



Developer's Guide

UniMate®

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. (hereafter referred to as SecuTech) 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 a 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 aid and assistance. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

Contact Information

Web: www.eSecuTech.com/support

E-Mail: Support@eSecuTech.com

Please e-mail any comments, suggestions or questions regarding this document or our products to us at: Support@eSecuTech.com

Version history

Version	Date
1.0	2012. 08

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.

USB



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 Compliance



All UniMate products are environmental friendly with RoHS certificates.

Contents

Contents	IV
Part 1 An Overview of UniMate.....	1
1.1 UniMate Device	1
1.1.1 Features.....	1
1.1.2 Specifications	2
1.2 UniMate Software	2
1.2.1 UniMate Tools.....	2
1.2.2 UniMate API	3
1.3 UniMate SDK	4
1.3.1 SDK Overview	4
1.3.2 Redistribution Package.....	4
Part 2 User's Guide	9
2.1 UniMate Monitor	9
2.2.1 UniMate Information.....	10
2.2.2 User Tools	11
Part 3 Applying Certificates with UniMate.....	18
3.1 Applying Digital Certificates.....	18
3.1.1 Applying VeriSign Certificates	18
3.1.2 Applying Microsoft Certificates.....	19
3.2 Using Digital Certificates	22
Appendix A Glossary	23

Part 1 An Overview of UniMate

Traditional USB Tokens provide a scalable two factor authentication security solution for desktops, VPNs, WLANs and Web portals to enhance enterprise security, but it cannot be used for Mobile devices. UniMate, the first dual enabled two factor authentication token providing customers with more flexibility and choice for both pc and mobile devices.

SecuTech UniMate TRRS and USB DUAL-Enabled two-factor authentication token enables customers to manage a broad range of authentication credentials, including one time password, digital certificates and static passwords, it's easy to works on iPhone, Ipod, Android, PC and MAC, and it is the first security token available for both computers and smartphones which can work seamlessly between devices.

UniMate has achieved an effective rights management and can provide a highly-secured file system. A built-in computing engine accomplishes fast and efficient information processing.

UniMate supports PKI applications and provides UniMate API for development in Android and iOS Mobile devices.

1.1 UniMate Device

1.1.1 Features

Key features of UniMate device:

- TRRS: 3.5mm
- USB Interface: USB Type A
- Hardware ID: 64 bits, globally unique
- Internal Memory: > 16KB
- Smart Card: High performance SmartCard, supports RSA, DES, 3DES, MD5 etc.
- USB Operation Mode: HID
- Power Supply: Lithium-Ion rechargeable battery
- Charge Mode: USB
- Middleware: PKCS#11, Mini-Driver, MS-CAPI, Audio Authentication API, X.509 digital Certificate

- Supported Platforms: iOS, Android, Symbian, Windows, Linux, Mac OS
- Time For Digital Signing via Audio: <2s
- Time For Digital Signing via USB: <0.5s

1.1.2 Specifications

Table 1.1: Relevant Specifications of UniMate Device

Dimensions	48.1 * 48.2 * 9.7 mm
Min. Operating Voltage	4.75V
Current Consumption	<= 50 mA
Operation Temperature	-10°C to 50°C
Storage Temperature:	-40°C to 80°C
Humidity Rate	1-90% without condensation
Memory Data Retention	At least 10 years
Memory Cell Rewriters	At least 100,000 times

1.2 UniMate Software

1.2.1 UniMate Tools

In order to simplify the management of UniMate, we provide two tools: UniMate Console and UniMate Monitor.

UniMate Console helps users to log on/off at different permission levels, operate on the passwords as well as manage the files and certificates.

UniMate Monitor is used to view the information of certificates and check the registration status.

UniMate provides different tools for different users, i.e. for developers, both UniMate Console and Monitor are provided; for end users, only UniMate Monitor is provided. While installing the PKI package, these tools will be installed. The installation of the PKI packages will be introduced in the section of redistribution package. Besides, the specific usage of the two tools will be introduced in Part 2.

1.2.2 UniMate API

UniMate provides a set of UniMate API, which allows users to manage UniMate hardware key in Mobile devices. It provides C interfaces in Android platform and Objective-C interfaces in iOS.

1.3 UniMate SDK

1.3.1 SDK Overview

Table 1.6 UniMate SDK Contents

COMPONENTS	DESCRIPTION
Include	Declaration of the standardized identifiers and interface of Android & iOS
Libraries	UniMate libraries for Android & iOS
Documents	Manual for UniMate SDK
Redistribution	Redistribution packages for Windows


1.3.2 Redistribution Package

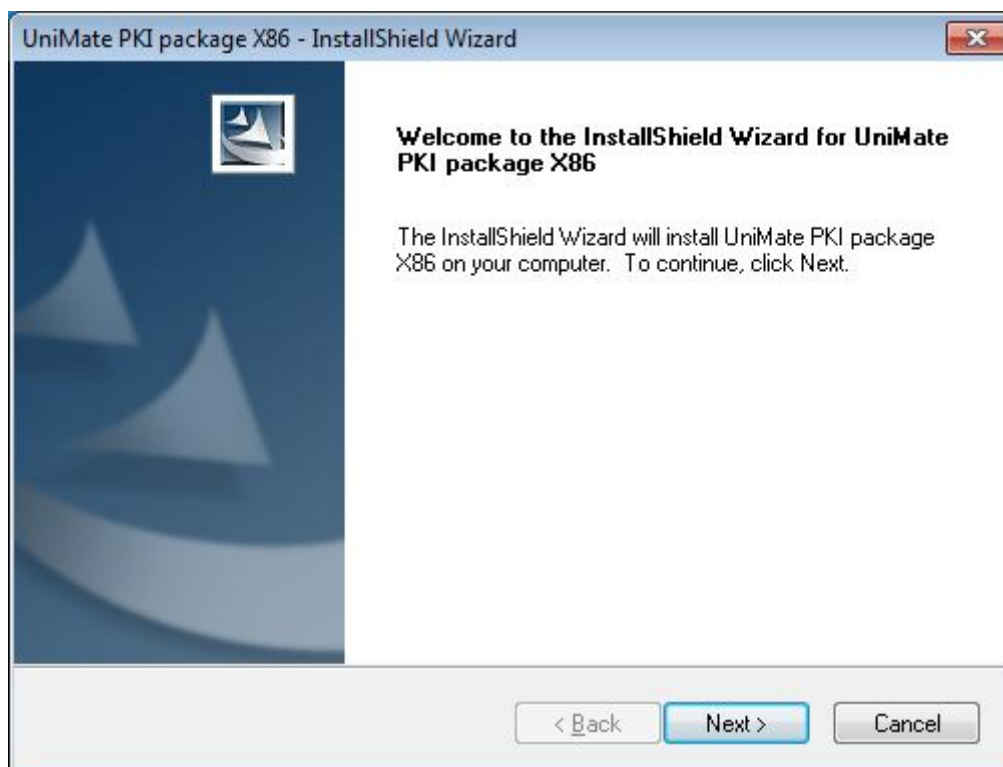
UniMate provides UniMate PKI installation package. If you want to use the PKI application, you must install it.

