

PKI Application for MULTOS Data Sheet

[SIM-MK-0001 Rev 1.0 10Dec01]

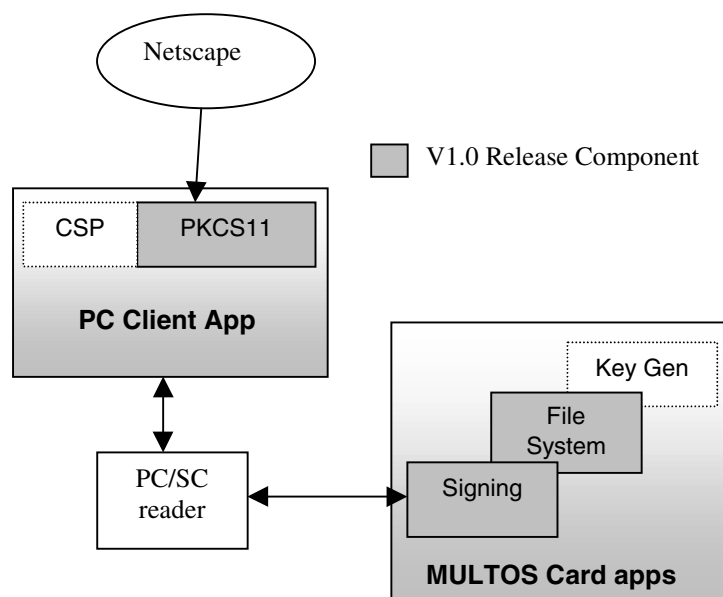
The Keycorp PKI for MULTOS product, V1.0 comprise of a set of MULTOS applications and Windows interface library components to implement a Netscape-compatible cryptographic token that will allow :

- storage of certificates issued from Certification Authority web-sites;
- secure E-mail communication (sign & encrypt);
- secure web-site access.

The Windows interface library components provide a single session PKCS#11 API which has been implemented to the PKCS#11 V2.10 standard. They interwork specifically with the Keycorp PKI card applications via a PC/SC layer provided by the Windows platform. The Windows interface library components are available as an installation package.

The MULTOS applications, Signing and File System , in their generic form, are capable of supporting storage of 2 Private/Public key pairs, 2 certificates and user Data Objects. The applications¹ support random number generation, signing and decryption with key sizes 512, 768 and 1024 bits.

The smartcard interface, implemented by the MULTOS applications, presents a WIM/PKCS15 command and information model structure.



PC Client App, PKCS#11 Interface

Files asn1.dll – ASN.1 encode/decode library,
 kcpkcs11.dll – PKCS#11 interface library,
 SmartCom.exe – card app interface component.

¹ On-card key generation is the subject of a third application which is not included in this release.

The PKCS#11 API has been implemented to PKCS#11 V2.10, “Cryptographic Token Interface Standard, RSA Laboratories (<http://www.rsasecurity.com/rsalibas/pkcs/>) and the following table details the level of support.

Function	Status
C_Initialize	Supported (pInitArgs must be NULL_PTR, current implementation does not support multi-thread)
C_Finalize	Supported
C_GetInfo	Supported
C_GetFunctionList	Supported
C_GetSlotList	Supported
C_GetSlotInfo	Supported
C_GetTokenInfo	Supported
C_WaitForSlotEvent	Returns CKR_FUNCTION_NOT_SUPPORTED
C_GetMechanismList	Supported
C_GetMechanismInfo	Supported
C_InitToken	Dummy function, returns CKR_OK but does not actually initialise; CardInit tool is used for initialisation.
C_InitPIN	Returns CKR_FUNCTION_NOT_SUPPORTED; PINs are initialised on MULTOS card application load, defaults to “1234”.
C_SetPIN	Supported
C_OpenSession	Supported; single session only
C_CloseSession	Supported
C_CloseAllSessions	Supported
C_GetSessionInfo	Supported
C_GetOperationState	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SetOperationState	Returns CKR_FUNCTION_NOT_SUPPORTED
C_Login	Supported
C_Logout	Supported
C_CreateObject	Supported
C_CopyObject	Supported
C_DestroyObject	Supported
C_GetObjectSize	Returns CKR_FUNCTION_NOT_SUPPORTED
C_GetAttributeValue	Supported
C_SetAttributeValue	Supported
C_FindObjectsInit	Supported
C_FindObjects	Supported
C_FindObjectsFinal	Supported
C_EncryptInit	Returns CKR_FUNCTION_NOT_SUPPORTED
C_Encrypt	Returns CKR_FUNCTION_NOT_SUPPORTED
C_EncryptUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_EncryptFinal	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DecryptInit	Supported
C_Decrypt	Supported
C_DecryptUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DecryptFinal	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DigestInit	Returns CKR_FUNCTION_NOT_SUPPORTED
C_Digest	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DigestUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DigestKey	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DigestFinal	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SignInit	Supported
C_Sign	Supported
C_SignUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SignFinal	Returns CKR_FUNCTION_NOT_SUPPORTED

C_SignRecoverInit	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SignRecover	Returns CKR_FUNCTION_NOT_SUPPORTED
C_VerifyInit	Supported
C_Verify	Supported
C_VerifyUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_VerifyFinal	Returns CKR_FUNCTION_NOT_SUPPORTED
C_VerifyRecoverInit	Returns CKR_FUNCTION_NOT_SUPPORTED
C_VerifyRecover	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DigestEncryptUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DecryptDigestUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SignEncryptUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DecryptVerifyUpdate	Returns CKR_FUNCTION_NOT_SUPPORTED
C_GenerateKey	Returns CKR_FUNCTION_NOT_SUPPORTED
C_GenerateKeyPair	Supported, returns CKR_MECHANISM_INVALID if card does not support key generation.
C_WrapKey	Returns CKR_FUNCTION_NOT_SUPPORTED
C_UnwrapKey	Returns CKR_FUNCTION_NOT_SUPPORTED
C_DeriveKey	Returns CKR_FUNCTION_NOT_SUPPORTED
C_SeedRandom	Returns CKR_FUNCTION_NOT_SUPPORTED
C_GenerateRandom	Supported
C_GetFunctionStatus	Supported
C_CancelFunction	Supported

MULTOS Card Applications

AID a000000063504b43532d3135 *(This is the AID for the Sign App which will delegate file system commands to the File App, selecting this AID will be sufficient to interact with the suite of PKI-related applications)*

Card Commands

Card commands are defined by Keycorp specification SIM-SP-0130, “PKI Application for MULTOS WIM Application Interface Specification”.

Command	Status
VERIFY	Supported
CHANGE REFERENCE DATA	Supported
RESET RETRY COUNTER	Supported
CREATE EF	Supported
SELECT (FILE)	Supported
SELECT (APPLICATION)	Supported
READ BINARY	Supported
UPDATE BINARY	Supported
MSE-RESTORE	Supported (dummy command processing only)
MSE-SET	Supported
PSO-DECRYPT	Supported
PSO-COMPUTE DIGITAL SIGNATURE	Supported
PSO-GENERATE RSA KEY	Not supported
PSO-READ RSA MODULUS	Supported
ASK RANDOM	Supported
GET RESPONSE	Supported

Application sizes

“Full” refers to the application not using the PKI mask codelets, and “Stub” refers to applications utilising codelets (1Q).

Application	Session Data	EEPROM requirement
File App (Full)	17	14277
File App (Stub)	17	11371
Sign App (Full)	7	5388
Sign App (Stub)	7	3027

Elementary Files :

File ID	Name	Size (bytes)	Access Conditions
5031	EF _{ODF} – Object Directory File	256	Read ALW Update SO
5032	EF _{TokenInfo} – Token Information File	256	Read ALW Update SO
5204	EF _{AODF} – Authentication Object Directory File	256	Read ALW Update SOIUSER
5200	EF _{PrKDF} – Private Key Directory File	256	Read ALW Update SOIUSER
6100	EF _{PrRSA1} – Private RSA Key File 1	322	Read NEV Update USER
6101	EF _{PrRSA2} – Private RSA Key File 2	322	Read NEV Update USER
5201	EF _{PuKDF} – Public Key Directory File	256	Read ALW Update SOIUSER
6000	EF _{PuRSA1} – Public RSA Key File 1	256	Read ALW Update SOIUSER
6001	EF _{PuRSA2} – Public RSA Key File 2	256	Read ALW Update SOIUSER
5202	EF _{CDF} – Certificate Directory File	256	Read ALW Update SOIUSER
5302	EF _{Cert1} – Certificate File 1	1536	Read ALW Update SOIUSER
5303	EF _{Cert2} – Certificate File 2	1536	Read ALW Update SOIUSER
6F20	EF _{DODF} – Data Objects Directory File	1024	Read ALW Update USER
6F01	EF _{DO} – Data Objects File	4096	Read ALW Update USER

Tools

CardInit A command line tool to initialise card file content for interoperation with Client App.