

# UniToken<sup>®</sup> Quick Start

PRO | DRIVE | CCID



# UniToken Family 0



## UniToken CCID

- FIPS 140-2 level2 Compliant
- Chip Card Interface Device (CCID)
- Smart Card Technology (High Performance 32bit Chip)
- On Board Encryption Process (All above)
- MS-CAPI/PKCS#11 Minidriver
- X.509 Certificate Standard
- API (for numerous platforms)
- 2MB Virtual CD-ROM Embedded
- Customization Service



## UniToken DRIVE

- Secure Mass Storage/Flash Memory
- Smart Card Technology
- On Board Encryption Process (RSA, AES, 3DS, MD5 & SHA-1)
- MS-CAPI/PKCS#11 Minidriver
- X.509 Certificate Standard
- API (for numerous platforms)
- Customization Service



## UniToken PRO

- Smart Card Technology
- Cryptographically Optimized
- On-board RSA, AES, 3DS, MD5 & SHA-1 Encryption Algorithms
- Browser Plug-ins for Web Authentication
- MS-CAPI/PKCS#11 Minidriver
- X.509 Certificate Standard
- API (for numerous platforms)
- Customization Service



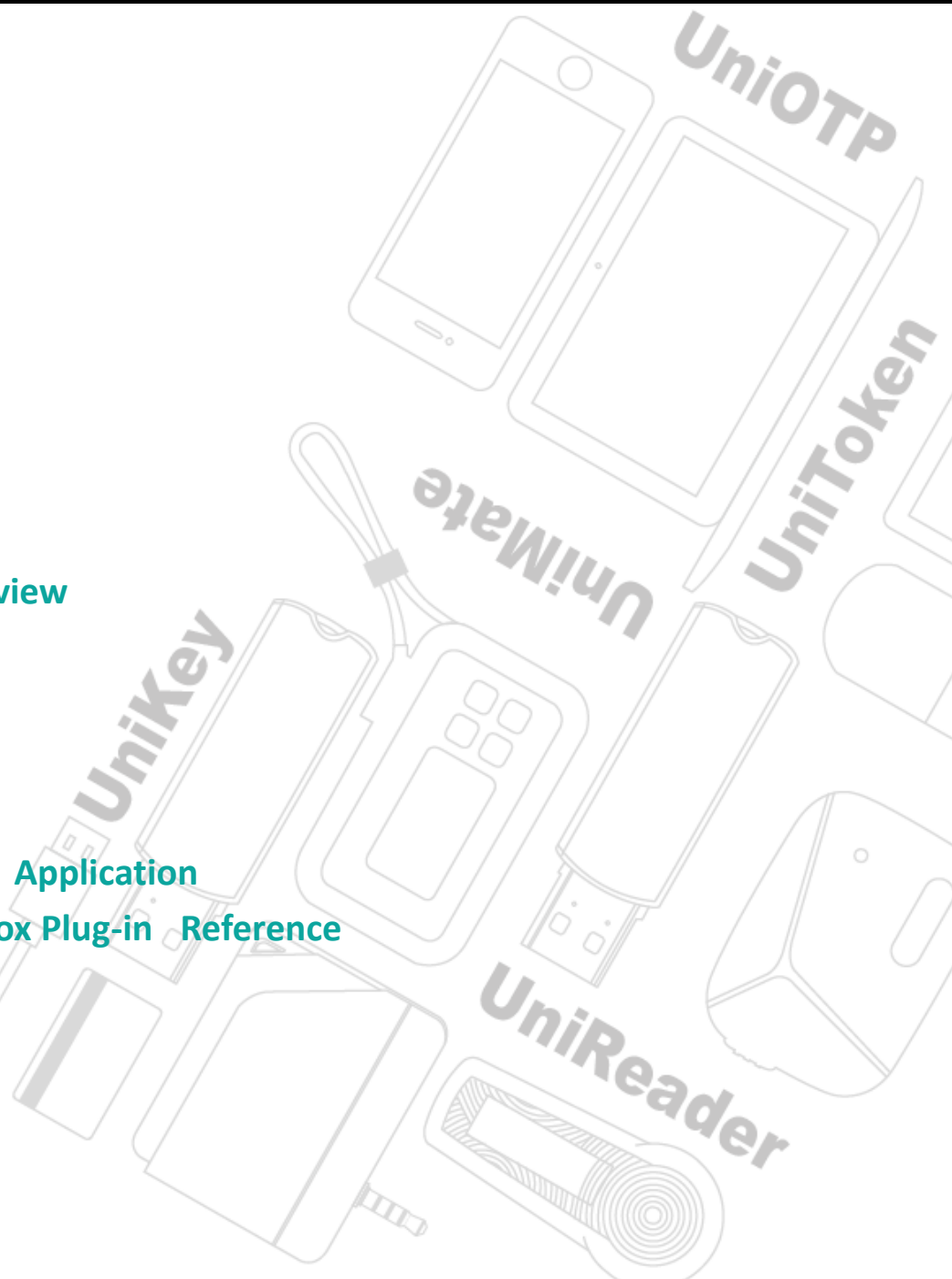
## UniToken STD (Legacy)