- Installation

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

For developers package

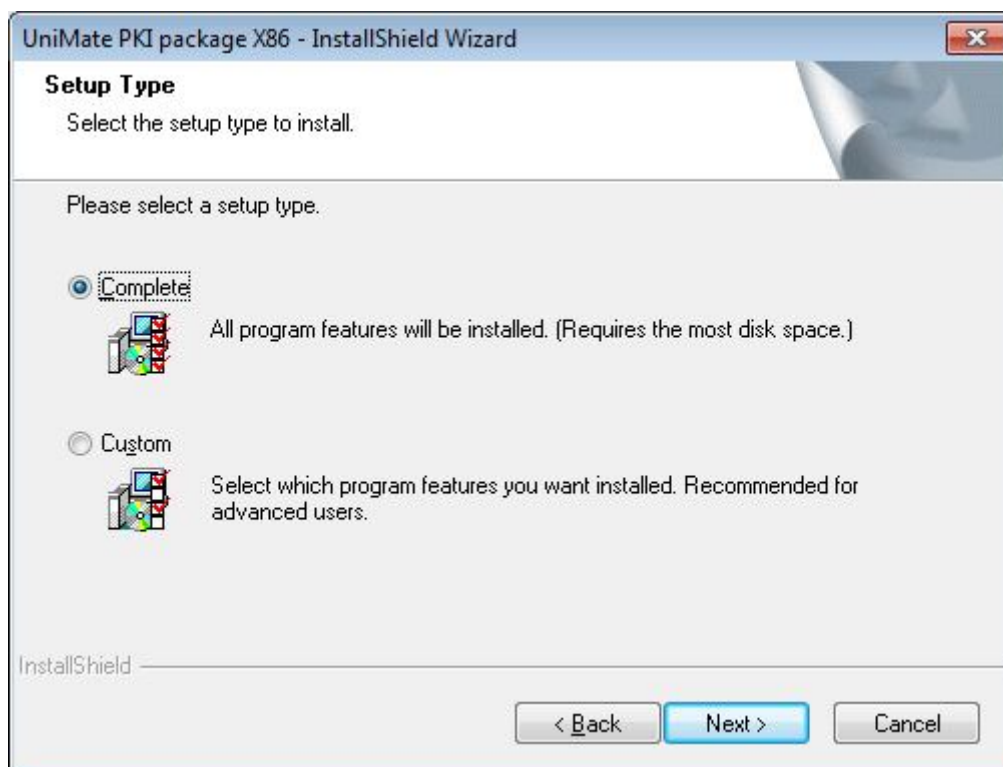
Double click the icon  to run the install shield wizard, and follow the illustration below:



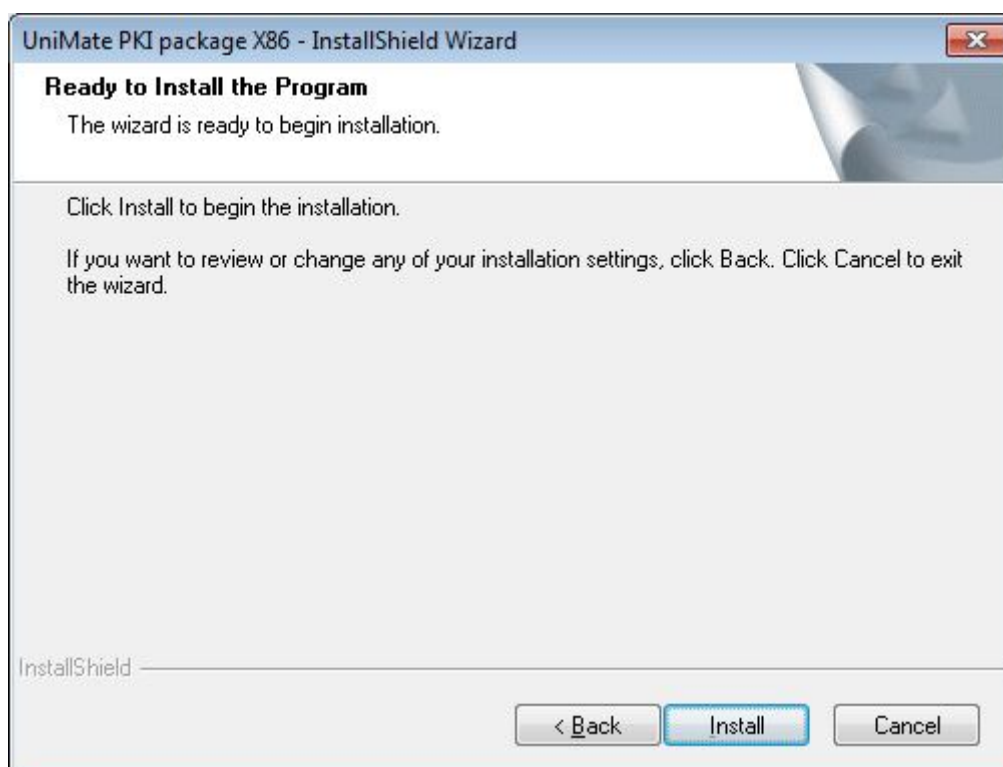
Click “Next”.

The screenshot shows the 'Customer Information' screen of the 'UniMate PKI package X86 - InstallShield Wizard'. The title bar is the same as the previous window. The section is titled 'Customer Information' with the instruction 'Please enter your information.' Below this, it says 'Please enter your name and the name of the company for which you work.' There are two input fields: 'User Name:' with the text 'test' and 'Company Name:' with the text 'SecuTech'. At the bottom left, it says 'InstallShield'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

