



UniToken[®] Drive

A Driverless Smart-card Based Token With Secure Mass Storage

RSA 2048-BIT HARDWARE ENCRYPTION
 MASS SECURE STORAGE
 ON-DEMAND PARTITION

Selective Mass Storage

UniToken Drive covers all of the features of UniToken Pro, with the addition of secure mass storage that can be partitioned on-demand. The four comprising drives are the general, virtual CD-ROM, password-protected and encrypted hidden partitions, the latter two suitable for secure storage, each resizable appropriate to the needs of different users.

Two-Factor Authentication

The two factors of authentication UniToken takes advantage of are known in information security as 'Something You Know', and 'Something You Have'. As such, both the correct password with the correct UniToken Drive device is needed to successfully complete the authenticate process. Other than providing a necessary second factor, UniToken Drive features the ability to generate encryption keys and store passwords, digital certificates and personal credentials within the key.

High-performance Smart Card Based Device

UniToken Drive is based on advanced 32-bit smart card technology,

significantly increasing the difficulty of duplicating credentials. Although RSA encryption is computationally intensive, the smart card based token is optimized to generate RSA encryption key pairs quickly, enabling sophisticated security with minimal hassle and effort.

Multi-level Permission Management

UniToken Drive utilizes three levels of token permission management: Administrator, User and Guest, where Administrator holds the highest permission level, to Guest holding the lowest. Any operation on the token requires explicit permissions, ensuring the security of the device is maintained to users with the appropriate permissions.

Secure File System

In addition to secure authentication, UniToken Drive also provides users with a secure file system. The file system operates using the multi-level protection method, protecting digital credentials with the password scheme. UniToken Drive implements three separate levels of permission: Administrator, User and Guest. Any operation on the UniToken Drive device requires explicit permission, certifying any and all operations on the device are granted to users with the appropriate permissions.

Features	UniToken [®] PRO	UniToken [®] Drive	UniToken [®] CCID
CCID			✓
Secure Mass Storage		✓	
On-demand Partition	✓	✓	✓
Smart-card Based	✓	✓	✓
Onboard Encryption	✓	✓	✓
PKCS#11 Supported	✓	✓	✓
MS-CAPI Supported	✓	✓	✓
X. 509 Certificate Supported	✓	✓	✓
Globally Unique Hardware ID	✓	✓	✓
Customized Token Name	✓	✓	✓
3-Level Permission Management	✓	✓	✓
Customization Service	✓	✓	✓
Secure Memory	✓	✓	✓

Mass Storage

UniToken® Drive embraces all the functions of UniToken® PRO, with a mass storage which can be partitioned on-demand. The four secure partitions are general drive, virtual CD-ROM, password-protected drive and hidden & encrypted drive.



- General Drive**
- Virtual CD-ROM**
- Password-protected Drive**
- Hidden & Encrypted Drive**

Normal Drive

The Normal Partition functions as ordinary memory that can be used to store files and other data. Capacity is as large as 32GB and is customizable upon customers' requests.

Virtual CD-ROM

The Virtual CD-ROM partition is emulated as a CD-ROM disc upon connecting the UniToken Drive. Much in the same way as CD and DVD discs, the contents of the virtual CD-ROM can only be read, ensuring unchanged transfer of data and consistent distribution of software. All files stored in the Virtual CD-ROM partition are protected against unauthorized deletion or modification, guaranteeing the integrity of data.

Password-protected Drive

Only with the correct password are users allowed access the drive. The password-protected partition provides two permission modes: User, authorizing only read operations on the partition; and Administrator, allowing both read and write operations on the partition.

Hidden Encrypted Drive

This partition will not appear in the directory/file explorer of the operating system. The partition can only be accessed through the use of APIs, enabling complete control over operations in the partition such as reading, writing, creating and deleting data. Since the partition is encrypted and concealed to users, it is suitable for storing sensitive data such as credentials.

CUSTOMIZATION 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.

TECHNICAL SPECIFICATIONS

Capacity	
Onboard capacity	32 KB in total
Flash memory	2G, 4G, 8G
Dimensions	57 mm * 16 mm * 8 mm
Weight	9 grams
Temperature	
Operating	0 °C, +70 °C
Storage	-10 °C, +85 °C
Humidity Rate	0-70% without condensation
Min. Operating Voltage	5V
Hardware	USB 2.0 high speed
Operating System Compatibility	Windows 2000, XP, 2003, Vista, 7, 8, Server 2008, 2010 and Linux (both 32 and 64 bits)
Hardware Encryption	
Data	AES Cipher-Block Chained model
Encryption Keys	256-bit Hardware
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 160-bit HMAC_SHA 128-bit MD5 128-bit HMAC_MD5



About SecuTech

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.

Join the conversation

Twitter
Twitter.com/eSecuTech

LinkedIn
<http://www.linkedin.com/company/secutech-solution-inc>

YouTube
<http://www.youtube.com/user/esechutech>

Facebook
<http://www.facebook.com/eSecuTech>

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/F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com