

PKCS#11 MANUAL

VERSION 1.0

The data and information contained in this document cannot be altered without the express written permission of SecuTech Solution Inc. No part of this document can be reproduced or transmitted for any purpose whatsoever, either by electronic or mechanical means.

The general terms of trade of SecuTech Solution Inc. apply. Diverging agreements must be made in writing.

Copyright © SecuTech Solution Inc. All rights reserved.

WINDOWS is a registered trademark of Microsoft Corporation.

The WINDOWS-logo is a registered trademark ^(TM) of Microsoft Corporation.

Software License

The software and the enclosed documentation are copyright-protected. By installing the software, you agree to the conditions of the licensing agreement.

Licensing Agreement

SecuTech Solution Inc. (SecuTech for short) gives the buyer the simple, exclusive and non-transferable licensing right to use the software on one individual computer or networked computer system (LAN). Copying and any other form of reproduction of the software in full or in part as well as mixing and linking it with others is prohibited. The buyer is authorized to make one single copy of the software as backup. SecuTech reserves the right to change or improve the software without notice or to replace it with a new development. SecuTech is not obliged to inform the buyer of changes, improvements or new developments or to make these available to him. A legally binding promise of certain qualities is not given. SecuTech is not responsible for damage unless it is the result of deliberate action or negligence on the part of SecuTech or its aids and assistants. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

Contact Information

HTTP: www.eSecuTech.com

E-Mail: Sales@eSecuTech.com

Please Email any comments, suggestions or questions regarding this document or our products to us at: Sales@eSecuTech.com

Version	Date
1.0	2015.7

CE Attestation of Conformity



UniMate is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. UniMate satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment.

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



The equipment of UniMate is USB based.

Conformity to ISO 9001:2000



The Quality System of SecuTech Solution Inc., including its implementation, meets the requirements of the standard ISO 9001:2000

ROHS



All UniMate products are environmental friendly with ROHS certificates.

Table of Contents

INTRODUCTION	1
SUPPORTED PKCS#11 ALGORITHMS AND API	2
UNIMATE PKCS#11 FUNCTION LIBRARY	3
SAMPLES	5

Introduction

PKCS#11 is a Public-Key Cryptography Standard (PKCS) for public key cryptography, developed by RSA Laboratories and includes both algorithm-specific and algorithm-independent implementation standards. It is an industry standard that defines a technology independent programming interface for cryptographic devices such as smartcards and PCMCIA cards. This standard specifies an application program interface (API), called Cryptoki (Cryptographic Token Interface), to devices, either physical or virtual, which hold cryptographic information (keys and other data) and perform cryptographic functions. This API is used across many platforms and is powerful enough for most security-related applications. SecuTech uses PKCS#11 as the main API for UniMate programming. UniMate supports PKCS#11 application via UniMate middleware.

The following files are needed when developing the UniMate PKCS#11 applications.

Files	Path
Cryptpki.h	Provided by RSA
pkcs11.h	Provided by RSA
Pkcs11f.h	Provided by RSA
Pkcs11t.h	Provided by RSA
UniMateP11.dll	C:\Windows\system32\

PKCS#11 module of UniMate supports the creation of the following objects:

Object Class	Description
CKO_DATA	For data structures defined by application
CKO_SECRET_KEY	For symmetric keys
CKO_CERTIFICATE	For X.509 v3 certificates
CKO_PUBLIC_KEY	For RSA/DSA public key
CKO_PRIVATE_KEY	For RSA/DSA private key All

All the objects listed in the above table can be created with UniMate. The secure storage in UniMate is limited, so objects can only be created in memory but can NOT be stored in the UniMate secure storage. Only encryption keys and permanently present data need to be saved in the UniMate.

