

UniMate

FLEX



UniMate



UniMate

STD

UniMate® Quick Start

USB(Mini) | Drive

Support: <http://www.eSecuTech.com/support>

Email: Support@eSecuTech.com

Website: www.eSecuTech.com

Wiki: www.eSecuTech.com/wiki



UniMate USB (Mini)

- CCID
- FIPS Certificated
- On-Demand Partition
- Smart Card
- PKCS#11 Supported
- MS-CAPI Supported
- X.509 Certificate Supported
- Globally Unique Hardware ID
- 3-Level Permission Management
- Secure Memory
- Highly Configurable



UniMate Drive

- Selective Mass Storage
- Two-Factor Authentication
- High-performance COS
- Multi-Level Permission Management
- Secure File System
- Normal Drive
- Virtual CD-ROM
- Highly Configurable

SecuTech Warranty Policy

When you buy a product from SecuTech, the product comes with guarantees that cannot be excluded under Australian consumer law.

You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage.

You also are entitled to have the products repaired or replaced if the products fail to be of acceptable quality and the failure does not amount to a major failure.

The relevant guarantees are as follows:

- **Quality** – Products supplied by SecuTech must be of acceptable quality. The test for acceptable quality is whether a reasonable person, fully aware of the state and condition of the products, would find them
 - ✓ **Safe**, durable, and free from defects;
 - ✓ **Acceptable** in appearance and finish; and
 - ✓ **Fit** for all the purposes for which goods of what kind are commonly supplied.

This must take into account the nature and price of the products, and any statements on packaging or labeling.

- **Disclosed purpose** – Products or services supplied by SecuTech that SecuTech represents are reasonably

fit for a purpose expressly disclosed by a consumer.

- **Description** – Products supplied by SecuTech must match the description provided by SecuTech.
- **Sample** – Products supplied by SecuTech must match any sample shown to you by SecuTech.
- **Title** – A customer who purchases a product from SecuTech must receive clear title to the product.
- **Due Care and Skill** – Services provided to you by SecuTech must be provided with due care and skill.
- **Express warranties** – SecuTech will be legally required to comply with the express warranty that is set out in its items and conditions.
- **Reasonable time** – Repair services provided by SecuTech must be provided within a reasonable time.

If you think you are entitled to any of the above remedies, please contact SecuTech at sales@eSecuTech.com

For further information on consumer rights, visit www.consumerlaw.gov.au and www.accc.gov.au/consumerguarantees

1. Contents
2. Product Overview
3. Remarks
4. SDK Contents
5. Preparation
 - For computer
 - For mobile device
6. Secure Mobile Payment Solution
7. Benefits of UniMate
8. Utilities
 - For Windows Users
 - For Linux Users
10. OEM Customization
11. Frequently Asked Questions



Product Overview

- **UniMate USB/Mini**

UniMate USB/Mini is a FIPS 140-2 algorithm certified smart card USB authentication token, and utilizes smart card technology for strong authentication. Smart card technology allows for highly robust authentication and verification solutions. Available in mini formats.

- **UniMate Drive**

UniMate Drive is an authentication token with mass storage empowering software vendors with the flexibility to choose the level of protection and types of licensing as well as providing 2 different types of drive emulation: a normal partition (read and write) and a Virtual CD-ROM (read only) partition.



Remarks

- Please refer to the manuals within the documents directory of the SDK for in-depth information regarding UniMate Utilities, procedures and associated information. Additional resources can be obtained from our Wiki page (www.eSecuTech.com/wiki).
- Please read the ReadMe file located in the root directory of the SDK (SDK/ReadMe.txt) for information on usage and further development.
- Please read the tool-specific ReadMe file located in each tool-specific directory before use.
- Console and Monitor tools in the SDK is needed for use. The Partition tool (only for UniMate Drive) is designed to run without the need to be installed on your OS.
- For technical assistance, email (Support@eSecuTech.com) or by opening a ticket at (www.eSecuTech.com/support).
- UniMate requires the installation of the PKI package to operate on a computer.
- The UniMate app must be downloaded and installed on the mobile device from the app store.





SDK Contents

SDK Contents

After obtaining a copy of the UniMate SDK, please read the ReadMe file located in the root directory of the UniMate SDK.

The following is an outline of the folder contents in the UniMate SDK:

CSP(MS-CAP): Declaration of the standardized identifiers and interface of CSP; CSP libraries; Redists/PKI package.exe;

Samples for CSP; CSP Manual.pdf.

Documents: 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 Partition.exe (Only for UniMate Drive)

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

ReadMe.txt

Preparation

For computer:

- Install the PKI package onto your computer.
- Connect the UniMate to the computer with the Micro to USB Type A cable provided. The UniMate device is ready when the LED light is on and the UniMate Monitor tool detects the UniMate.
- To access the UniMate, input the PIN code, the default Admin PIN is “00000000”, the default User PIN is “11111111”, without quotation marks.

