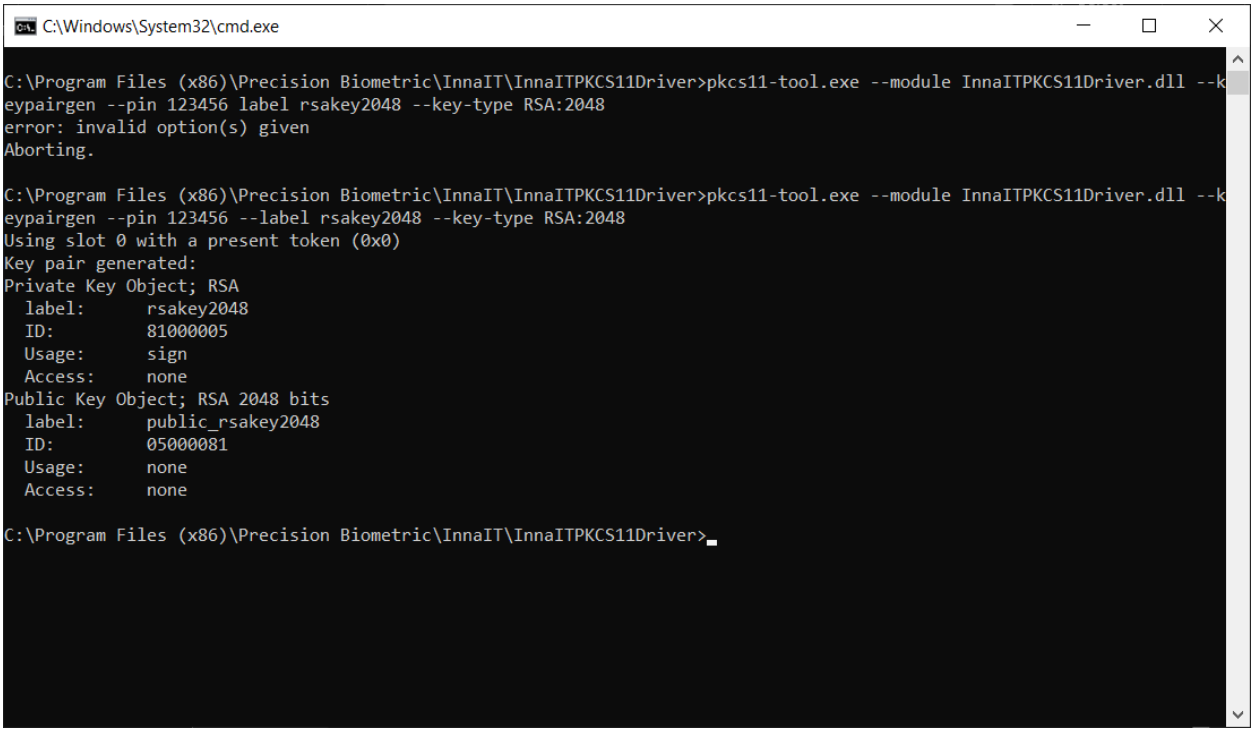
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --keypairgen --pin <pin for new keypair> --label <label for keypair> --key-type <Key algorithm>:<key bit size>

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:

