[SafeGuard® LAN Crypt]

Unique protection for confidential data against access by any unauthorized insider or outsider

Most data protection measures are designed to counter danger from outside a company, while most in-house risks are usually ignored. However, the potential for damage caused by the misuse of confidential company data is exactly the same. In almost every organization, valuable information such as business reports, HR documentation, customer data and research results is saved electronically without being protected. The current practice of saving data centrally on servers, multi-site workplace networking and the use of mobile data media means that security risks are become greater and greater. As more and more organizations outsource their IT departments in an effort to reduce costs, their worries about data confidentiality increase accordingly.

What is needed is a security solution that only lets authorized user groups access sensitive data across an organization. Even in-house system administrators or personnel from the outsourcing company should not be permitted to see confidential data. This is exactly the security issue that **SafeGuard LAN Crypt** is designed to resolve.

It uses fully-automated file encryption to provide effective protection for confidential files. In **SafeGuard LAN Crypt** the roles of System Administrator and Security Administrator are strictly defined, giving it a unique advantage in handling data security. The System Administrator can still manage the system as usual but has no means to decrypt any files. This is because the keys are managed by the Security Administrator who in turn cannot access the stored, encrypted files.

The Security Administrator defines the individual access rights for working groups or individual users in accordance with the company's security guidelines. These access rights are then bundled in encryption profiles. This means that each user is assigned a unique "key group" based on his profile, with which he can read the released files in plain text in the normal way. Unauthorized persons can only see an enciphered, unreadable string of characters.

SafeGuard LAN Crypt does not force users to change the way they work. The encryption process is transparent and runs invisibly in the background. SafeGuard LAN Crypt can be used for different types of memory media, network drives or file servers, hard disks and removable media, and also on terminal servers.

SafeGuard LAN Crypt provides comprehensive protection for all a company's data. It is scalable so it can be used in small temporary teams, in departments and project groups or throughout entire organisations.

SafeGuard LAN Crypt – Intelligent file encryption.

Benefits

Enhanced security

- Transparent data security for user groups and individual users
- Encryption on all standard media and in heterogeneous environments
- Division of power between system and security administration
- Simple implementation of a company-wide security policy
- Flexible definition of encryption rules for user groups
- Uncomplicated PKI integration and support for certificates, smartcards and USB tokens

Easy to deploy

- Seamless integration into heterogeneous IT infrastructures
- Uncomplicated, central administration using existing directories or domains
- No need for additional upgrades to existing IT infrastructure
- Scalable from individual user groups up to a company-wide rollout

Easy to use

- Simple to use by integration in familiar working environments
- Transparency for users
- Self-explanatory functionality, meaning high levels of user acceptance

About Utimaco Safeware

Utimaco developed it's first IT security software in 1983. Today, Utimaco is a global leader in enterprise information security. Using the most advanced techniques, Utimaco software provides unmatched information security. Highly reliable, easy to use, and easy to administer, Utimaco products ensure low total cost of ownership. For more information, visit **www.utimaco.com**.

utimaco® safeware

Key Features/ Functionality

Security

- Comprehensive security solution for preventing unauthorized access to data
- Protects valuable company data and confidential personal information
- Strictly separates system and security administration responsibilities
- Best-possible protection if IT is outsourced because, although outsourcing staff can manage the files, they cannot read them in plain text
- Uses tried and tested security algorithms
- Automatic encryption and decryption in the background
- Protects data on hard disks, network drives and portable media such as diskettes, CD-ROMs, DVDs, ZIP drives, JAZ, MO disks, USB and flash memory cards
- User authentication by X.509 certificates
- Supports smartcards and USB tokens

System administration

- Simple, central installation, configuration and administration through integration in existing IT environments and by using existing directory services (LDAP, Active Directory) or domains
- Uncomplicated integration in existing PKI systems
- No reduction in server performance. Encryption and decryption is only carried out by a filter driver on the devices
- Cost-effective and quickly implementable solution which does not need any additional infrastructure
- Less time and money needed for helpdesk services
- Recovery strategy, so that encrypted data can also be accessed in an emergency situation

Easy to use

- Authorized users can save their shared information securely on their usual memory media without any risk of unauthorized access by outsiders
- No need for changes to their familiar working environments and working habits
- High level of acceptance by users: no additional training required

System Requirements

Hardware

- PC with an Intel Pentium processor or a compatible processor

Operating system

- Microsoft Windows XP
- Microsoft Windows 2000

Supported file server operating systems

- Microsoft Windows
- Novell Netware
- Linux, Unix (Samba)

Supported Terminal Servers

- Microsoft Windows 2000 Terminal Server
- Microsoft Windows 2003 Terminal Server
- Supports Citrix MetaFrame

Certifications

- FIPS 140-2 (cryptographic library in evaluation)
- Aladdin eToken certified

Complementary SafeGuard® Products

- This solution can be used together with SafeGuard® Advanced Security modules to create other supplementary solutions. These can be used, for example, for Multi-Desktop Applications, Single Sign On, Plug & Play Management, and Application Specific Access Rights

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 authentification

Supported media

- Hard disks, network drives, diskettes, CD-ROMs, ZIP drives, USB drives and many others

Interfaces

- ODBC (Database)
- Crypto API
- Microsoft cryptographic service provider (CSP – Token and smart cards)

Standards/ Protocols

- Authentication: user authentication via X.509v3 certificates
- PKCS#12
- LDAP
- Encryption: 3DES 168-bit, IDEA 128-bit, AES 128-bit and 256-bit
- Hash: MD5, SHA-1, SHA-256
- Tokens: smart cards and USB tokens via Crypto API

Language Versions

- English, German

Contact

Utimaco Safeware AG
P.O. Box 20 26
DE-61440 Oberursel
Germany
Phone +49 (61 71) 88-0
Fax +49 (61 71) 88-1010
Info@utimaco.com
www.utimaco.com

More information about SafeGuard LAN Crypt:
www.utimaco.com/SG-LANCrypt

Utimaco Safeware Partner: