

UNIMATE MANUAL

VERSION 1.0



The Key to the Information Security

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

OVERVIEW	1
Chapter 1: UniMate Features	2
1.1 UniMate Drive	2
1.2 UniMate Flex	3
1.3 UniMate USB	4
Chapter 2: Security	7
2.1 PIN	7
2.2 Factory default settings	7
Chapter 3: SDK	8
Chapter 4: Applying Digital Certificates	9
4.1 Applying Microsoft Certificates	9
4.2 Using Digital Certificates	11
Chapter 5: Specifications	12
5.1 UniMate Drive	12
5.2 UniMate Flex	13
5.3 UniMate USB	14
Chapter 6: Frequently Asked Questions	16

Overview

The UniMate device, hereinafter referred to as UniMate, is a mobile authenticator and information security PKI product based on CCID technology (except UniMateDrive) and is a secure container for digital credentials. An advanced processor and secure memory is built into the UniMate device to guarantee the security for exchanging, storing and handling electronic information.

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

UniMate supports PKCS#11, CSP and Value added API (CD-ROM and Partition). Abundant samples provided in the SDK bring ease to integration.

UniMate supports iOS, Android and a multitude of other devices through either a USB port using the CCID protocol or 3.5mm TRRS audio jack.

Chapter 1: UniMate Features

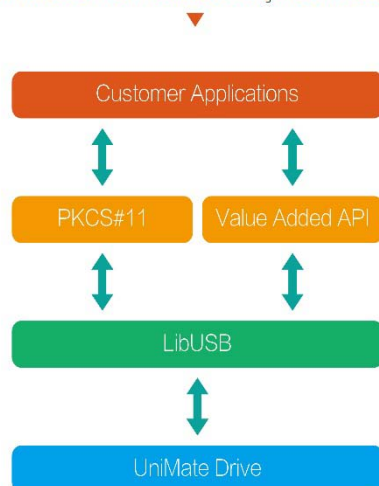
Universal features of UniMate:

- Globally unique hardware ID
- Customizable software ID
- Smartcard-based
- On-board encryption
- Two levels of PIN management mechanism
- A secure file system
- Large memory, up to 64KB
- Stylish and cute case
- Lead free

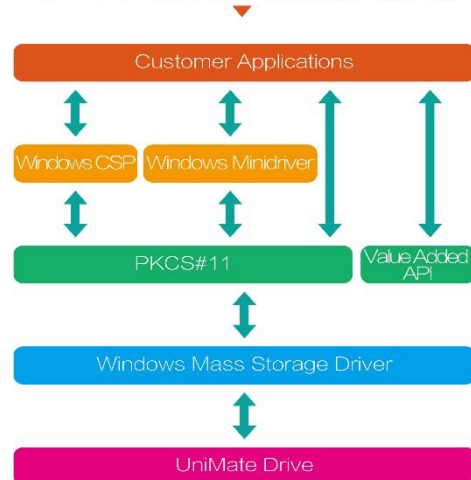
1.1 UniMate Drive

The UniMate Drive is a mobile authenticator and information security PKI product which can store the key certificates. UniMate Drive includes storage district: U-disk and CD-ROM. You can set up the size of storage district using special tool and Value Added library, ISO files can be loaded into CD-ROM. You can also format U-Disk and copy files into it, and so on. The total capacity of UniMate Drive is from 2G to 32G, you can partition it as you wish, UniMate Drive supports PKCS#11, CSP and Value added API (CD-ROM and Partition).

UniMate Drive Architecture (Linux/MacOs)



UniMate Drive Architecture (Windows)



1.2 UniMate Flex

UniMate Flex is an interactive hybrid mobile authentication token designed particularly for use in banking. The two-factor authentication device makes use of a high-performance smart card, a LED display and confirmation buttons to verify the secondary form of authentication. Users can visually confirm transaction information on-screen and press the confirmation button to approve only authorised transactions.

UniMate Flex features PKI based digital certificate and private key storage, as well as on-board encryption, with the ability to generate and store RSA secret key pairs within the key.



1.3 UniMateUSB



UniMate USB is a FIPS 140-2 algorithm certified smart card USB authentication token, and utilises smart card technology for strong authentication. Smart Card technology allows for highly robust authentication and verification solutions.

Organizational Use

Enhanced Business - With secure access in place, organizations can enable business through network connectivity and online services anytime, anywhere, with confidence.

Security - UniMate USB provides robust protection of sensitive business data from unauthorized access.