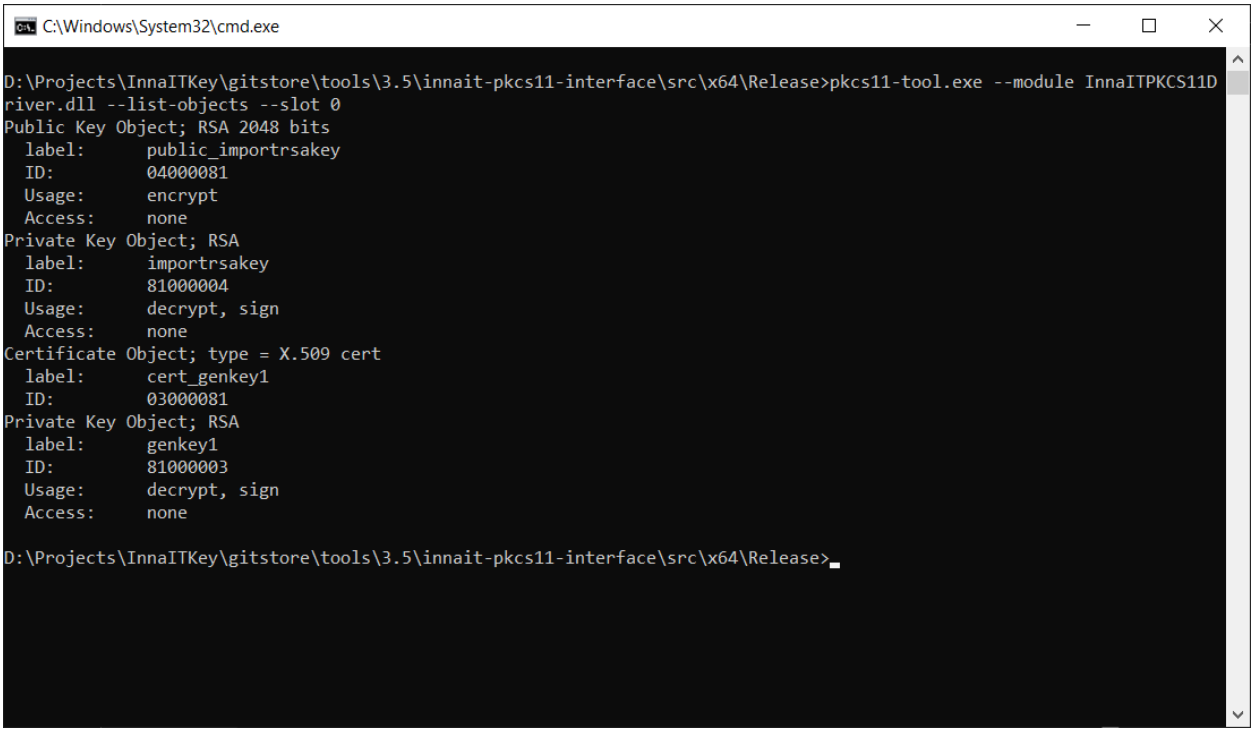
- prime256v1
- secp256r1
- ansiX9p256r1
- prime384v1
- secp384r1
- ansiX9p384r1