- Two-Factor Driverless USB Authentication
- Three-Level Permission System
- Secure Credential Storage
- MS-CAPI/PKCS#11 Compliant
- X.509 Certificate Standard
- Self Lock Capability
- API (for numerous platforms)
- Customization Service



# Contents 1

1. Contents
2. Product overview
2. [Product Overview](#)
3. Remarks
3. SDK Checklist
3. Preparation
4. UniToken PRO, DRIVE, CCID
4. [Software Development Kit Overview](#)
5. [UniToken Software](#)
5. [UniToken Drive](#)
6. Integration
6. [UniToken Certificate Integration](#)
6. [UniToken PKCS#11 and MS-CAPI Application](#)
6. [UniToken API, Active X and Firefox Plug-in Reference](#)
6. [UniToken Video Tutorials](#)
7. [UniToken Case Solutions](#)
8. OEM Customization
9. Frequently Asked Questions (FAQ)
10. FAQ Continued





# Product Overview 2

- **UniToken** offers various solutions for implementing strong two-factor token authentication. UniToken benefits from driverless operation, which allows for unproblematic yet secure verification of users in web authentication for a wide range of web applications/services, this also includes solutions for network and local authentication. Data stored on the UniToken device is encrypted and unable to be exported, this is enforced with a three-level permission system to ensure strict separation of duties among users. Moreover, a wide host of APIs are available for seamless integration with existing , or custom authentication applications on a wide range of platforms: Windows: XP - 8, Windows Server: 2003 – 2012, Linux as well as MAC OS X 10.5 or above (for CCID drivers).
- **UniToken STD** includes a secure file system for storing digital credentials with an enforced three-level permission scheme, self-locking function (automatic lock/shutdown when the incorrect login attempt threshold has been reached), as well as support for MS-CAPI, PKCS#11 AND X.509 certificate standards.
- **UniToken PRO** has the addition of an inbuilt smart card chip which handles smart card authentication, and can perform cryptographic processes – AES, DES, 3DES, RSA, MD5 and SHA-1. UniToken PRO supports web authentication for both Windows Server and Linux.
- **UniToken DRIVE** further contains secure mass storage (flash memory). The mass storage device is partitioned in four parts: normal/public, virtual CD-ROM, password protected & encrypted hidden partition. Partitions can be managed and modified to best suit the users' needs.
- **UniToken CCID** relies on the same principles and authentication methods as the previous UniTokens, however utilizes CCID drivers (instead of HID). CCID drivers work to protect the USB connection and are therefore less susceptible to packet sniffing.



# PRO | Drive | CCID 3

## Remarks

- The UniToken Quick Start Guide serves to cover the features and functions of the UniToken in brief. For detailed information regarding certain aspects of the UniToken, please refer to the UniToken manual, which can be found in the SDK (SDK\Documents\UniToken Manual.pdf) .
- Please read the Readme file located in the root directory of the UniToken SDK regarding information for usage and further development. This is located at (SDK\ReadMe.txt).
- Please read the sample, library specific Readme located in the directory of each respective folder before use.
- Please examine the samples for they will answer frequently asked questions.

