



CSP MANUAL

VERSION 1.0

A large, thick orange line forming a mountain peak shape, spanning the width of the page and extending from the bottom left towards the top right.

The Key to the Information Security

Trademarks

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
CHAPTER 1: ALGORITHMS AND API'S	2
CHAPTER 2: SAMPLES	3
2.1 Algorithm sample	4
2.2 Container Sample	5
2.3 List Certificate Sample	6
CHAPTER 3: PKI PACKAGE	7
3.1 Installation	7
3.2 Un-installation	8

Introduction

CAPI (Cryptographic Application Programming Interface), developed by Microsoft as part of Microsoft Windows, is an interface to a library of functions software developers can call upon for security and cryptography services. It is intended for use by developers of applications for MS Windows platforms.

CAPI allows multiple cryptographic service providers (CSP) to coexist on the same computer and to be used in the same application. It is also possible to associate a CSP with a particular smartcard, so that smartcard-enabled Windows applications will call the correct CSP. MS Windows contains many helper functions that application developers may use to simplify code when working with cryptographic functions or with complicated data structures (such as certificates).

Choosing which API to use when developing applications is dependent on the needs of the particular application.

Chapter 1: Algorithms and API's

Connection functions	
CPAcquireContext	Create a context and initialize access to CSP which must be specified
CPReleaseContext	Release the context created in CPAcquireContext and other resources
CPGetProvParam	Return information related to CSP
CPSetProvParam	Set parameters of CSP
Key to generate and exchange function	
CPGenKey	Generate key or key pair
CPDeriveKey	Derive a session key from a data hash and guarantee the generated key difference
CPSetKeyParam	Set key attributes
CPGetKeyParam	Get the attributes of encryption-operating key
CPExportKey	Export key from container
CPImportKey	Import the key to CSP container
CPDestroyKey	Release key handle, after which the handle will be invalid and no access allowed
CPDuplicateKey	Create a duplicate of key
CPGenRandom	Generate random data
CPGetUserKey	Get the enduring key pair from CSP container
Data encryption function	
CPDecrypt	Decrypt encrypted document
CPEncrypt	Encrypt unencrypted document
CPCreateHash	Create hashing objects and initialize them
CPDestroyHash	Delete hashing objects handle
CPDuplicateHash	Create a duplicate of hashing object
CPHashData	Hash the input number
CPGetHashParam	Get the computing result of hashing object
CPHashSessionKey	Hash a session key but not reveal the key value to the application
CPSetHashParam	Set the attribute of a hashing object
CPSignHash	Sign a hashing object
CPVerifySignature	Verify a digital signature

Chapter 2: Samples

All the samples are implemented in the C language, and they all support the MS-CAPI standard. We provide the samples below, located in path: SDK\CSP(MS-CAPI)\Sample

Function	Files	Description
Algorithm	algorithmTest.cpp algorithmTest.h	The sample provides the operations on symmetric keys, hashing and asymmetric keys.
Container	kcsTest.cpp kcsTest.h	The sample provides the operations on enumeration, deletion and creation of files.
Certificates	listcerts.cpp listcerts.h	The sample provides the operations on certificate list.

2.1 Algorithm sample

These samples include 3 functions:

- `int GenerateAlgTest(ULONG ulALG);`
- `int DeviceAlgTest(ULONG ulALG);`
- `int RstTest(ULONG version);`

GenerateAlgTest is used for DES key generation, encryption and decryption operations.

Steps	Function
1. Create a container	CryptAcquireContext
2. Retrieve parameters that govern the operations of a CSP	CryptGetProvParam
3. Generate a key	CryptGenKey
4. Data Encryption	CryptEncrypt
5. Data Decryption	CryptDecrypt

DeviceAlgTest is used for key derivation, data encryption and decryption operations.

Steps	Function
1. Create a container	CryptAcquireContext
2. Initiate the hashing of a stream of data	CryptCreateHash
3. Add data to a specified hash object	CryptHashData
4. Derive a key	CryptDeriveKey
5. Data Encryption	CryptEncrypt
6. Data Decryption	CryptDecrypt

RstTest is used for RSA key generation, data encryption and decryption operations.

Steps	Function
1. Create a container	CryptAcquireContext
2. Generate a key	CryptGenKey
3. Data Encryption	CryptEncrypt
4. Data Decryption	CryptDecrypt

2.2 Container Sample

The sample demonstrates how to enumerate, add and delete containers with `int kcsTest(ULONG ulActive)` function.