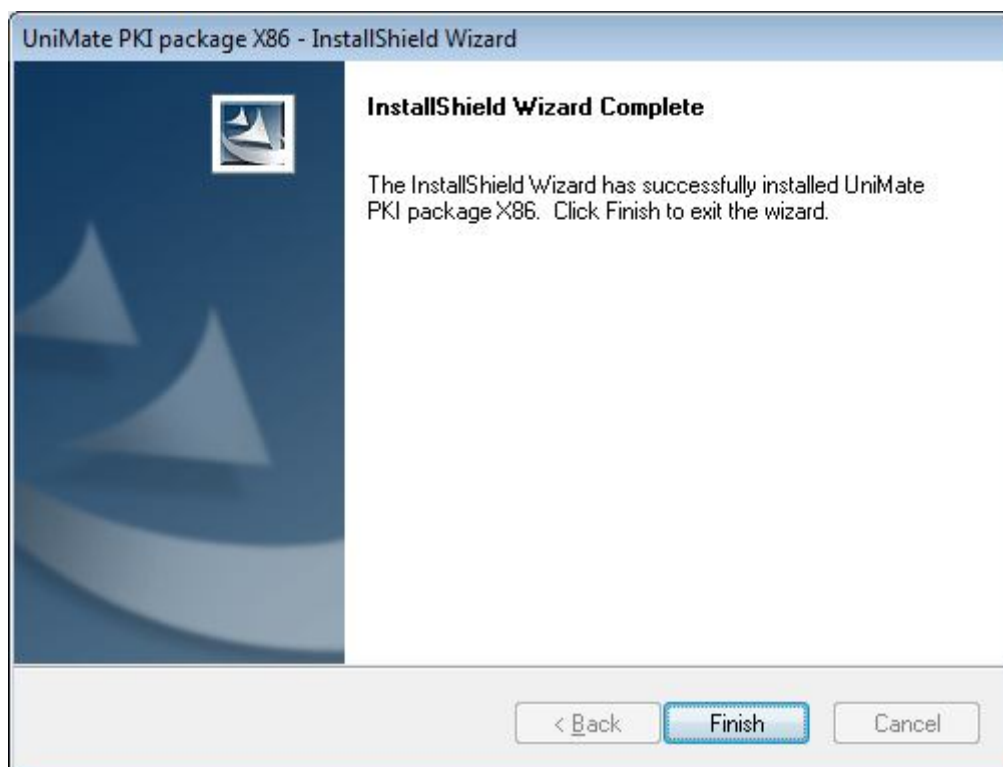
In this section, user name and company name are required. And click “Next”.



Users are allowed to choose setup type. And click “*Next*”.

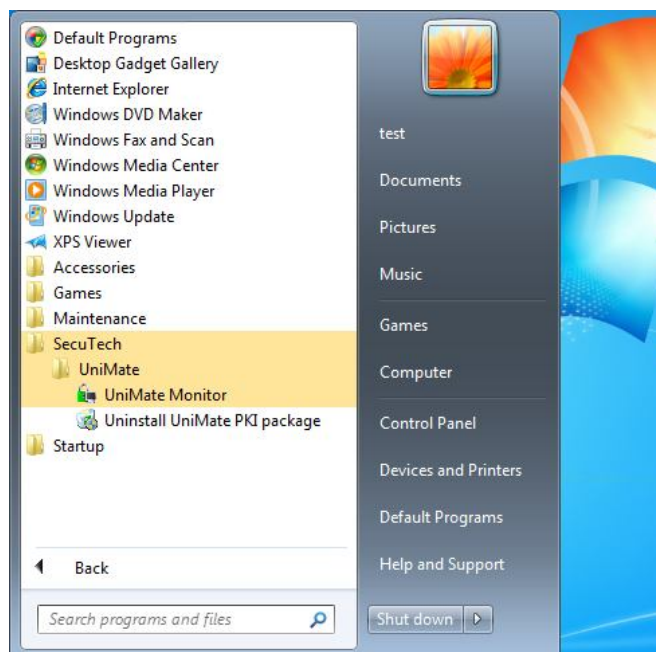


Click “*Install*”.



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

After installation, UniMate Monitor will be installed. Users can access it by the desktop shortcuts or the Start menu→All Programs→Secutech→UniMate.

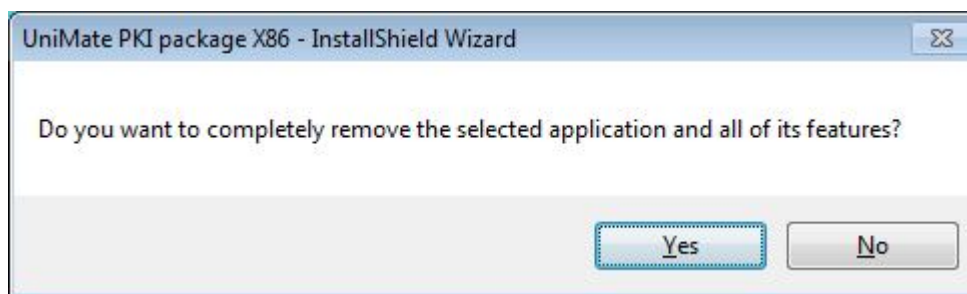


- Uninstallation

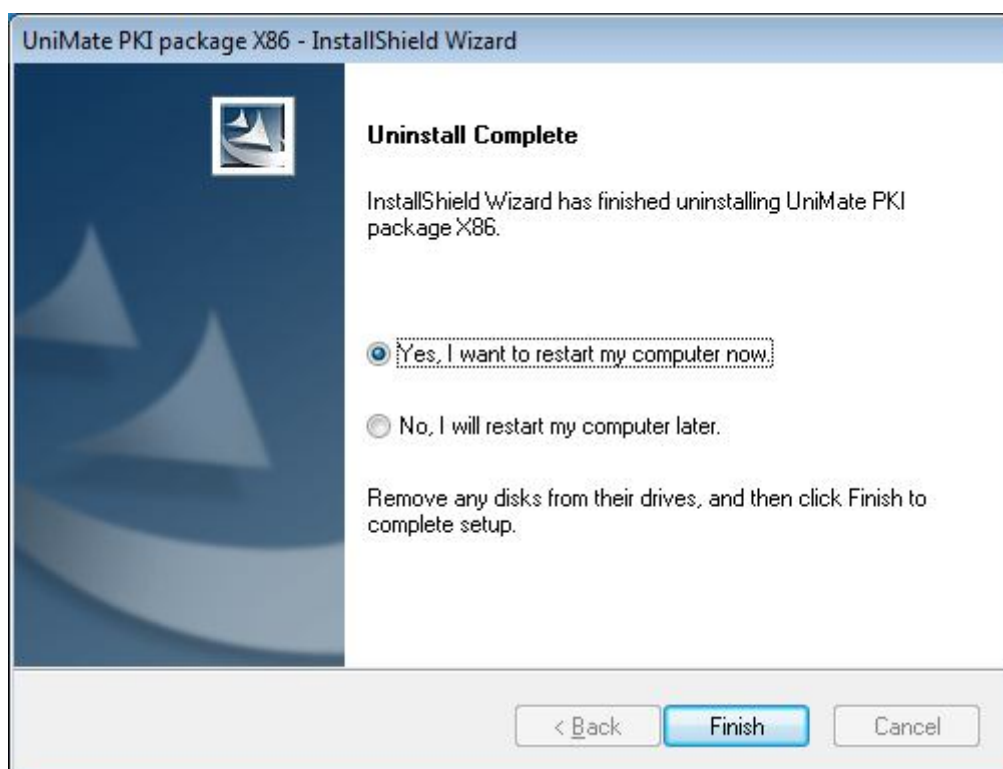
To uninstall the software, there are two ways: start menu and control panel.

Start Menu:

Select “Start-All Programs-SecuTech-UniMate-Uninstall UniMate PKI package”



Click “Yes”.



Click “Finish”.


Part 2 User's Guide

In the first part, we introduced that we designed a tool to help manage our UniMate. In this section and the next, we will introduce the usage in detail.

2.1 UniMate Monitor

UniMate Monitor is used to view the detailed information of certificates imported into the UniMate and register or unregister certificates. Here, it also provides a way to change User PIN.

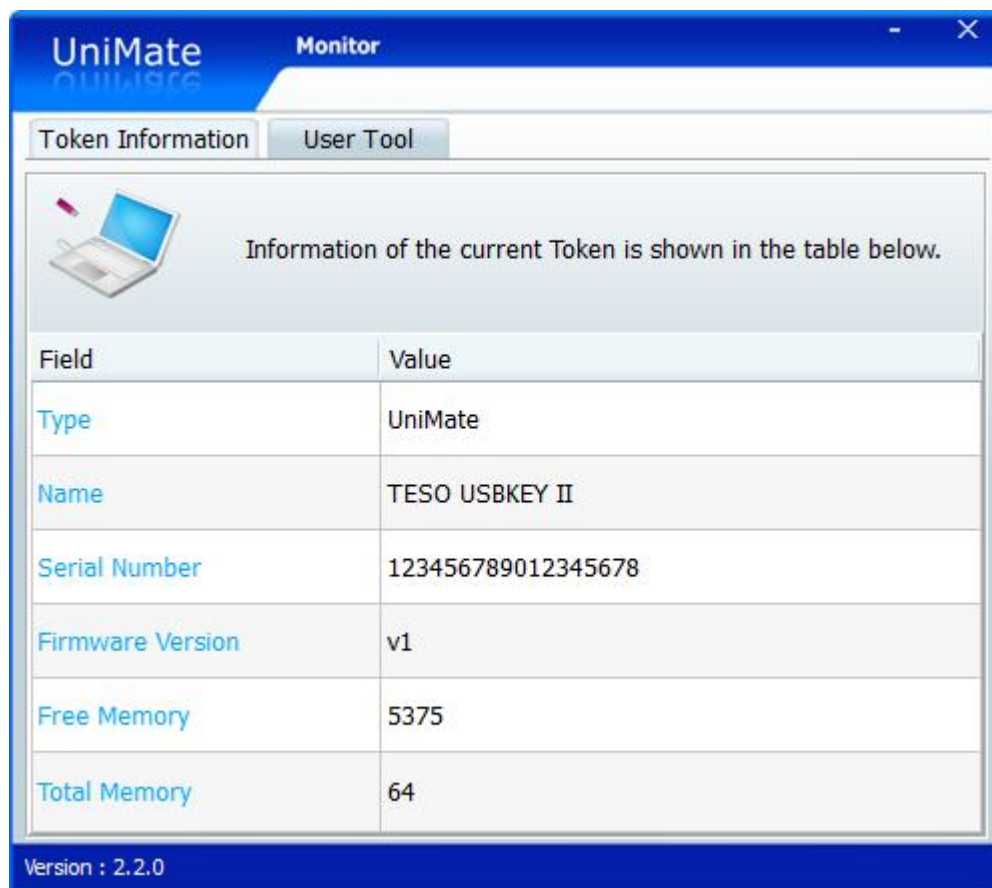
- To start the UniMate Monitor

Double click the UniMate Monitor. exe in the SDK folder, and  will appear in the notification area of the task bar. Double click it, the Monitor interface will pop up, illustrated as the picture below:

With this tool, you can view the information of certificate, change password and check the registration status.

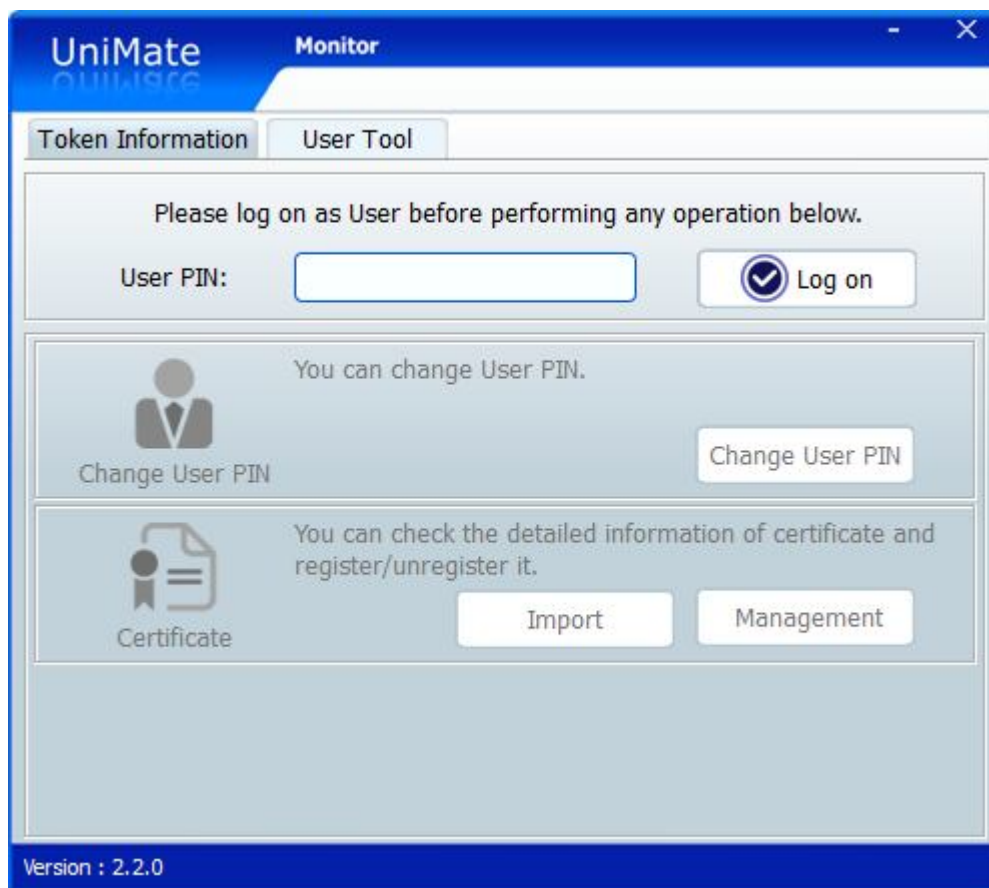
2.2.1 UniMate Information

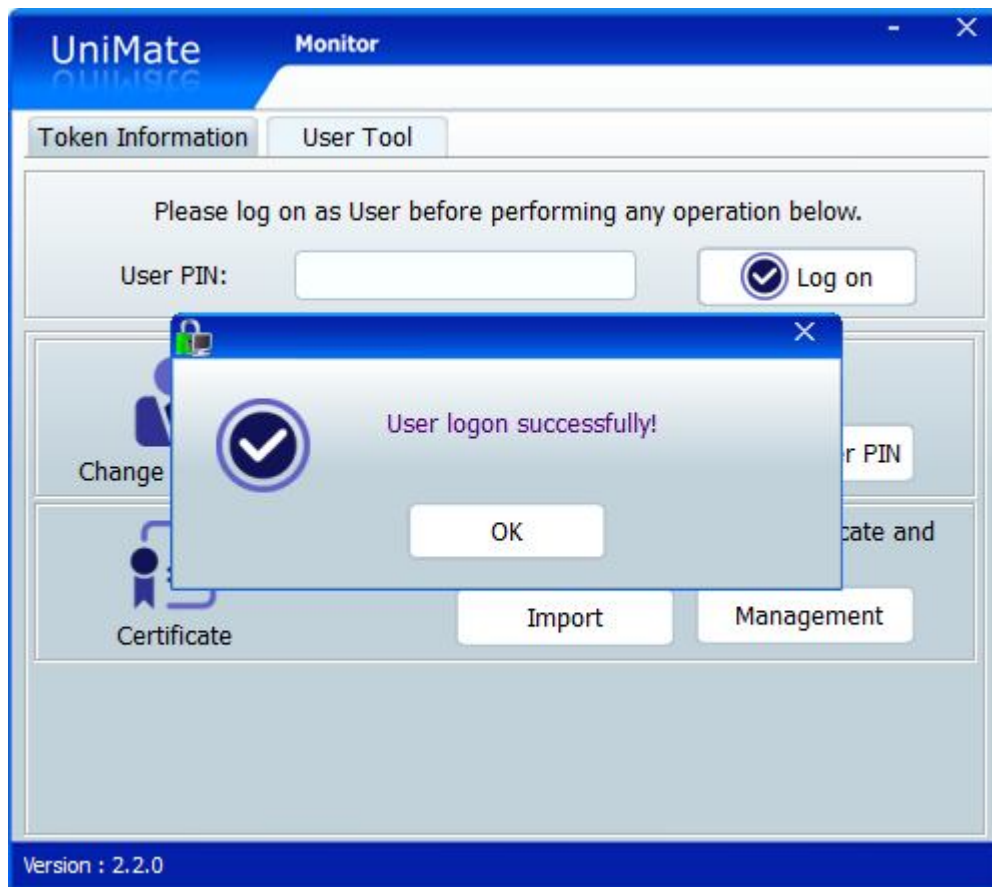
In this tab, the detailed information of UniMate will show as below.



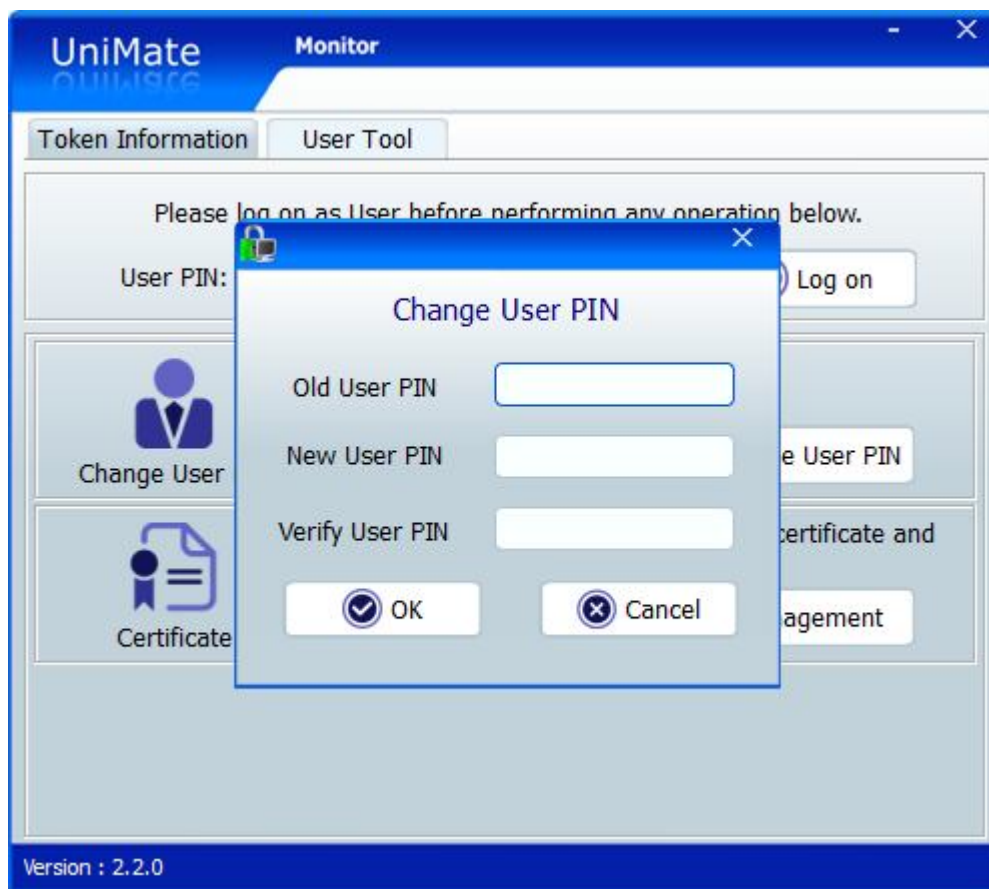
2.2.2 User Tools

This tab provides an interface to perform all the operations by User.