List Credentials

Command: -

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



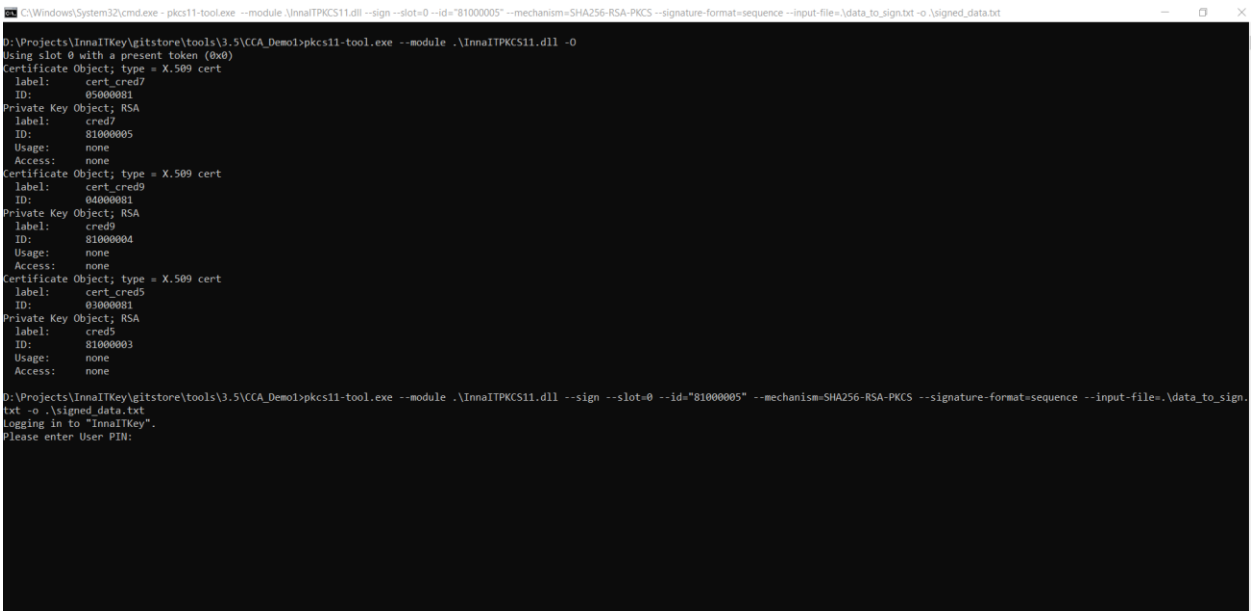
Sign

Command: -

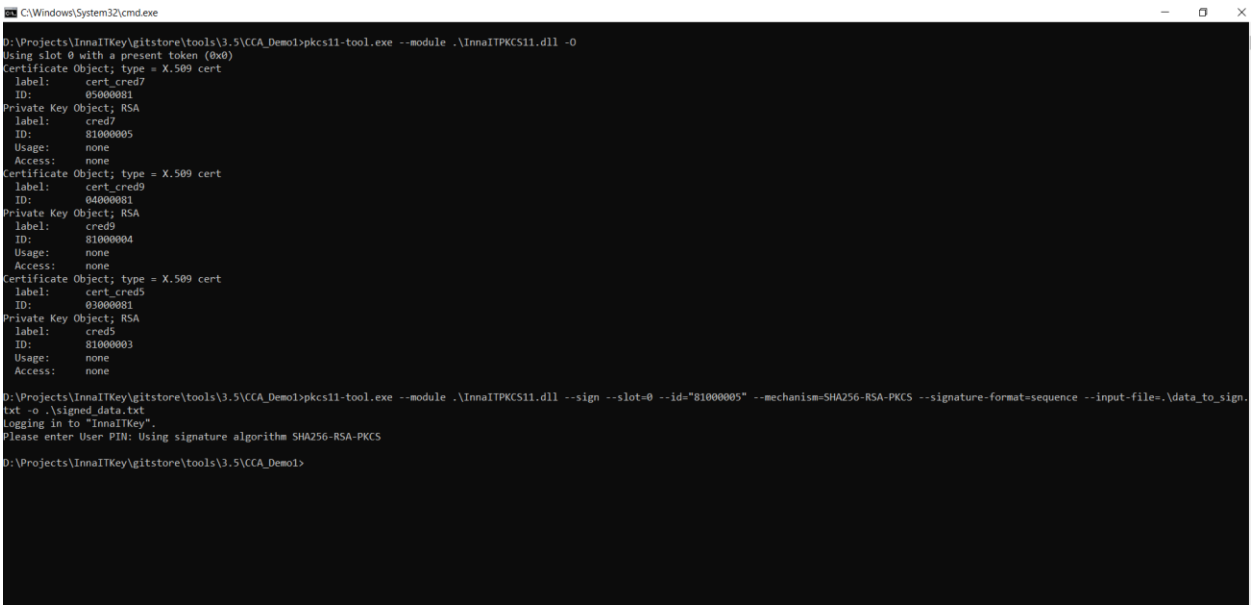
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --sign --slot 0 --id <ID of private key object> --mechanism SHA256-RSA-PKCS --signature-format=sequence --input-file <input file contains the data to sign> --output-file <output file to write the signature>

Mechanism for EC Key:

- ECDSA-SHA256



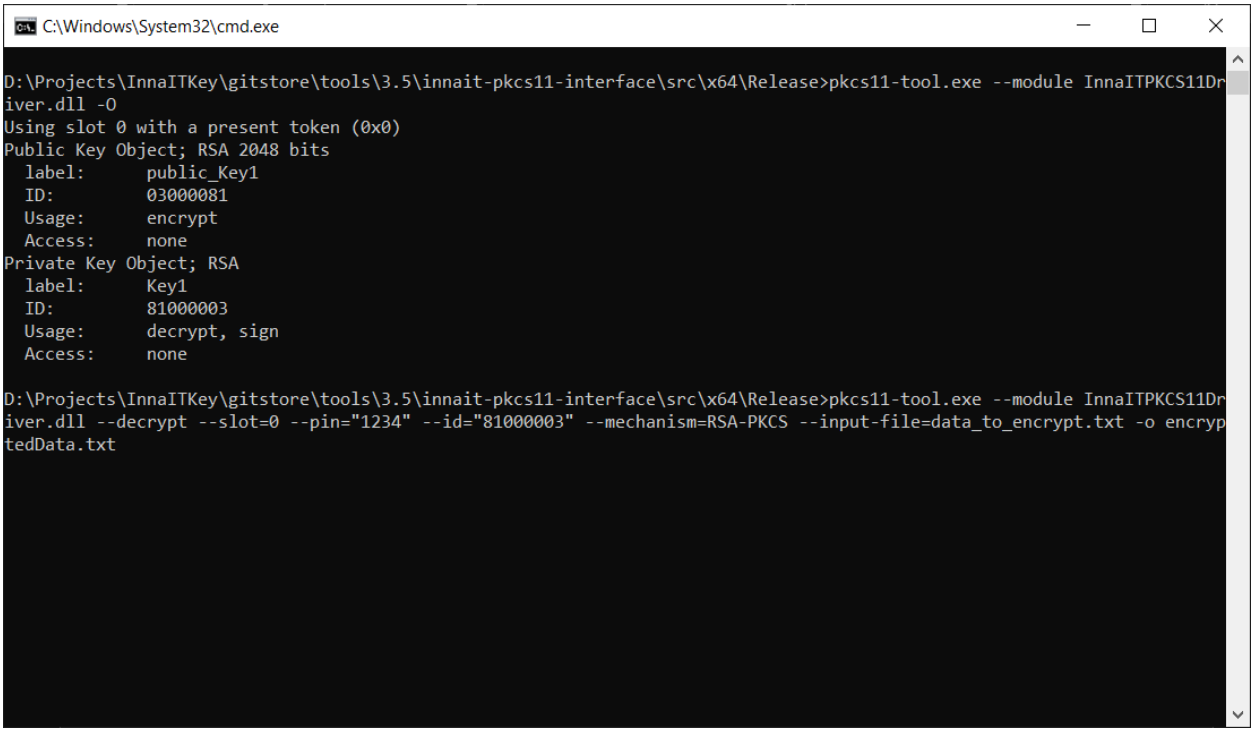
Enter PIN of the credential



Decrypt

Command: -

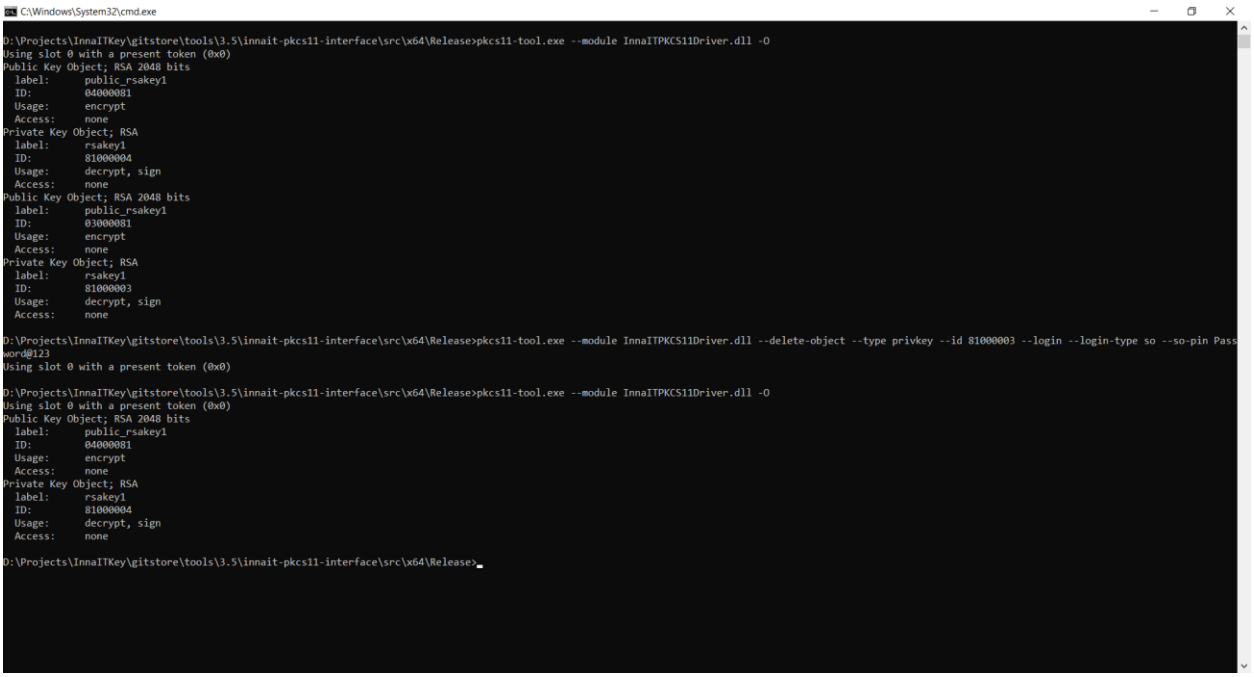
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --decrypt --slot 0 --id <ID of private key object> --mechanism RSA-PKCS --input-file=<input file contains the encrypted data> --output-file <output file to write the decrypted data>



