



Product



fideAS® file enterprise

fideAS® file enterprise in a nutshell

- Data Leakage Prevention
- Easy and central administration
- Connection to existing directory services via LDAP or Windows adapter
- Centralized software distribution via MSI packets
- Supports smartcards and USB tokens
- Automated encryption of the file system
- Easy integration into existing system environments
- High scalability and system availability through redundant Security Servers
- Emergency function for data recovery
- Integration into terminal server environments possible
- Supports Microsoft DFS

Encryption and Data Leakage Prevention

fideAS® file enterprise is a user-friendly solution for the enterprise-wide protection of sensitive data. Automated encryption, the control of mobile devices and copy protection mechanisms for confidential data converge to a powerful tool for Data Leakage Prevention.

Easiest installation and administration

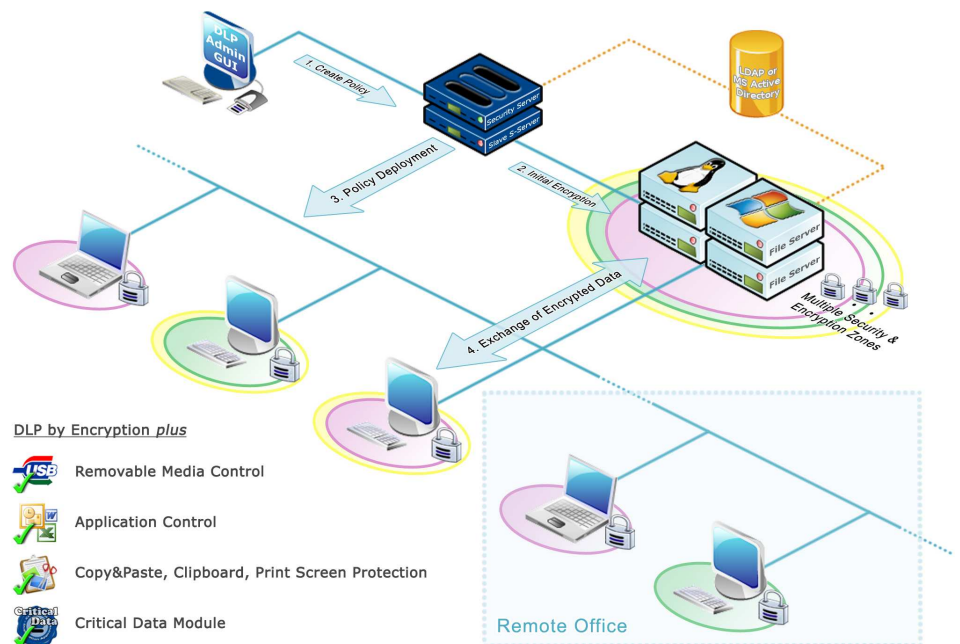
The entire administration of fideAS® file enterprise is performed centrally with the help of a clearly laid out and easy-to-use graphical user interface. The integration with existing directory services like the Microsoft Active Directory renders double user administration unnecessary. Keys and certificates are generated automatically and can be distributed to the users as software keys or on smartcards and USB tokens. The configuration of the file servers remains untouched. Pre-configured MSI packets ensure an easy software distribution via central mechanisms even in large quantities.

System stability, scalability and high performance

The encryption with fideAS® file enterprise is highly performing and saves system resources. The Security Server responsible for the administration of access rights can be operated redundantly. The clients will automatically log on to the second system should the first one not be available.

Revision-proof logging

All security-critical operations by users and security administrators are logged and stored in a revision-proof manner. Digital signatures prevent the manipulation of logging journals and facilitate the auditing of the system.



fideAS® file enterprise can be used in a distributed environment within a domain.



Product

Technical Data:

Cryptographic algorithms

AES (up to 256 bits), 3DES
RSA (up to 4096 bits)

Certificates

X.509v3
PKCS#7

Interfaces for key media

PKCS#11
PKCS#12
Microsoft CSP

Supported SmartCards and USB tokens

Aladdin eToken
Kobil mIDentity
SafeNet iKey 2032
ePass2000
StarKey100
CryptoIdentity5
Athena ASECard
AR PrivateCard
D-Trust
Giesecke & Devrient
Reiner SCT mateKey
SignTrust
TeleSec NetKey
and others

Supported SmartCard readers

AR PrivateSafe 2.5
Athena ASEDrive
Cherry SmartBoard G86-6744
Kobil KAN Pro
OmniKey CardMan 2010
OmniKey CardMan 3620
REINER SCT CyberJack
SCM SPR532

Supported Biometric devices

Feitian BioPass3000 Fingerprint USB

Supported operating systems

Windows XP
Windows Vista
Windows 7
Windows 2003 Server
Windows 2008 Server
Microsoft Terminal Server
Citrix XenApp

Hardware requirements (minimum)

Client: 512 MB RAM, 1 GHz
Server: 1 GB RAM, 3 GHz
Network: 100 Mbit/s



Test SC Magazine October 2008

"fideAS® file enterprise's ability to encrypt and decrypt files on-the-fly is impressive."

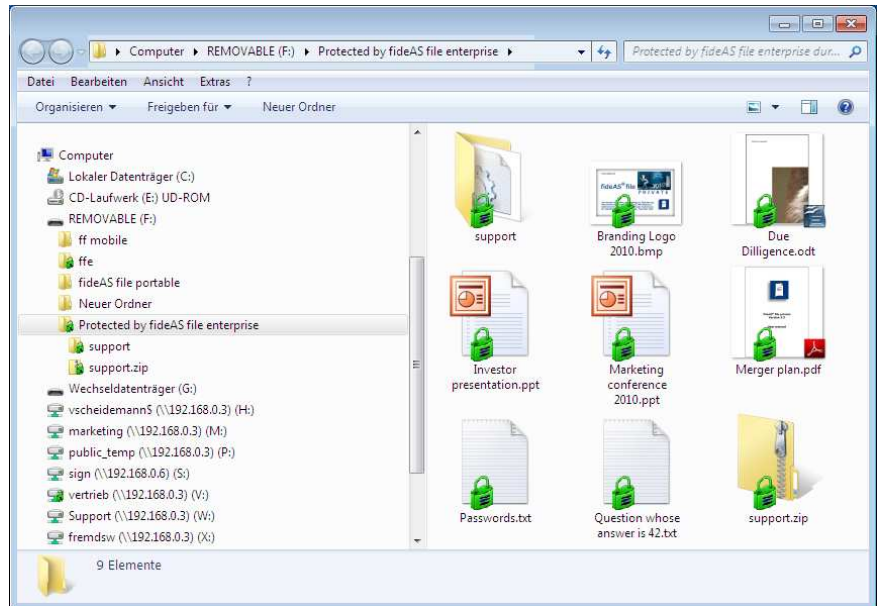


Figure: Transparent encryption of sensitive data with fideAS® file enterprise

fideAS® file enterprise covers



Encryption & Auditing



Data Leakage Prevention



Application Control



Critical Data 4-Eyes Principle



Removable Media Control

Talk to us.

apsec offers a wide variety of services dealing with all relevant questions of data security.

Consulting

Design of security policies, threat analysis, internal network security

Network security

Internet/Intranet/Extranet security, access control for databases, firewalls, VPN, virus protection, remote access

Software security

Cryptographic functions in applications, PKI, secure email, digital signatures, encryption