

PKI Smartcard

Combining high security technologies to produce the leading security token



51582909080 80 850 025 132 087890513218 0856464 545158290908 80 850 025 132 087890513218 2
7890513218 0856464 5451582909080 80 850 025 132 087890513218 2
68247829090380 850 0025 132 087890513218 0856464 545158290

Keycorp is a leader in providing e-commerce solutions with the Nobil Internet payment gateway platform. The biggest challenge to business-to-business transactions is establishing a trusted platform for high value transactions in the public space of the Internet. Some key elements are required to build this platform: security, authentication and confidentiality.

With Keycorp's world leadership in smartcard platforms, we now offer a complete smartcard PKI solution.

PKI (Public Key Infrastructure) is the technology of choice for securing electronic commerce, and smartcards are the obvious tool for security tokens.

Standard interfaces are used throughout the design to ensure interoperability with other solutions:

- Microsoft CryptoAPI for the cryptography interface from the supplied software to applications such as Microsoft Internet Explorer
- PKCS#11 V2.10 for the cryptography interface from the supplied DLL to applications such as Netscape and Baltimore UniCERT
- PKCS#15, ISO7816-4 file system for interfacing to the smartcard application certificates stored in standard X.509 V3 format
- WAP WIM interface to smartcard cryptographic services.

Keycorp's MULTOS card, (with its highly secure ITSEC E6 classification), ensures maximum security for private keys from other applications and external examination.

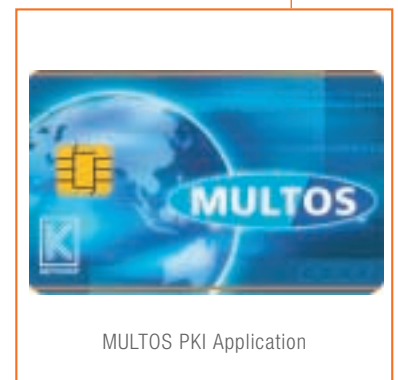
KEY FEATURES PKI

- based on Keycorp's ITSEC E6 certified MULTOS card
- 512 to 1024 bit RSA key lengths
- private storage space for two private keys
- public storage space for two X.509 V3 certificates and other data
- RSA and DES resistant to cryptographic attacks
- PIN/password access control
- on-card key generation
- PC/SC card reader interface

Technical Specifications

Keycorp/PKI supports the following PKCS#11 V2.10:

Category	Function	Description
General purpose	C_Initialize	initializes Cryptoki
	C_Finalize	clean up miscellaneous Cryptoki-associated resources
	C_GetInfo	obtains general information about Cryptoki
	C_GetFunctionList	obtains entry points of Cryptoki library functions
Slot and token management	C_GetSlotList	obtains a list of slots in the system
	C_GetSlotInfo	obtains information about a particular slot
	C_GetTokenInfo	obtains information about a particular token
	C_GetMechanismList	obtains a list of mechanisms supported by a token
	C_GetMechanismInfo	obtains information about a particular mechanism
	C_SetPIN	modifies the PIN of the current user
Session management	C_OpenSession	opens a connection between an application and a particular token
	C_CloseSession	closes a session
	C_CloseAllSessions	closes all sessions with a token
	C_GetSessionInfo	obtains information about the session
	C_Login	logs into a token
	C_Logout	logs out from a token
Object management	C_CreateObject	creates an object
	C_CopyObject	creates a copy of an object
	C_DestroyObject	destroys an object
	C_GetAttributeValue	obtains an attribute value of an object
	C_SetAttributeValue	modifies an attribute value of an object
	C_FindObjectsInit	initializes an object search operation
	C_FindObjects	continues an object search operation
	C_FindObjectsFinal	finishes an object search operation
Decryption	C_DeCryptInit	initializes a decryption operation
	C_DeCrypt	decrypts single-part encrypted data
Signing and MACing	C_SignInit	initializes a signature operation
	C_Sign	signs single-part data
Key management	C_GenerateKeyPair	generates a public-key/private-key pair



Keycorp Limited

Level 5, 799 Pacific Highway Chatswood
NSW 2067 SYDNEY Australia

Tel +61 2 9414 5200 Fax +61 2 9415 1363

Email: info@keycorp.net www.keycorp.net