Supported PKCS#11 Algorithms and API

Mechanisms	Encrypt / Decrypt	Sign / Verify	Digest	Generate key/pair
CKM_RSA_PKCS_KEY_PAIR_GEN				✓
CKM_RSA_PKCS	✓	✓		
CKM_DSA_KEY_PAIR_GEN				
CKM_DSA				
CKM_RC2_KEY_GEN				
CKM_RC2_ECB				
CKM_RC2_CBC				
CKM_RC2_CBC_PAD				
CKM_RC4_KEY_GEN				
CKM_RC4				
CKM_DES_KEY_GEN				✓
CKM_DES_ECB	✓			
CKM_DES_CBC	✓			
CKM_DES3_KEY_GEN				✓
CKM_DES3_ECB	✓			
CKM_DES3_CBC	✓			
CKM_DES3_CBC_PAD	✓			
CKM_MD2				
CKM_MD5			✓	
CKM_SHA_1			✓	
CKM_DH_PKCS_KEY_PAIR_GEN				
CKM_AES_KEY_GEN				✓
CKM_AES_CBC	✓			
CKM_AES_ECB	✓			

The table below lists all the key sizes in UniMate PKCS#11.

Mechanisms	Key Sizes
CKM_RSA_PKCS_KEY_PAIR_GEN	1024bits,2048bits
CKM_DES_KEY_GEN	8 bytes
CKM_DES3_KEY_GEN	24 bytes
CKM_AES_KEY_GEN	16~32 bytes

UniMate PKCS#11 Function Library

UniMate PKCS#11 library only implements the standard PKCS#11 APIs. Any other API beyond PKCS#11 is not implemented. If such API is called, an error return code like CKR_FUNCTION_NO_SUPPORT will be returned.

Category	Function	Supported
General Purpose Function	C_Initialize	YES
	C_Finalize	YES
	C_GetInfo	YES
	C_GetFunctionList	YES
Slot and UniMate Management Function	C_GetSlotList	YES
	C_GetSlotInfo	YES
	C_GetUniMateInfo	YES
	C_WaitForSlotEvent	YES
	C_GetMechanismList	YES
	C_GetMechanismInfo	YES
	C_InitUniMate	YES
	C_InitPIN	YES
	C_SetPIN	YES
Session Management Function	C_OpenSession	YES
	C_CloseSession	YES
	C_CloseAllSessions	YES
	C_GetSessionInfo	YES
	C_GetOperationState	NO
	C_SetOperationState	NO
	C_Login	YES
	C_Logout	YES
Objects Management Function	C_CreateObject	YES
	C_CopyObject	NO
	C_DestroyObject	YES
	C_GetObjectSize	YES
	C_GetAttributeValue	YES
	C_SetAttributeValue	YES
	C_FindObjectsInit	YES
	C_FindObjects	YES
	C_FindObjectsFinal	YES

Category	Function	Supported
Encryption Function	C_EncryptInit	YES
	C_Encrypt	YES
	C_EncryptUpdate	YES
	C_EncryptFinal	YES
Decryption Function	C_DecryptInit	YES
	C_Decrypt	YES
	C_DecryptUpdate	YES
	C_DecryptFinal	YES
Message Digesting Function	C_DigestInit	YES
	C_Digest	YES
	C_DigestUpdate	YES
	C_DigestKey	NO
	C_DigestFinal	YES
Signing and Hashing Function (MAC)	C_SignInit	YES
	C_Sign	YES
	C_SignUpdate	NO
	C_SignFinal	NO
	C_SignRecoverInit	NO
	C_SignRecover	NO
Functions for Verifying Signatures and Hashing (MAC)	C_VerifyInit	YES
	C_Verify	YES
	C_VerifyUpdate	NO
	C_VerifyFinal	NO
	C_VerifyRecoverInit	NO
	C_VerifyRecover	NO
Dual-purpose Cryptographic Function	C_DigestEncryptUpdate	NO
	C_DecryptDigestUpdate	NO
	C_SignEncryptUpdate	NO
	C_DecryptVerifyUpdate	NO
Key Management Function	C_GenerateKey	YES
	C_GenerateKeyPair	YES
	C_WrapKey	YES
	C_UnwrapKey	YES
	C_DeriveKey	NO
Random Number Generation Function	C_SeedRandom	NO
	C_GenerateRandom	YES
Callback Function		YES

Samples

All the samples are implemented in C language, and they all support PKCS#11 standard v.2.20. We provide the samples located in: SDK\ PKCS#11\Sample

