



# UniMate

## Quick Start

STD | FLEX

# UniMate

SecuTech Solution Inc.

Website: [www.eSecuTech.com](http://www.eSecuTech.com)

Support: [Support@eSecuTech.com](mailto:Support@eSecuTech.com)



### UniMate STD

- Connect and authenticate
- TRRS audio and USB hybrid interface
- Host-device communication encrypted
- Onboard smart card technology
- Rechargeable
- Globally unique hardware ID



### UniMate Flex

- Connect, interact and authenticate
- Inbuilt LED screen
- Transaction confirmation button
- TRRS audio and USB hybrid interface
- Onboard smart card technology
- Rechargeable
- Globally unique Hardware ID

# Table of Contents

0. UniMate Family
1. Table of Contents
2. Product Overview
3. Remarks for STD and Flex  
Checklist  
Preparation
4. General Guide to the SDK  
Integration
5. Secure Mobile Payment Solution  
Benefits of UniMate
6. Platform Specific Guide
7. FAQ

# Product Overview

- **UniMate STD** is a simple and compact two-factor mobile authentication token, the first of its kind to operate using the 3.5 mm TRRS audio interface. Users simply connect the device to their mobile device to confirm a transaction. UniMate STD can be used to provide strong authentication and transaction signature services, with ease, for mobile devices.

Using the onboard high performance smart card, UniMate STD can perform advanced algorithms such as 1024/2048 bit RSA, DES, 3DES encryption algorithms and hashing algorithms.

- **UniMate Flex** is a two-factor mobile authentication token providing input and output for greater security requirements. Users can visually verify transactions on the device through an inbuilt LED screen and confirm or cancel the transaction using the confirmation buttons, drastically reducing the risk of unauthorised transactions. UniMate Flex possesses the same onboard high performance smart card functionality as UniMate STD.

# Remarks for STD, Flex

- 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.
- Please read the Readme file located in the root directory of the UniMate SDK regarding information for usage and further development.
- Please consult the UniMate manual for in-depth integration and usage details of the UniMate.

## Checklist

The UniMate SDK includes

- The UniMate device and Micro to USB Type A cable
- UniMate PKI package and libraries for iOS and Android
- UniMate brochures, datasheets and manual
- UniMate Quick Start Guide

# Preparation

On computer:

- Install the PKI package onto your computer.
- Connect the UniMate STD/Flex 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, by default “00000000”.

On the 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.

# General Guide to the SDK

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 folders contents in the UniMate SDK:

- Documents: Contains product information, technical datasheets and the manual.
- Android/iOS: Contains necessary library files for integrating the UniMate with your mobile application, and our demo application for Android and iOS system respectively.
- Windows: contains libraries for integrating the UniMate, samples for code demonstration for the use of the UniMate API, and utilities for UniMate device management in Windows system.



# Integration

Integrating UniMate with a mobile device begins with the mobile application. To utilise two factor authentication with mobile, an application must be created which handles the internal communications between the two devices.

A SecuTech provided app for UniMate STD and Flex provides simple functionality of importing and management of certificates, however the level of protection afforded by UniMate can be taken much further. Through the use of the API, the ability to bind a mobile app to a particular UniMate device, require a specific UniMate device to be plugged in to run an app or particular functionality, and many other customizations can be achieved, not only for authentication.

# 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 anytime and place. All critical security data is stored on the UniMate, instead on the mobile device and cannot be accessed, thwarting attempts to siphon data significantly.

PKI technology requires a digital certificate and the correct password for the corresponding digital certificate entered by the user to complete a transaction. Storing the digital certificate on 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.

Apps or mobile devices can be bound to a specific UniMate device, preventing certain functions from initiating without the proper UniMate device. Flex's LCD screen provides an additional measure of security, where transaction details to be signed by users are displayed on the screen and allow users to verify the transaction before pressing the confirmation button to sign a transaction.

# 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, permission system and more impede attacks drastically. Arming yourself with the UniMate will ensure that your data and interests are safe.

# Platform Specific Guide

## For Windows Users

- UniMate API

The UniMate API allows for a flexible and dynamically customizable development of integration with UniMate devices. For application programmers, the UniMate API is highly recommended for utilising your UniMate to its highest potential. The UniMate API folder can be found in UniMate SDK/Windows/Library.

- UniMate Monitor

The UniMate Monitor tool lets 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.

## For Android & iOS Users

UniMate currently supports iOS and Android in Objective C and C respectively. Developer can find the corresponding library from UniMate SDK/Android (or iOS)/Library respectively.

### SDK\_Show

For each mobile system, SecuTech provides a demo application named SDK\_Show to help developers learn integration of their application with UniMate quickly and easily.

# Frequently Asked Questions

## 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.

## 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.

## 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.

4. What is the default PIN?

The default PIN is eight zeros, or "00000000", without quotation marks.

5. 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 for unauthorised access than with only one factor, such as a password alone.

6. 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.

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](mailto:support@esecutech.com).