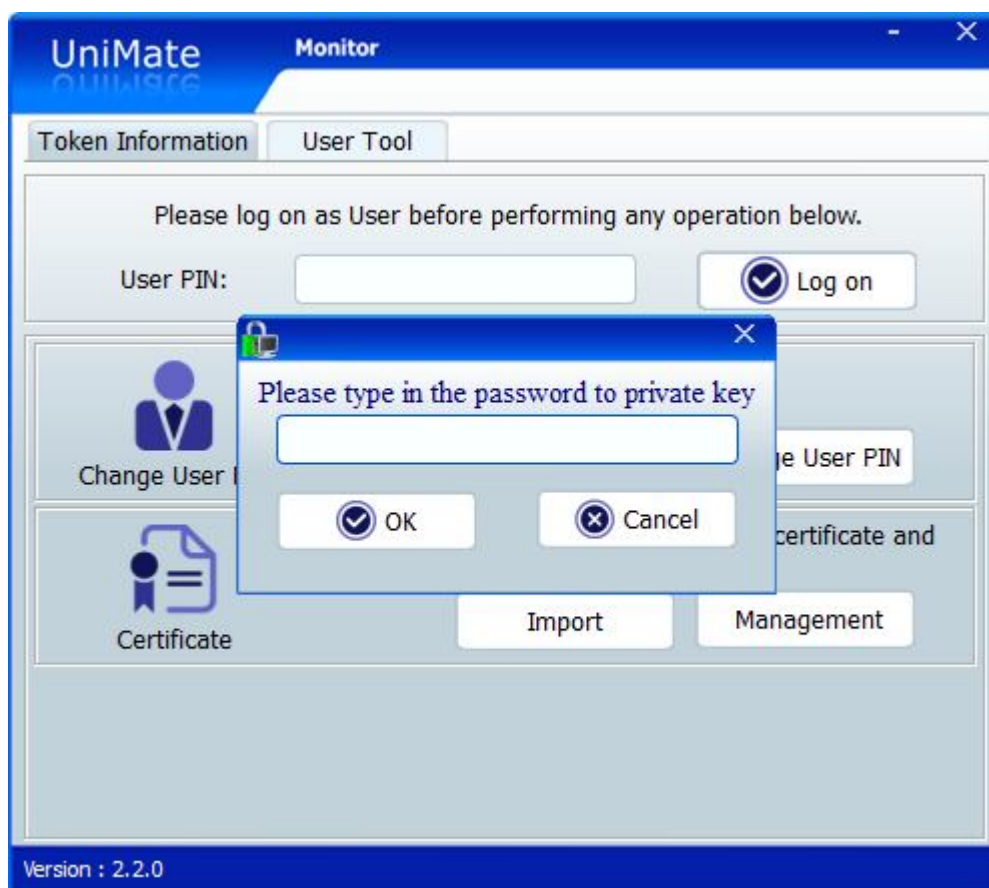




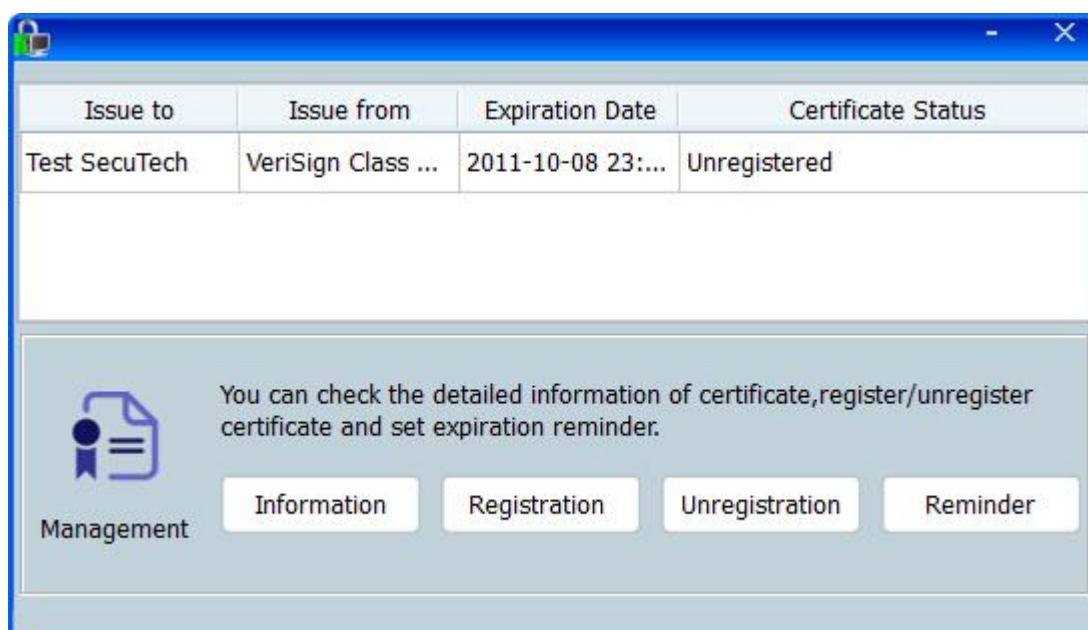
- Change User PIN



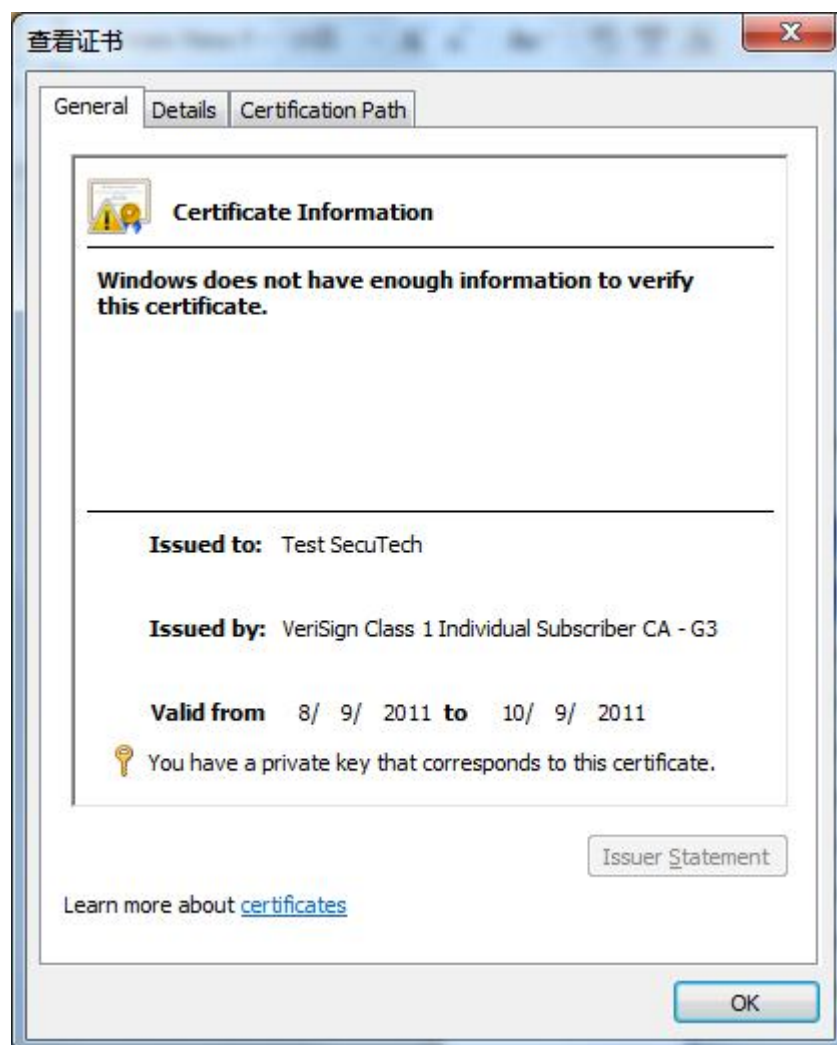
