

Sensitive and valuable data needs protection. It is especially important in mobile environments, where confidential information is at risk of being accessed by unauthorized personnel. Today, many companies and organizations give their staff mobile devices to increase efficiency. Confidential in-house information such as research results, management analysis or even customer data is stored on these notebooks and PDAs. If this valuable information was on paper, the documents would be kept in locked filing cabinets or safes to protect them from being stolen or read by the wrong people. SafeGuard PrivateDisk gives electronic documents exactly the same protection. SafeGuard PrivateDisk generates an encrypted “virtual” disk drive on the device. This disk is a well-protected electronic safe: Any critical, sensitive and valuable data can be securely encrypted and stored safely on it.

Two versions of SafeGuard PrivateDisk are available: The Personal Edition is designed for use in small and medium-sized companies, while the Enterprise Edition, with its extended configuration and distribution options, is designed to meet the needs of larger organizations.

Many managers and external service staff are now enjoying the benefits of using SafeGuard PrivateDisk Portable: They can read encrypted data on their mobile memory media, wherever they are, while still complying with their company’s security standard. In addition, SafeGuard PrivateDisk Enterprise Edition provides administration tools and interfaces that ensure easy and cost-effective integration into existing IT environments. SafeGuard PrivateDisk can be used as a standalone security solution or can be integrated in an existing PKI (public key infrastructure). In company-wide rollouts, SafeGuard PrivateDisk also supports the use of smartcards for strong authentication access to the file volume.

SafeGuard PrivateDisk—Your electronic safe.

Key benefits

Enhanced security

- » Electronic safe protects valuable and sensitive company data
- » Flexible data protection on networks, local hard disks, terminal servers and portable media
- » Uses tried and tested security algorithms
- » Enterprise Edition also provides recovery certificates, which guarantee that encrypted data can be accessed in an emergency

Easy to deploy

- » Central, uncomplicated installation and distribution via Windows Installer or other software management systems
- » No need for additional upgrades to existing IT infrastructure
- » Scalability: from individual devices up to a company-wide rollout

Easy to use

- » Easy exchange of protected files between PC and PDA platforms guaranteed by complete interoperability
- » Self-explanatory functionality, meaning high levels of user acceptance
- » No time-consuming training required for users or administrators
- » PrivateDisk Portable gives you high flexibility: with it, you can access encrypted data on other end devices, but you don’t need to install it on them
- » Optional integrated key management with SafeGuard Enterprise data security solution enables greater transparency in secure data sharing

Key Features/Functionality

Security

- Generates an automatically encrypted virtual disk drive
- Fast and transparent encryption by simulating an additional disk drive
- Protects data on hard disks, network drives and portable media such as diskettes, CD-ROMs, DVDs, USB drives and flash memory cards
- User authentication via a password and/or X.509 certificates
- Optional shared keyring management with SafeGuard Enterprise enables easy transparent encrypted data exchange within company user groups without the need for separate passwords
- Supports smartcards and USB tokens
- Windows pagefile can be deleted, if required, when the computer is switched off
- Implements the most up-to-date, cutting-edge AES encryption algorithm

System administration

- Cost-effective, quickly implemented solution with no need for extra infrastructure or training
- Windows Installer (MSI)-based installation or installation using other software management systems
- Central administration of security settings via Group Policy Objects
- Optional integration of Recovery Certificates so that encrypted data can also be accessed in an emergency situation

Easy to use

- High level of user acceptance: no need for additional training
- Each user can use several PrivateDisks at one time
- Several authorized users can share one PrivateDisk to store shared information securely
- Users can protect and store any kind of confidential file on their PDA, notebook and PC
- Seamless integration in Windows Explorer
- PrivateDisk Portable allows secure data access (read) on devices without the need to have special software installed

Certification

- » FIPS 140-2 (cryptographic library in evaluation)
- » Aladdin eToken certified
- » Gemalto Secure Digital Companion
- » Interoperability
- » Microsoft Crypto API integration: the use of cryptographic service providers (CSPs) means that any RSA-enabled components from third-party suppliers (such as smartcards or USB tokens) can be implemented for user authentication

System requirements

Hardware

- » PC with an Intel Pentium or compatible processor
- » Pocket PC with an ARM or XScale processor

Operating system

- » Microsoft Windows Vista 64-bit
- » Microsoft Windows Vista
- » Microsoft Windows XP 64-bit
- » Microsoft Windows XP
- » Microsoft Windows 2000
- » Pocket PC 2002/Pocket PC 2002 Phone Edition
- » Windows Mobile 2003/Windows Mobile 2003 Phone Edition

Interfaces

- » Crypto API/Microsoft Cryptographic Service Provider (CSP)
- » Scripting API for integration in automatic administration procedures
- » LDAP (only for Enterprise Edition)

Standards/Protocols

- » Authentication: user authentication via X.509 certificates
- » Encryption: AES (Rijndael)—128 and 256 bit
- » Hash: SHA-1

Language Versions

- » English, German, French, Dutch, Spanish, Portuguese (Portugal and Brazil), Italian, Danish, Swedish, Finnish, Norwegian, Japanese, Chinese, Korean