Delete Credential

Command: -

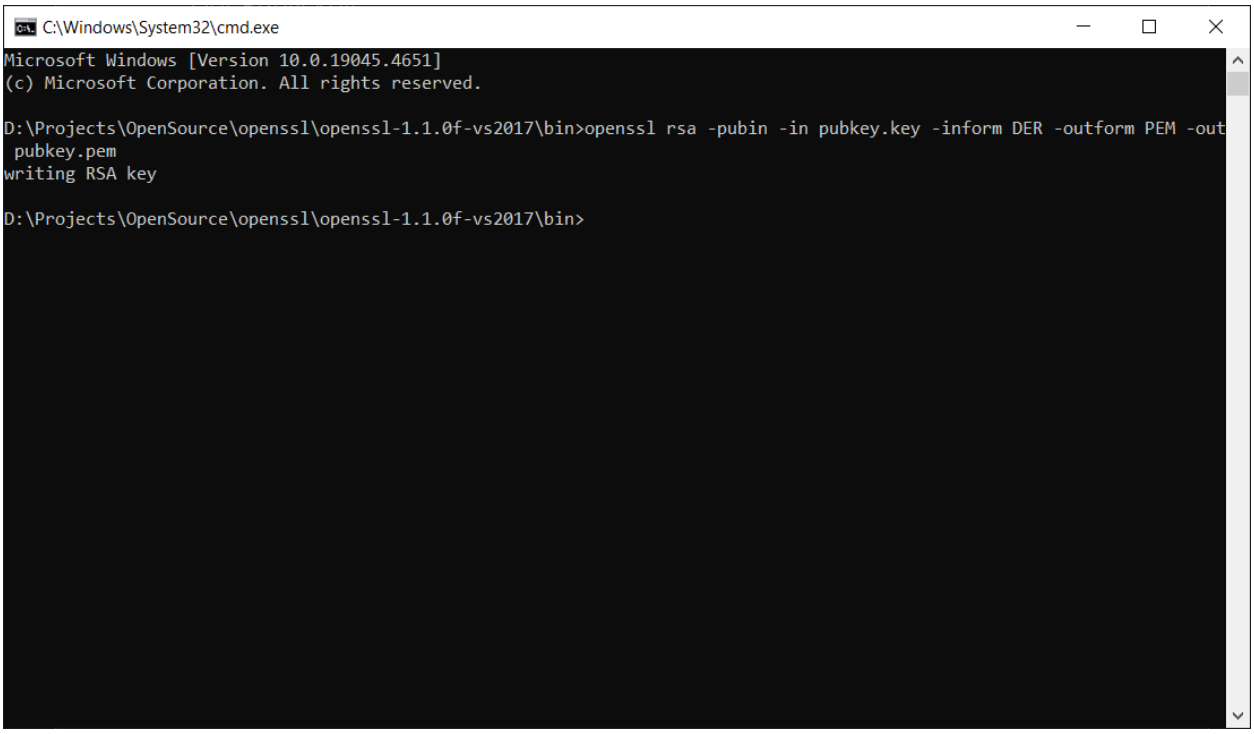
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --delete-object --type privkey --id <id of private key object to delete> --login --login-type so --so-pin <Owner hierarchy password>