Cost Effective - UniMate USB reduces password administration costs and losses from data breaches, and provides multiple flexible solutions in one platform.

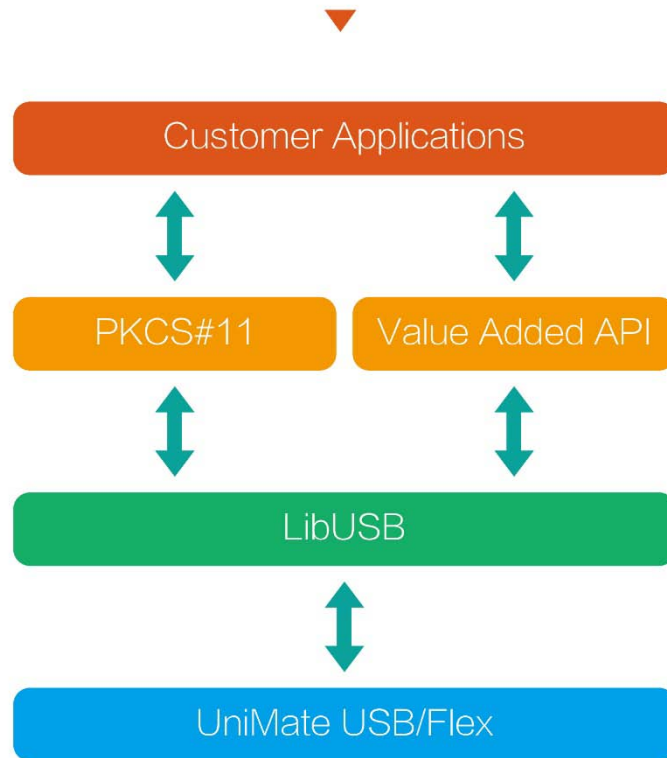
Personal Use

Identity Protection - UniMate USB provides individuals with a secure digital identity protected from theft and abuse.

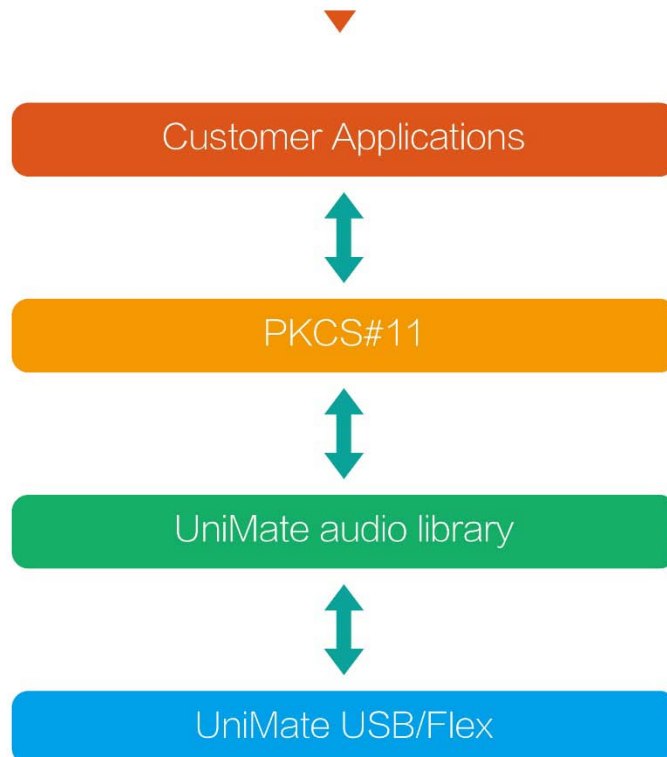
Portability and Convenience - UniMate USB enables users to access their credentials securely wherever they go, whenever they want.