FUNCTION	DESCRIPTION
C_Initialize	Initialize the PKCS#11 library
C_GetSlotList	Get the slot list
C_OpenSession	Open an session
C_Login	Log in
C_InitPIN	Initialize user PIN
C_Logout	Log out
C_FindObjectsInit	Initialize the search for any object
C_FindObjects	Find the objects which match
C_FindObjectsFinal	Cleanup the search
C_CloseSession	Close an session
C_GetAttributeValue	Get the attribute value
C_Finalize	Close PKCS #11 library
C_GenerateKeyPair	Generate new key pair
C_GenerateKey	Generate a secret key
C_UnwrapKey	Unwrap (decrypts) a wrapped key
C_WrapKey wraps	Encrypt a key
C_DeriveKey	Derive a key from a base key
C_SetPIN	Change PIN
C_GetTokenInfo	Get the slot information
C_SignInit	Initialize a signature
C_Sign	Sign data
C_SignUpdate	Continue a multiple-part signature
C_SignFinal	Finish a multiple-part signature
C_SignRecoverInit	Initialize a signature
C_SignRecover	Sign data
C_DestroyObject	Destroy the objects
C_GetFunctionList	Return the function list
C_GetMechanismList	Obtain a list of mechanism types
C_GetMechanismInfo	Obtain information about a particular mechanism possibly supported by a token
C_InitToken	Initialize a token
C_GetSessionInfo	Obtain information about the session
C_GetOperationState	Obtain the state of the cryptographic
C_SetOperationState	Restore the state of the cryptographic

Function	Description
C_EncryptInit	Initialize an encryption operation
C_Encrypt	Encrypt single-part data
C_EncryptUpdate	Continue a multiple-part encryption
C_EncryptFinal	Finish a multiple-part encryption operation
C_DecryptInit	Initialize a decryption
C_Decrypt	Decrypt encrypted data in a single part
C_DecryptUpdate	Continue a multiple-part decryption
C_DecryptFinal	Finish a multiple-part decryption
C_DigestInit	Initialize a message-digesting operation.
C_Digest	Digest data in a single part
C_DigestUpdate	Continue a multiple-part message-digesting
C_DigestFinal	Finish a multiple-part message-digesting
C_VerifyInit	Initialize a verification
C_Verify	Verify a signature
C_VerifyUpdate	Continue a multiple-part verification
C_VerifyFinal	Finish a multiple-part verification
C_VerifyRecoverInit	Initialize a signature verification
C_VerifyRecover	Verify a signature
C_SeedRandom	Mix additional seed material into the token's random number generator
C_GenerateRandom	Generate random data
C_GetFunctionStatus	Obtain an updated status of a function running in parallel with an application
C_CancelFunction	Cancel a function
C_WaitForSlotEvent	Wait for a slot event to occur

Follow us!


[Twitter](#)

[Facebook](#)

[Youtube](#)

[Linked in](#)


About SecuTech

SecuTech Solution Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.

SecuTech

www.eSecuTech.com SecuTech Solution Inc.

North America

1250 Boulevard René-Lévesque Ouest, #2200,
Montreal, QC, H3B 4W8,
Canada
T: +1 -888-259-5825
F: +1 -888-259-5825 ext.0
E: INFO@eSecuTech.com

China

Level 12, #67 Bei Si Huan
Xi Lu,
Beijing, China, 100080
T: +8610-8288 8834
F: +8610-8288 8834
E: CN@eSecuTech.com

APAC

Suite 5.14, 32 Delhi Rd,
North Ryde,
NSW, 2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002
Lyon, France
T: +33-042-600-2810
F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com

©Copyright 2012 SecuTech Solution Inc. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech UniMate and the SecuTech logo are trademarks of SecuTech Inc. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.

Email: sales@eSecuTech.com / Web: www.eSecuTech.com / WIKI: www.eSecuTech.com/wiki

Support portal: www.eSecuTech.com/support / SDK software download : (PW: opensesame)

[Http://www.eSecuTech.com/downloads](http://www.eSecuTech.com/downloads) / Order: www.eSecuTech.com/store