For enumerating a container

Steps	Function
1. Acquire a "VERIFYCONTEXT" handle	CryptAcquireContext
2. Enumerate the key containers	CryptGetProvParam
3. Acquire a handle to the key container found	CryptAcquireContext
4. Try to get a handle to the key pair	CryptGetUserKey
5. Get key permissions	CryptGetKeyParam
6. Display key permissions	

For adding a container

Steps	Function
1. Check whether the container already exists	CryptAcquireContext
2. If not, create a container	CryptAcquireContext

For deleting a container

Steps	Function
1. Check whether the container already exists	CryptAcquireContext
2. If there is, release the handle to the context	CryptReleaseContext
3. Delete the container	CryptAcquireContext

2.3 List Certificate Sample

The sample demonstrates how to enumerate certificates with `int listcerts(void)` function

For enumerating certificates

Steps	Function
1. Open a handle to the MY\UniMateStore certificate store	CertOpenStore
2. Go over each and every certificate within the certificate store	CertEnumCertificatesInStore
3. Get and display the subject name from the certificate	CertGetNameString

Chapter 3: PKI package

UniMate provides a PKI package for developers and end users respectively. The package provides UniMate PKI installation. If you want to use the PKI application, you must install it.

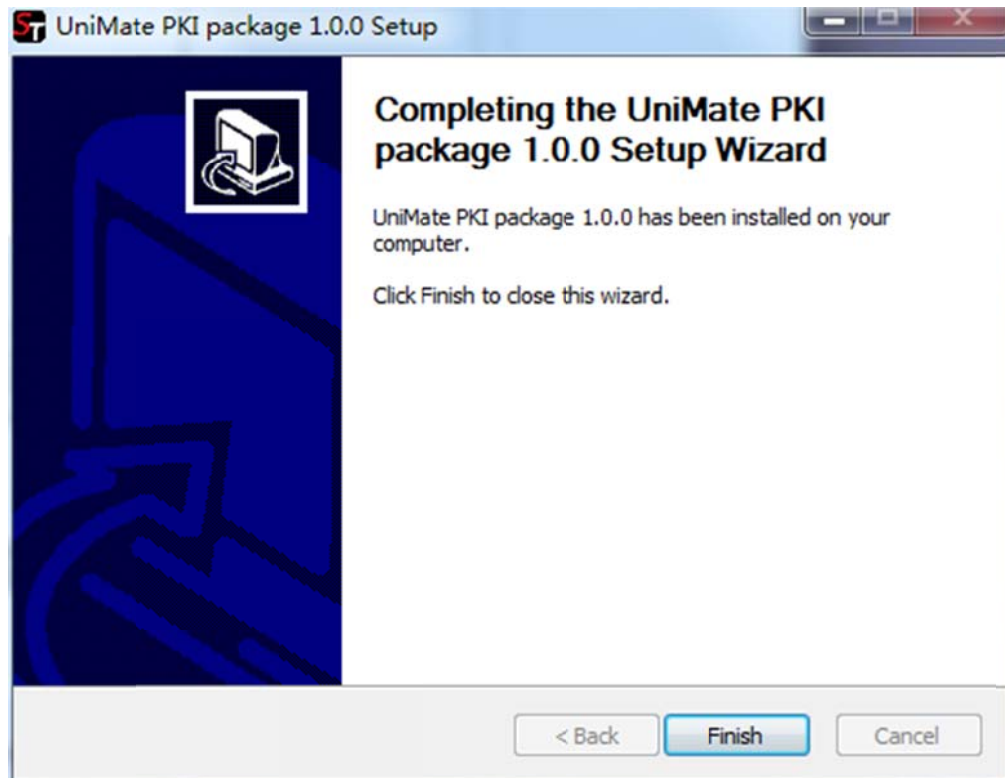
3.1 Installation

UniMate PKI package can be found in the redist folder of UniMate SDK.

For the developer package, double click the icon to run the PKI package.exe, and follow the illustration below:



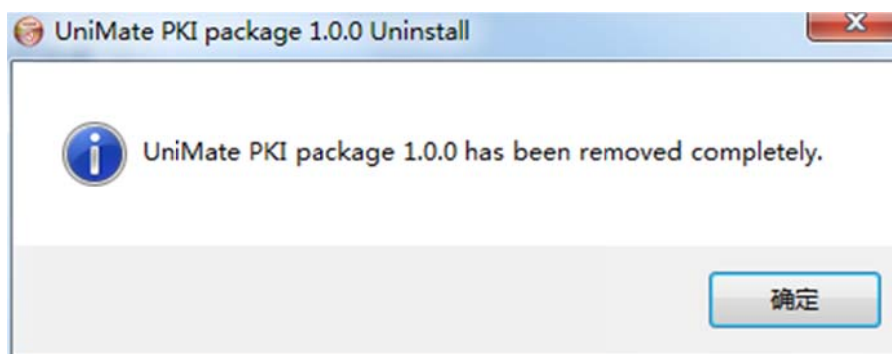
Click "Install".



At last, click “Finish” to close the setup wizard.

3.2 Un-installation

To uninstall the software, select “Start-All Programs-UniMate Drive-PKI package-uninstall”



Click “OK” and restart your computer to finish the un-installation.

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> / Order: www.eSecuTech.com/store