Get PublicKey

Command: -

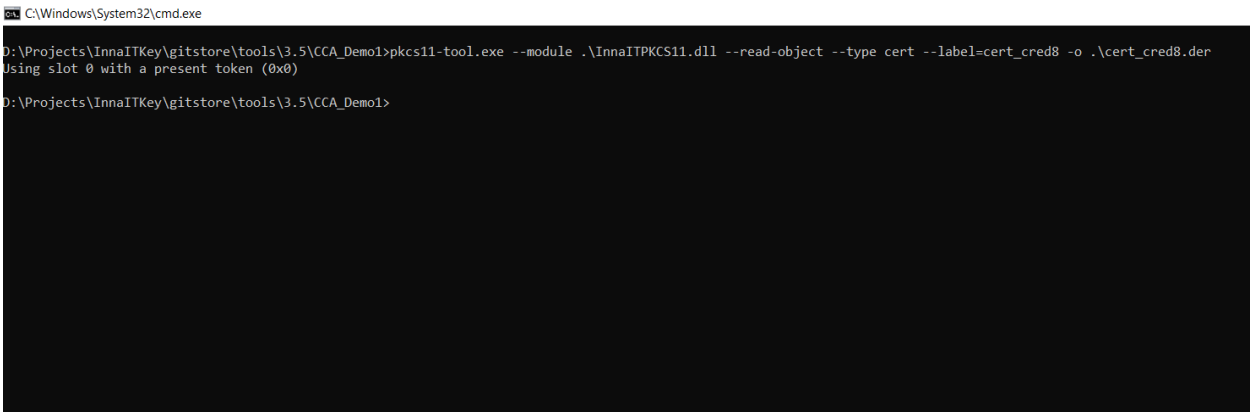
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --read-object --type pubkey --id <id of public key object to read> --output-file <path for the public key to write>



Get Certificate

Command: -

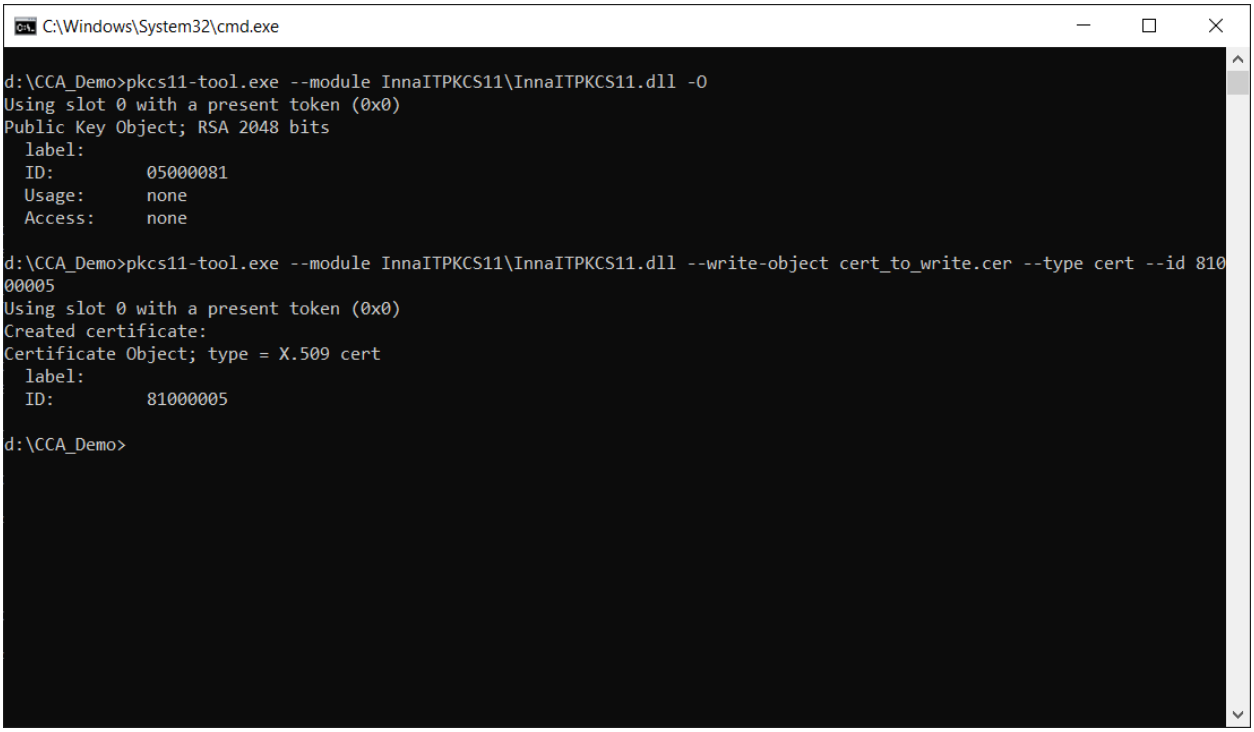
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --read-object --type cert --id <id of certificate object to read> --output-file <path for the read certificate to write>