## SDK Contents

The UniToken SDK includes

- ✓ Documents, including: Manual, Datasheet and Application References.
- ✓ Libraries, in various programming languages.
- ✓ Samples, in various programming languages.
- ✓ Related UniToken Installers/Redistributables, for Software, Tools and Guides.

## Preparation

- Insert the UniToken dongle into an available USB port. The UniToken device is ready when the LED light is continuously on.
- Make sure you have the appropriate UniToken SDK (CCID, PRO, Drive), which can also be downloaded from our website ([www.esecutech.com/sdk](http://www.esecutech.com/sdk)).
- After the installation of either Developer or End-user Redistributable Package, the UniToken can be accessed or managed through the Console or Monitor tool. Default PIN is “admin” or “user”, for Admin or User respectively .



# PRO | Drive | CCID 4

## Software Development Kit (SDK) Overview

After obtaining a copy of the UniToken SDK, please read the Readme file located in the root directory of the SDK (SDK\ReadMe.txt).

The following is an outline of the folders contents in the UniToken SDK:

- **Documents** – Contains product information, data sheets of technical specifications and usage manuals.
- **Include** – Contains declarations of the standardized identifiers and interface of PKCS#11.
- **Integration Guides** – Contains numerous guides on integrating the UniToken with other corresponding applications.
- **Libraries** – Contains multiple libraries for programming languages (API) supported by UniToken.
- **Redist** – Contains the redistributable packages for developers and end users which provide UniToken PKI application support.
- **Samples** – Contains sample applications that outline the UniToken's functions and usage within several programming languages (API). They provide a brief guide on the implementation and usage within the development environment of your choosing.
- **Web Authentication** – Contains the respective files, utilities, text and video guides on integrating UniToken with corresponding web applications.

**Note that the above outline corresponds to the UniToken PRO SDK layout, and while other SDK's from the UniToken family may omit certain features, the above outline reflects the majority of the UniTokens' SDK contents.**



# PRO | Drive | CCID 5

## UniToken Software

To simplify the operation of UniToken devices, two utilities are provided for the configuration and management of UniToken devices: Console and Monitor. In short, the Console tool is concerned with managing the different permission levels, files, certificates and performing administrator operations. The Monitor tool is used for viewing certificates and applicable information, such as registration and token information.

## UniToken Drive

For UniToken Drive, storage is divided in four partitions: Normal/Public, Virtual CD-ROM, Password protected and Hidden partition.

- The Normal/Public partition functions as a normal mass storage device.
- The Virtual CD-ROM partition functions as read-only access.
- The Password protected partition requires the correct password before data can be accessed within the encrypted partition of the drive. This is best suited for storing confidential information or data.
- The Hidden partition can only be accessed through the use of the API and the correct password from the user, thus gaining access to the stored data without using the OS's file explorer.



# Integration 6

## UniToken Certificate Integration

The use of UniToken for authentication in Adobe PDF files, FreeOTFE, GINA Logon, Microsoft Office 2003 Documents/Spreadsheets , Outlook Mail, TrueCrypt Keyfiles, Windows Smart Card Logon and more can be achieved through UniToken's management of digital certificates.

To obtain documentation specific to a certain application, please locate or download the relative integration guides from the SDK (SDK\Integration Guides), or our website ([www.esecutech.com](http://www.esecutech.com)).

## UniToken PKCS#11 and MS-CAPI usage

For PKCS#11 and MS-CAPI usage, please refer to the UniToken Manual found within the SDK (SDK\Documents\UniToken Manual.pdf).

## UniToken API, Active X and Firefox Plug-in Reference

Reference for usage of UniToken API, Active X and Firefox Plugin integration can be found in the SDK (SDK\Documents).