- Import certificate



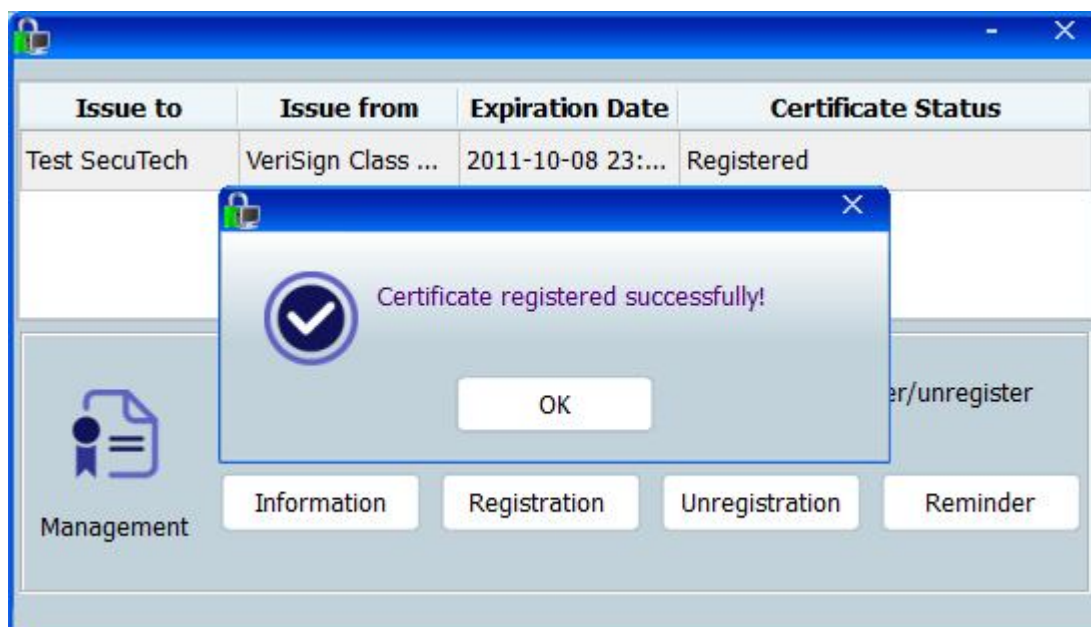
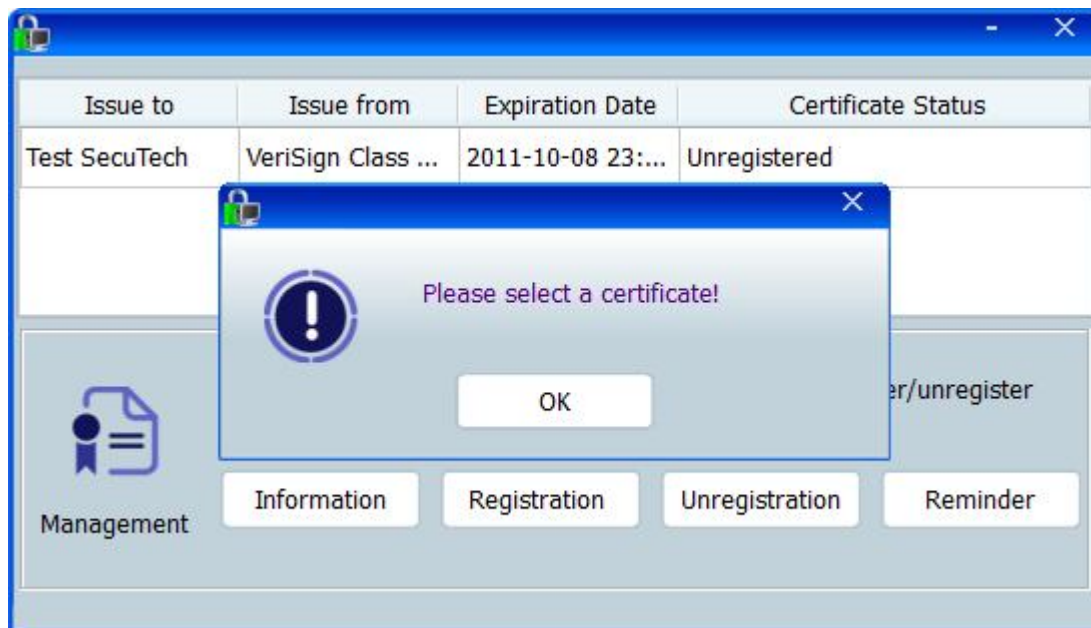
- Certificate Management