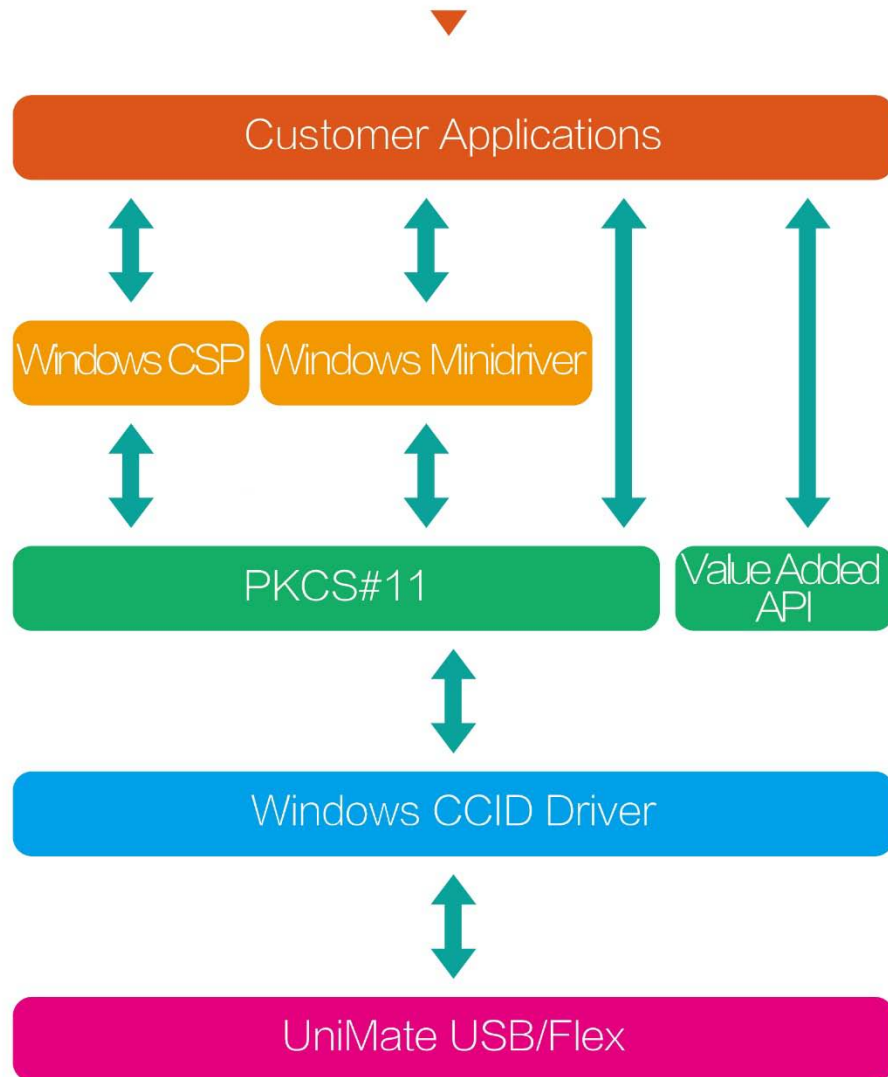
UniMate USB/FLEX Architecture (Linux/MacOs)



UniMate USB/FLEX Architecture (iOS/Android)



UinMate USB/FLEX Architecture (Windows)



Chapter 2: Security

Security is the most important part in the UniMate system, which involves an identification and verification method, including the file access permission control mechanism inside the UniMate, a confidential access system. This security attribute is changed based on the current state of the device, when the card is reset or after the UniMate has finished some commands.

2.1 PIN

The following table describes different key types and use.

PIN Type	Use
User PIN	Directory level authentication. Control different users' read and write permission, generate key pairs, certificate management, sign and so on.
Admin PIN	Ensures the security during the card initialization or is used to reset User PIN/Unlock a user

User PIN: a personal identification number which is firstly hashed and then stored in the device.

Admin PIN: a console identification number.

2.2 Factory default settings

The default User PIN is "11111111" and the default Admin PIN is "00000000".

Chapter 3: SDK

Components	Description
CSP(MS-CAPI)	Declaration of the standardized identifiers and interface of CSP; CSP libraries; Redists /PKI package.exe Samples for CSP; CSP Manual.pdf
Documents	Manual.pdf(UniMate manual)
PKCS#11	Declaration of the standardized identifiers and interface of PKCS; PKCS libraries; Samples for PKCS; PKCS#11.pdf
Utilities	Utilities Installation(Console setup.exe , Monitor setup.exe) and Utilities Manual.
Value Added API	Declaration of the standardized identifiers and interface of Value Added API; Value Added API libraries; Samples for Value Added API; API Manual.pdf
Quick Start.pdf	Product Overview, Software introduction, Utilities introduction and Factory default settings should be included in the File.
ReadMe.txt	Change log