Set Certificate

Command: -

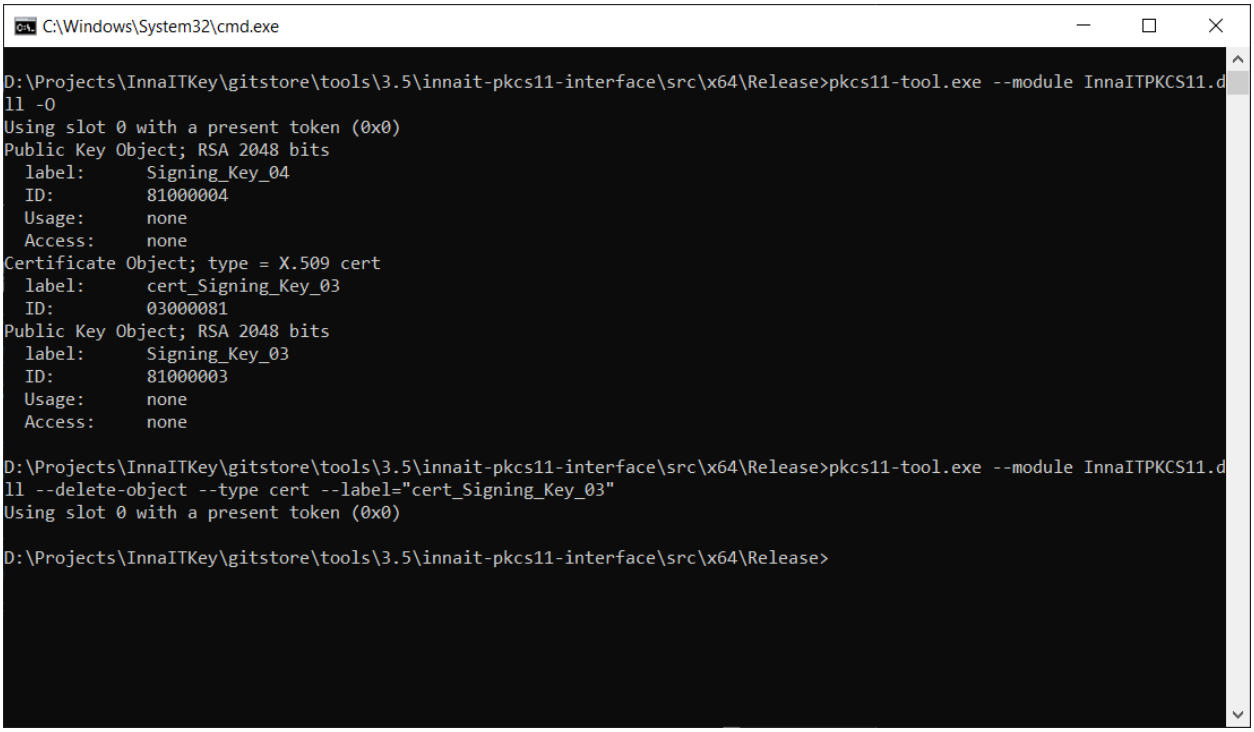
pkcs11-tool.exe --module <path of InnaITPKCS11Driver.dll> --write-object <path of the certificate to write> --type cert --id <ID of the private key object for which certificate need to set> --label <label for certificate(optional)> --login --login-type so --so-pin <Owner hierarchy password>



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>



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>