



UniMate® Drive

PKI USB Two Factor Authentication Token with Partitionable Mass Storage

The UniMate® Drive consists of two partitions: a normal partition (read/write) and Virtual CD-ROM partition (read only).

Two-Factor Authentication

As opposed to single-factor authentication, where only a password is required to verify the user's credentials, two-factor authentication requires two separate modes of validation: "something you know" – the password, & "something you have" – the UniMate® device. Both password and the UniMate® device are needed to successfully complete the login process. UniMate® features the ability to generate encryption keys, and store passwords, digital certificates and personal credentials within the token.

High-Performance USB Attached SCSI Protocol (UASP)

The UniMate® device is optimized with the latest USB 3.0 compatible transfer hardware and protocol, to quickly transfer data between devices, while also enabling sophisticated security with minimal hassle and effort.

Multi-Level Permission Management

UniMate® utilizes three levels of token permission management: administrator, user and guest. Administrator holds the highest permission level, and 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 permission level.

Secure File System

The UniMate® device also provides users with a secure file system, which allows users to store credentials and other important information on the token's internal memory (separate from Mass Storage).

On-demand Partition

The available flash memory can be resized and comes in two partitions:

Public: Simple "plug-and-play" token that can be viewed and modified by the OS and user.

Virtual CD-Rom: Data is viewed and stored as a CD-ROM, allowing users to view and read, but not modify any stored content. The integrity of the data is always guaranteed to be intact.

Features	UniMate® Drive
CCID	
Secure Mass Storage	✓
On-Demand Partition	✓
Smart Card	
Onboard Encryption	✓
PKCS#11 Supported	✓
MS-CAPI Supported	✓
X.509 Certificate Supported	✓
Globally Unique Hardware ID	✓
Customized UniMate Name	✓
3-Level Permission Management	✓
Customization Service	✓
Secure Memory	✓

Technical Specifications - UniMate® Drive

Hardware	
Onboard Capacity	> 64 KB
Flash Memory	2GB, 4GB, 8GB, 16GB, 32GB
Dimensions	52.8mm x 17mm x 7mm
Weight	7.2g
Case Material	Tamper-Resistant Metal
Color (Factory Default)	Black
Operating Temperature	0°C to 70°C
Storage Temperature	-10°C to 85°C
Humidity Rate	0-70% without condensation
Min.Operating Voltage	5 V
Current Consumption	150mA
Device Interface	USB 2.0
USB Protocol	USB Attached SCSI Protocol (UASP)
Hardware Algorithms	
PKI Middleware	PKCS#11, MS-CAPI, FIDO
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-1, 160-bit HMAC_SHA, 128-bit MD5, 128-bit HMAC-MD5
Performance Index	
Time For Digital Signing via USB	<0.5s
RSA 1024-bit Key Generation Time	< 3s
RSA 1024-bit Sign Time	< 300ms
RSA 2048-bit Key Generation Time	< 12s
RSA 2048-bit Sign Time	< 500ms
Certifications	
Manufactory	CE/FCC, RoHS
Device Identification	
Hardware ID	Globally-unique
Hardware Encryption Algorithms	AES (ECB 128-bit, 192-bit, 256-bit), AES (CBC 128-bit, 192-bit, 256-bit) DES (ECB), DES (CBC), RSA (1024-bit, 2048-bit), 3DES (ECB), 3DES (CBC)
Hardware Hashing Algorithms	MD5,SHA-1
PKI Support	PKCS#11, MS-CAPI, X.509v3
Memory Cell Rewrites	At least 100,000
Memory Data Retention	At least 10 years
Operating Systems	Windows 98 SE , Windows 2000, Windows ME, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008. Windows 7, Windows 8, Windows 10, Linux (2.2+), FreeBSD (5.x, 6.x, 7.x, 8.x, 9.x), Mac OS X (10.4, 10.5, 10.6), (32-bit and 64-bit all above)
Warranty	
Manufacturing & Material Defects	1 year