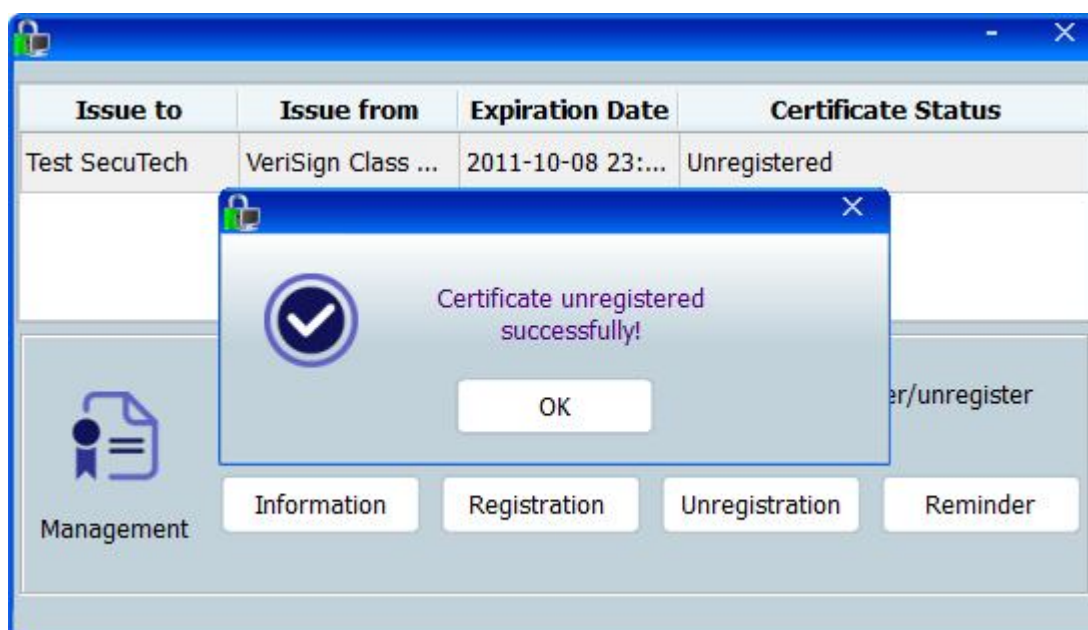


- View Certificate Information

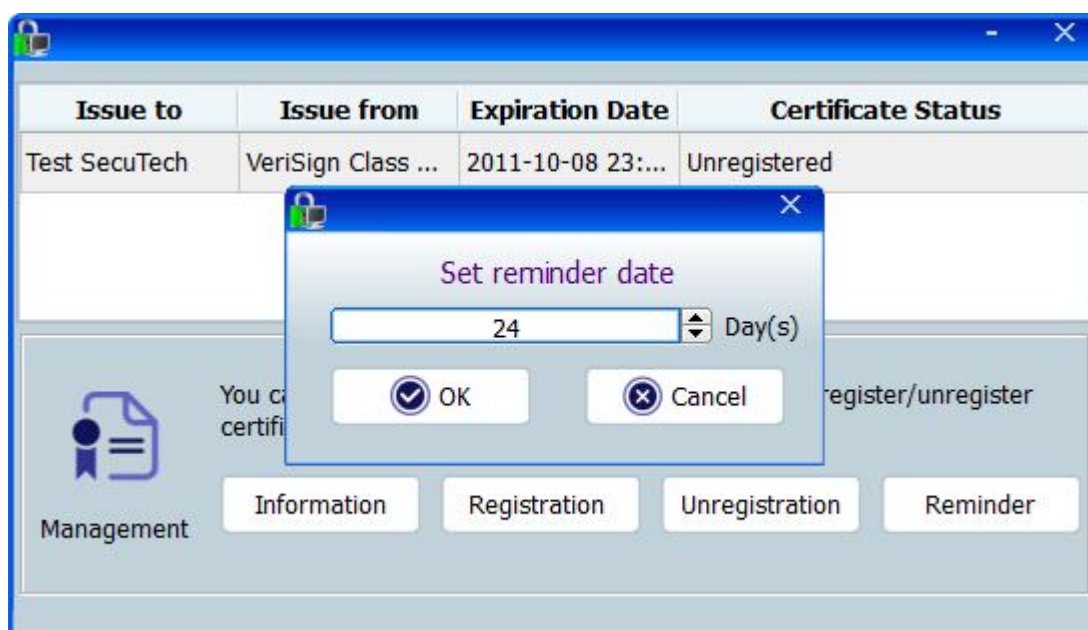


- Register / Unregister Certificate





- Set reminder date



Part 3 Applying Certificates with UniMate

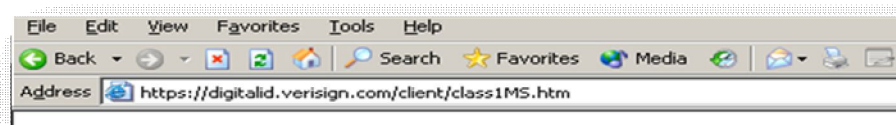
3.1 Applying Digital Certificates

UniMate provides a perfect container for digital certificates. UniMate supports X.509 digital certificates. UniMate PKI package is the middleware software, which provides digital certificate usage. (See also 1.4.2)

Digital certificate is used to certify that the UniMate is the right device. Without it, any operation of the UniMate is forbidden. In this part, we will introduce how to apply digital certificates. We will take the VeriSign certificate and Microsoft Certificate for example.

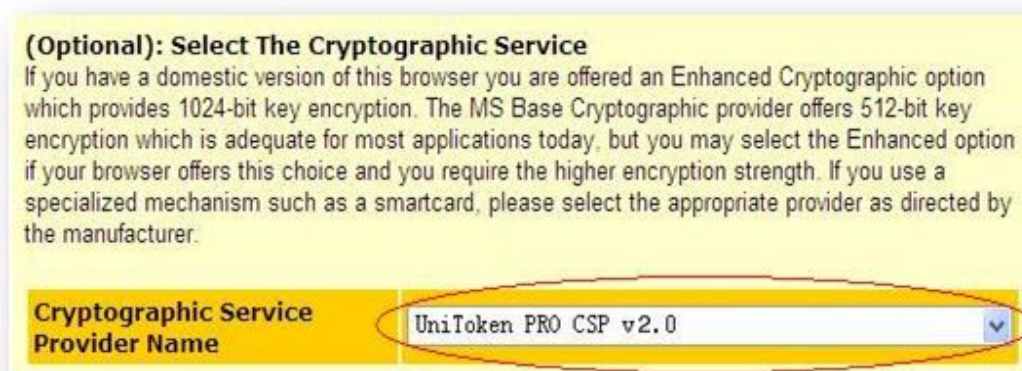
3.1.1 Applying VeriSign Certificates

Insert one UniMate into USB port first, and start IE, type in <https://digitalid.verisign.com/client/class1MS.htm> to open the certificate applying page.



There are four steps for applying a certificate. The page provides comprehensible instructions. It is easy to apply certificates by following the instructions step by step.

In particular, at the step of complete the enrollment, after filling all the information required, select **UniToken PRO CSP v2.0** from the drop down list of Cryptographic Service Provider Name.



Click “Accept” to start processing. In the following steps, you should check e-mail, pick up digital ID and then install the digital ID according to the page tips. RSA encryption key is generated in the UniMate.



If more than one UniMate are inserted in USB ports, please select the UniMate you want to perform this operation. “Logon” dialog box will pop up and User PIN needs to be input.

3.1.2 Applying Microsoft Certificates



Insert one UniMate into USB port first, and start IE to open Microsoft certificate applying page.

This is the home page of the certificate applying site. Firstly, you should click *Request a certificate*.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

And then, select *advanced certificate request*.

Microsoft Certificate Services -- pscST

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

On the page of Advanced Certificate Request, select *create and submit a request to this CA*.

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

For certificate template, select *smartcard logon* in the list; for CSP, select **UniToken PRO CSP v 2.0**

Microsoft Certificate Services -- pscST

Advanced Certificate Request

Certificate Template:

Smartcard Logon

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: UniToken PRO CSP v 2.0

Key Usage: ☒ Signature

Key Size: 1024 Min: 512 Max: 1024 (common key sizes: 512 1024)

☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

☐ Enable strong private key protection

☐ Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Then, a window will appear to ask you to type in UniMate PIN. Click “OK”. The system will generate certificate automatically.

☒ Create new key set ☐ Use existing key set

CSP: UniToken PRO CSP v1.0

Key Usage: ☒ Exchange

Key Size: 1024 Min: 1024 Max: 16384 (common key sizes: 1024 2048 4096 8192 16384)

☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

☐ Enable strong private key protection

☐ Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ☒ CMC ☐ PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

☐ Save request to a file

Attributes:

Verify Pin: UniTokenPro

User Pin: []

OK Cancel


Generating request...

Click “install this certificate” for installation.

Microsoft Certificate Services -- pscST

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

After installation, the system will prompt that certification has been successfully installed.

Microsoft Certificate Services -- pscST

Certificate Installed

Your new certificate has been successfully installed.

3.2 Using Digital Certificates

SecuTech provides a series of solutions about the use of digital certificates, in the aspects of IE, Outlook, PDF, Office and so on.

For the detailed instructions about that, please download relative integration guides from www.eSecuTech.com.

Appendix A Glossary

TERM	DESCRIPTION
AES	Advanced Encryption Standard
API	Application Programming Interface
COM	Component Object Model
Cryptoki	Cryptographic token interface. See PKCS#11.
CSP	Cryptographic Service Provider
DES	Data Encryption Standard.
3DES	Triple Data Encryption Algorithm (TDEA) block cipher
HID	Hardware ID of UniMate
HID	Human Interface Device
HMAC	Hash-based Message Authentication Code, a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key.
MAC	Message Authentication Code, a short piece of information used to authenticate a message
MD5	Message-Digest algorithm 5, a widely used cryptographic hash function
MS-CAPI	Microsoft Cryptographic Application Programming Interface (CryptoAPI or CAPI) standard.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	stands for Rivest, Shamir and Adleman who first publicly described it, an algorithm for public-key cryptography
SDK	Software Developer's Kit.
SHA1	Secure Hash Algorithm1, a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.