For mobile device:

- Download and install the UniMate app.
- Connect a charged UniMate to the mobile device via the audio port and access it within the UniMate app.



Secure Mobile Payment Solution

Secure Mobile Payment Solution

Mobile devices equipped with UniMate two-factor authentication can safeguard sensitive data from malicious attacks. User verification, cryptographic, offline authorization can be performed by UniMate technology and customers can buy anything at any time and place. All critical security data is stored on the UniMate, instead of on the mobile device and cannot be accessed, significantly thwarting attempts to siphon data.

PKI technology requires a digital certificate and the correct password for the corresponding digital certificate to be entered by the user to complete a transaction. Storing these digital certificates on a UniMate as a second-factor token separate from the mobile device effectively reduces the potential risk of security breaches from malware and man-in-the-middle attacks, as digital certificates stored on the token cannot be exported or otherwise accessed without the appropriate credentials.



Benefits of UniMate

As the mobile platform grows in popularity and in functionality, smart mobile devices will become progressively more mainstream, and with the advent of 4G network connectivity, mobile devices are becoming an ever-increasing integral part of our digital lives. Along with this increased dependence and trust put into mobile devices, so too will the need to protect sensitive and confidential data on our devices. To provide improved security with this new trend in technology, proven methods of protection must be applied.

UniMate brings two-factor authentication to the mobile platform by using a knowledge factor, the password, and a possession factor, the UniMate Device. Comparatively, without UniMate, a sole password can be susceptible to many different security concerns, but with UniMate's hardware encryption capabilities and permission system attacks are drastically impeded. Arming yourself with the UniMate will ensure that your data and interests are safe.





Utilities

For Windows Users

- **1.1 Value Added API**

The API allows for flexible and dynamically customizable integration with UniMate. For application programmers, the API is highly recommended for utilizing your UniMate to its highest potential. The API folder can be found in UniMate SDK/Value Added API.

- **1.2 CSP(MS-CAPI)**

Provides 32-bit and 64-bit library for CSP(MS-CAPI).

- **1.3 PKCS#11 Library**

Provides 32-bit and 64-bit library for PKCS#11.

- **1.4 UniMate Utilities**

The UniMate Monitor tool and Console tool let you access your UniMate in a desktop environment, allowing you to perform administrative tasks such as changing the user PIN or viewing/modifying the stored certificates.

The Partition tool (only for UniMate Drive) allows you to partition the drive.

For Linux Users (Ubuntu 10.04 and higher)

- **2.1 Value Added API**

The API allows for flexible and dynamically customizable integration with UniMate. For application programmers, the API is highly recommended for utilizing your UniMate to its highest potential. The API folder can be found in UniMate SDK/Value Added API.

- **2.2 PKCS#11 API**








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 applications via UniMate middleware.



OEM Customization

UniMate Customization

UniMate products come with a wide range of OEM customization options to suit your business' many needs. Some of these customization options include: **Logo** laser engraving, **Case** design/modification options, custom **Color** options, as well as custom **HID/Device** naming service.

	Logo Customization	With a customer specific logo, you can get company specific branding according to your corporate identity and improve the recognition of your product.
	Case Options	Metal case with your own color, logo and a unique serial number.
	Color Options	Any color in the color palette is available for the case customization.
	Device Naming Service	With the device naming service, you can get company specific branding according to your corporate identity and improve the recognition of your product.
	CSP Naming Service	CSP (cryptographic service provider) name can be under a custom name and improve the recognition of your product.
	Encryption algorithm customization	The customized encryption algorithm might be developed by SecuTech and embedded to UniToken products to meet various local standards.
	Display option	A special welcome splash or a standby display can be customized under a customer's request.

Frequently Asked Questions



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.

How does UniMate work?

UniMate authentication utilizes 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 a desktop platform.

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.

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.

Why use UniMate?

Using UniMate is safer than using a static password alone, as authentication requires two factors. The first is the physical UniMate device itself, which contains the digital certificate used during the authentication process.

The second factor is the password to log onto the UniMate device before beginning the transaction process. Adding these factors into the authentication process make it substantially more difficult to gain unauthorized access in comparison to only one factor, such as a static password.

What should I do if my UniMate is locked?

If the user account associated with your UniMate device is locked, please contact the administrator to unlock your user account.

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.



SecuTech is a global leader in providing strong authentication and software licensing management solutions for Fortune 500 global corporations and government agencies. SecuTech's comprehensive solutions focus on the protection of intellectual property, to assorted strong USB, TRRS and Apple Dock PKI authentication solutions across desktops and mobile platforms. Hundreds of customers, including commercial enterprises and government agencies have chosen SecuTech's solutions and products to control and protect access to invaluable data.