Chapter 4: Applying Digital Certificates

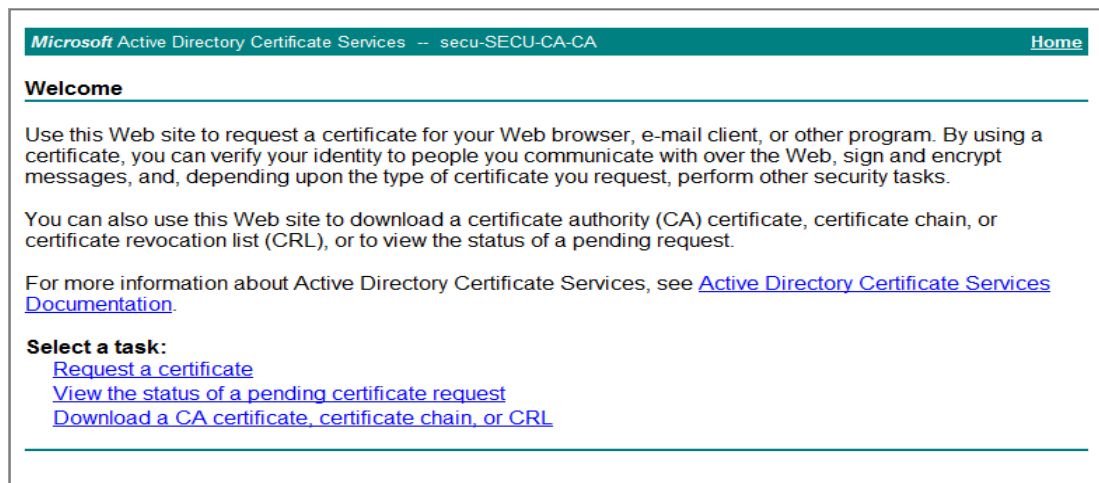
UniMate provides a perfect container for digital certificates, supporting X.509 digital certificates. UniMate PKI package is the middleware software, which provides digital certificate usage.

A digital certificate and authenticated access is needed to be used with the UniMate. Without it, any operation on the UniMate is forbidden. In this part, we will introduce how to apply digital certificates. We will take the VeriSign certificate and Microsoft Certificate as examples.

4.1 Applying Microsoft Certificates



Insert a UniMate into the 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.



And then, select advanced certificate request.

Microsoft Active Directory Certificate Services -- secu-SECU-CA-CA
Home

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.

Microsoft Active Directory Certificate Services -- secu-SECU-CA-CA
Home

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 a certificate template, select Smartcard User in the list; for CSP, select UniMateDRIVE CSP v2.0.

Microsoft Active Directory Certificate Services -- secu-SECU-CA-CA
Home

Advanced Certificate Request

Certificate Template:

Smartcard User

Key Options:

☒ Create new key set
☐ Use existing key set

CSP: UniMate DRIVE CSP v2.0

You may have selected a CSP that does not support the key type defined in the template. Please modify the key type in the template or select either different CSP or certificate template.

Key Usage:

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

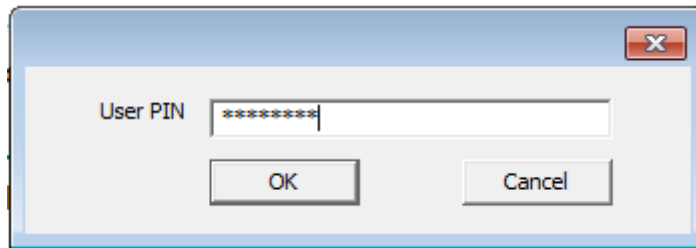
☒ Automatic key container name
☐ User specified key container name

☐ Mark keys as exportable

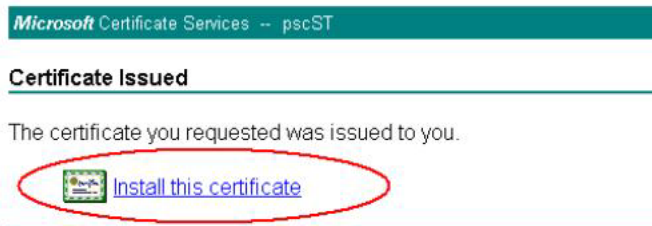
☐ Enable strong private key protection

Additional Options:

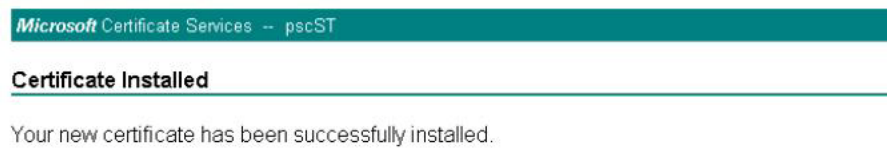
Then, a window will appear to ask you to type in your UniMate's PIN. Click "OK". The system will generate a certificate automatically.



Click "install this certificate" for installation.



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



4.2 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.

