

# UniMate USB CSP Manual

From SecuTech Wiki

## Contents

- 1 CSP Manual
- 2 Introduction
- 3 Algorithms and APIs
- 4 Samples
  - 4.1 Algorithm samples
  - 4.2 Container sample
  - 4.3 List Certificate sample
- 5 PKI package
  - 5.1 Installation
  - 5.2 Uninstallation

## CSP Manual

Version 2.0

Version	Date
1.0	2015.7
2.0	2016.7

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 <sup>(TM)</sup> 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

Web: <http://www.esecutech.com>

Email: [sales@esecutech.com](mailto:sales@esecutech.com) (<mailto:sales@esecutech.com>)

Please Email any comments, suggestions or questions regarding this document or our products to us at:  
sales@esecutech.com (mailto:sales@eSecuTech.com)

#### 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 USBbased.

#### 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 environmentally friendly with ROHS certificates.

## 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.

## Algorithms and APIs

Connection functions	
CryptAcquireContext	Create a context and initialize access to CSP which must be specified
CryptReleaseContext	Release the context created in CryptAcquireContext and other resources
CryptGetProvParam	Return information related to CSP
CryptSetProvParam	Set parameters of CSP
Generate and exchange key functions	
CryptGenKey	Generate key or key pair
CryptDeriveKey	Derive a session key from a data hash and guarantee the generated key difference
CryptSetKeyParam	Set key attributes
CryptGetKeyParam	Retrieves the data that controls the operations of the key
CryptExportKey	Export key from container
CryptImportKey	Import the key to CSP container
CryptDestroyKey	Release key handle, after which the handle will be invalid and cannot be accessed
CryptDuplicateKey	Create a duplicate of the key
CryptGenRandom	Generate random data
CryptGetUserKey	Gets a handle to a permanent user key
Data encryption function	
CryptDecrypt	Decrypt document
CryptEncrypt	Encrypt document
CryptCreateHash	Returns a handle to a created hashing object and initializes it
CryptDestroyHash	Delete hashing object handle
CryptDuplicateHash	Duplicates a hashing object, including state, up to when the duplication is done
CryptHashData	Hash input data
CryptGetHashParam	Get the hash value and data that control the operations of the hash object
CryptHashSessionKey	Hash a session key without revealing the key value to the application
CryptSetHashParam	Set the attributes of a hash object, such as specific algorithm or initial contents
CryptSignHash	Sign a hash object
CryptVerifySignature	Verifies the signature of a hash object

## 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	This sample demonstrates operations on symmetric keys, hashing and asymmetric keys.
Container	kcsTest.cpp kcsTest.h	This sample demonstrates enumeration, deletion and creation of files.
Certificates	listcerts.cpp listcerts.h	This sample demonstrates operations on a certificate list.

### Algorithm samples

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

### Container sample

This sample demonstrates how to enumerate, add and delete containers with the function – int kcsTest(ULONG ulActive)

For enumerating a container:

Steps	Function
1. Acquire a "VERIFYCONTEXT" handle	CryptAcquireContext
2. Enumerate through 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 it does, release the handle to the context	CryptReleaseContext
3. Delete the container	CryptAcquireContext

## List Certificate sample

This sample demonstrates how to enumerate certificates with the function - int listcerts(void)

For enumerating certificates:

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

## PKI package

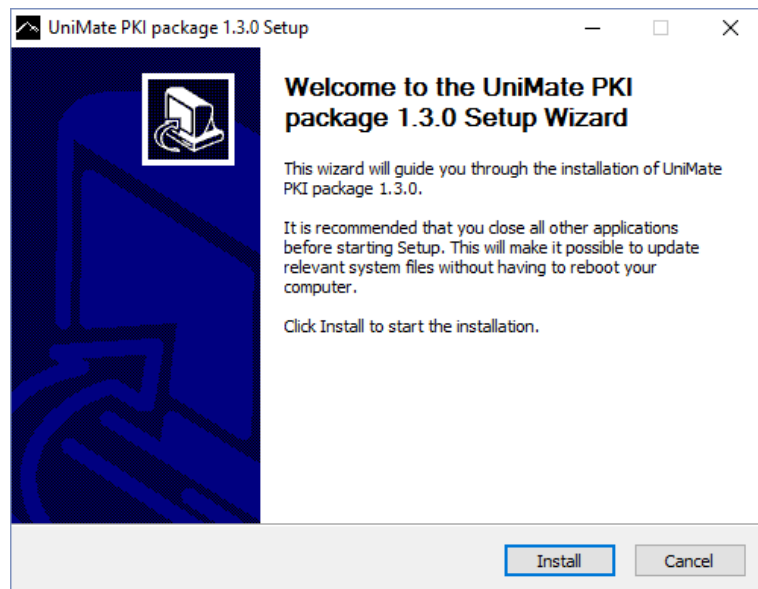
UniMate provides a PKI package for developers and end users respectively. The package provides the UniMate PKI installation, if you want to use the PKI package, you must install it.