## Video Tutorials

Short video guides are available within the SDK (SDK\Web Authentication\Video Tutorial Guides).





# Integration 7

## UniToken Case Solutions

### **Windows Server 2003, 2008 Smart Card Logon (UniToken Pro, Drive, CCID)**

Enables two-factor authentication on Windows 2003, 2008 Active Directory Domain with the utilization of the UniToken Smart Card Chip. Guides elaborating configuration options (for Windows XP – 8, Server 2003 -2012) can be found in the SDK.

### **BitLocker Hard Disk Encryption (UniToken, PRO, Drive, CCID)**

Encrypted Hard Disks with BitLocker utilizing UniToken's Smart Card Chip. Guides elaborating how to encrypt a partition or an entire drive with BitLocker can be found in the SDK.

### **Adobe PDF Document Encryption**

Encrypting Adobe Portable Document Format files with a second factor authenticator (digital certificates), is possible with the UniToken. Corresponding guides can be found in the SDK.

### **Outlook Express Email Signature and Encryption**

Sign and encrypt Outlook Express emails with the storage of certificates on UniToken. Corresponding guides can be found in the SDK.

### **Microsoft Word/Excel 2003 encryption**







Either password-protect or wholly encrypt (using digital certificates) Microsoft Word documents and Excel workbooks with UniToken. Corresponding guides can be found in the SDK.

# OEM Customization 8

## UniToken Customization

UniToken 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 **Colour** options, as well as custom **HID/Device naming** service.

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



# FAQ (Frequently Asked Questions) 9

## 1. What is the default Administrator and User PIN?

The factory default PIN for Administrator is “admin” and for User is “user”.

## 2. My UniToken device is locked. What should I do?

If the UniToken device has locked itself, only the Administrator can Unlock the device. To do so, the administrator must log in and unlock the device through “Unlock”. This function is found under the User tab.

## 3. How many digital certificates can be stored on a single UniToken device?

In general, each UniToken can store two digital certificates.

## 4. What does “driverless” mean?

The UniToken authentication dongle is driverless, meaning the usage of UniToken requires no installation of drivers or additional software. Supported operating systems already possess drivers needed by UniToken to operate (HID and CCID), and are automatically installed upon the first connection of the UniToken device. Thus significantly reducing the problems associated with driver-dependent devices.

## 5. Which redistributable package should I use?

For the software developer, please install the developer’s package. This provides full support and administrator tools/options. For end users, please install the end user’s package. This does not include any administrator options.

## 6. What programming interfaces (API) does UniToken support?

UniToken supports PKCS#11, MS-CAPI and UniToken specific API’s.



# FAQ (Frequently Asked Questions) 10

## 7. What encryption algorithms does UniToken Support?

UniToken supports RSA, AES and 3DS encryption algorithms, as well as MD5 & SHA-1 hashing algorithms.

## 8. Can I use UniToken for Smart Card login?

Yes, installing the PKI redistributable package allows you to perform Windows Smart Card Authentication with UniToken.

## 9. What steps does SecuTech take to ensure UniToken is environmentally sustainable?

SecuTech is committed to supplying products that are environmentally friendly. The production process and all parts within the UniToken are lead-free and ROHS-compliant.

## 10. What is the meaning of the light on the UniToken dongle?

If the LED light on the UniToken device is continually on, it is recognized by the computer and should be functioning correctly. If the LED light on the UniToken is flashing, then the UniToken is not recognized by the computer. If this is the case, reconnect the UniToken device through the USB connection. If this persists, contact **SecuTech Support**.

## 11. Where can I receive further support?

We, at SecuTech, are dedicated to providing high-quality technical support to our customers. If you have any questions, please feel free to contact us at: [www.eSecuTech.com/support](http://www.eSecuTech.com/support) or [support@eSecuTech.com](mailto:support@eSecuTech.com).

# UniToken®

## SecuTech Solution Inc.

Phone: +1-888-259-5825

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

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

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

Wiki: [www.eSecuTech.com/wiki](http://www.eSecuTech.com/wiki)

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 from 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.