Chapter 5: Specifications

5.1 UniMate Drive

Key feactures	
Driverless Operation 2GB, 4GB, 8GB, 16GB and 32GB	
Seletive Mass Storage	virtual CD-ROM 和 general
Dimensions	57×16×8 mm
Weight	9g
Min. Operating Voltage	5V
Current Consumption	<= 50 mA
Operation Temperature	0℃ to 70℃
Storage Temperature	-10℃ to 85℃
Humidity Rate	0-70% without condensation
Casing	Tamper-evident Metal
Memory Data Retention	At least 10 years
Memory Cell Rewriters	At least 100,000 times
PKI	PKCS#11, MS-CAPI
Onboard Encryption Algorithms	2048-bit RSA 1024-bit RSA 128-bit AES 192-bit AES 64-bit DES 64-bit TDES
Onboard Hashing	160-bit SHA
Operating System Compatibility	Windows 2000,XP,2003,Vista,7,8, Server 2008,Server 2012 and Linux

5.2 UniMate Flex

Hardware	
Dimensions	65×36×11.4 mm
Weight	23g
Audio Interface	3.5mm TRRS
USB Interface	USB Type A
Display	LCD
Hardware ID	64-bit Globally Unique
Internal Memory	> 16KB
Mobile Device Software	Audio Authentication Interface
Casing	Tamper-evident Metal
Middleware	PKCS#11
	MS-CAPI
	Audio Authentication API
	X.509 Digital Certificate
Performance	
Min. Operating Voltage	5V
Current Consumption	≤ 50 mA
Operation Temperature	0°C to 70°C
Storage Temperature	-10°C to 85°C
Humidity Rate	0-70% without condensation
Memory Data Retention	At least 10 years
Memory Cell Rewriters	At least 100,000 times
Supported Platforms	Mobile OS: iOS, Android, Symbian, Windows Phone PC: Windows, Linux, Mac OSX

5.3 UniMate USB

Key Features	
PKI token with CCID interface	
Embedded Smart Card	
Three-level Permission System	
Three-level Permission System	
Secure File System	
Auto-lock Mechanism	
MS-CAPI, PKCS#11, X.509 v3 Standard Compliant	
Globally Unique Hardware ID (32-bit)	
User-Defined Token ID	
Lead-Free	
Robust Case	
Hardware	
Dimensions	57×16×8 mm
Weight	9 g
Interface	USB
Performance	
Min. Operating Voltage	5V
Current Consumption	<= 50 mA
Operation Temperature	0°C to 70°C
Storage Temperature	-10°C to 85°C
Humidity Rate	0-70% without condensation
PKI	PKCS#11, MS-CAPI
Onboard	2048-bit RSA 1024-bit RSA 128-bit AES 192-bit AES 64-bit

Encryption Algorithms	DES 64-bit TDES
Onboard Hashing	160-bit SHA
Supported Platforms	Windows2000,XP,2003,Vista,7,8,Server 2008,Server 2012 and Linux
Software Developers	- UniMate USB API libraries in Windows, Linux
	UniMate USB Console for management of UniMate USB devices
	UniMate USB PKI middleware for PKCS# 11 and MS-CAPI applications
	UniMate USB IE ActiveX Control, Firefox Plugin
Software - Users	UniMate USB Monitor for registration and management of user digital certificates

Chapter 6: Frequently Asked Questions

6.1.1 What is UniMate?

UniMate is SecuTech's mobile authentication product family focusing on secure transaction authentication and platform inter-changeability by employing two-factor authentication.

6.1.2 How does UniMate work?

UniMate authentication utilises PKI technology, where certificates are securely stored within the UniMate device and are inaccessible without the appropriate permissions to interact with the device.

The TRRS audio port found on most mobile devices is used for secure communication during use of the device, in addition to providing a micro USB interface for use and configuration on the desktop platform.

6.1.3 What is PKI?

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

6.1.4 What Algorithms is supported?

UniMate supports 2048-bit RSA, 1024-bit RSA, 128-bit AES, 192-bit AES, 64-bit DES, 64-bit TDES.

6.1.5 What is middleware?

The middleware contains PKCS#11, MS-CAPI, Audio Authentication API and X.509 Digital Certificate.

6.1.6 What is the default PIN?

The default Admin PIN is eight zeros, or "00000000", the default User PIN is eight ones, or "11111111", without quotation marks.

6.1.7 Where can I receive further assistance?

If you have any questions, please feel free to contact us

at <http://www.esecutech.com/support> or support@esecutech.com.

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

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. SecuTechUniMate 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.