### Installation

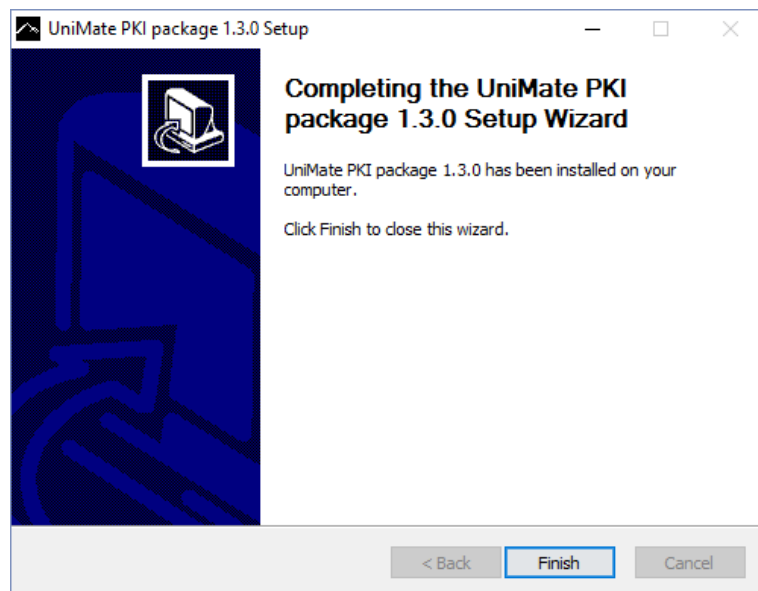
The UniMate PKI package can be found in the redists folder of the SDK.

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

Click Install.



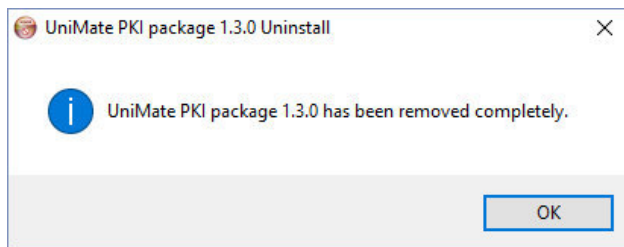
Afterwards, click Finish to close the setup wizard.







### Uninstallation

To uninstall the software, select Start Menu -- All apps -- UniMate Drive\PKI package\uninstall (on Windows 8/10 you may need to right-click the file in the folder, mouse over More and select Open file location). Otherwise, by default the uninstaller is located in: C:\Users\<your\_username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\UniMate Drive\PKI package

Click OK and restart your computer to finish the uninstallation.



If you have any questions, please feel free to contact us at: <http://www.esecutech.com/support> or [support@esecutech.com](mailto:support@esecutech.com) (<mailto:support@esecutech.com>)

Follow Us!			
			
Twitter ( <a href="https://twitter.com/eSecuTech">https://twitter.com/eSecuTech</a> )	Facebook ( <a href="https://www.facebook.com/eSecuTech/">https://www.facebook.com/eSecuTech/</a> )	YouTube ( <a href="https://www.youtube.com/user/esecutech">https://www.youtube.com/user/esecutech</a> )	LinkedIn ( <a href="https://ca.linkedin.com/in/secutech-solutions-inc-39110b25">https://ca.linkedin.com/in/secutech-solutions-inc-39110b25</a> )



## 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 that are effective against increasingly sophisticated cyber attacks. Enabling enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing.

<http://www.esecutech.com>  
SecuTech Solution Inc.

### Contact Us:

	North America	China	Asia-Pacific	EMEA
Address	1250 Boulevard Ren-Lvesque Ouest, #2200, Montreal, QC, H3B 4W8, Canada	Level 12, #67 Bei Si Huan Xi Lu, Beijing, China, 100080	Suite 5.14, 32 Delhi Rd, North Ryde, NSW, 2113, Australia	4 Cours Bayard 69002 Lyon, France
Phone	+1 -888-259-5825	+8610-8288 8834	00612-9888 6185	+33-042-600-2810
Fax	+1 -888-259-5825 ext.0	+8610-8288 8834	00612-9888 6185	+33-042-600-2810
Email	<a href="mailto:info@esecutech.com">info@esecutech.com</a> ( <a href="mailto:info@esecutech.com">mailto:info@esecutech.com</a> )	<a href="mailto:cn@esecutech.com">cn@esecutech.com</a> ( <a href="mailto:cn@esecutech.com">mailto:cn@esecutech.com</a> )	<a href="mailto:aus@esecutech.com">aus@esecutech.com</a> ( <a href="mailto:aus@esecutech.com">mailto:aus@esecutech.com</a> )	<a href="mailto:europe@esecutech.com">europe@esecutech.com</a> ( <a href="mailto:europe@esecutech.com">mailto:europe@esecutech.com</a> )

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.

# SecuTech

TOP

Retrieved from "[https://esecutech.com/wiki/index.php?title=UniMate\\_USB\\_CSP\\_Manual&oldid=2704](https://esecutech.com/wiki/index.php?title=UniMate_USB_CSP_Manual&oldid=2704)"

Category: UniMate Manuals

- This page was last modified on 30 June 2016, at 06:24.