



dekart

Make IT Secure!

Dekart Data Privacy

A corporate environment,
has different operating systems - we have solutions for them,
has different systems for remote access - we work with them,
has different vendors of key storage devices - we support them,
Dekart provides solutions to ease implementing your corporate security policy.

Dekart offers a holistic approach to protection of information assets.

What do you expect
from a security solution?

We offer:

Reliability

FIPS validated encryption algorithm implementation
(AES, SHA-1)

Transparency

- easy local and remote access
- fault-tolerance
- consistent and predictable performance

High-speed encryption

fast encryption, without hindering system performance

Convenience

properly implemented security functionality

Flexibility

user's viewpoint - friendliness
system's viewpoint - evolution and migration
modularity, scalability, portability and interoperability

Return on Investment

Dekart saves you time and money by eliminating
50% of help desk calls related to lost, stolen and
forgotten passwords.



dekart

Make IT Secure!

Dekart data privacy - value proposition:

- Reduces costs
- Integrates into existing business process
- Increases productivity
- Ensures strong FIPS validated encryption

Corporate Profile

For over ten years, Dekart has been providing solutions to facilitate secure communication between individuals and businesses.

Employing state-of-the-art encryption algorithms, certified by the National Institute of Standards and Technology (AES and SHA-1 algorithm), Dekart offers cost-effective and reliable solutions to provide robust, enterprise-class security to store and transmit sensitive data. Designed to protect enterprise information, allowing customers to securely share data and automate sensitive processes, Dekart cross-platform security products significantly reduce costs and accelerate return on investment for organisations and individuals.

These products are developed by Dekart SRL
All rights reserved, 2003

Dekart Security Suite - built on a highly modular and flexible multi-factor authentication platform. Supports leading authentication technologies such as biometrics (fingerprint), PKI, USB tokens and smart cards.

Dekart Private Disk - virtual encrypted disk for protecting sensitive data

Dekart Secrets Keeper - encrypt and decrypt any type of files including Microsoft Word, Excel and PowerPoint documents

Dekart Logon - safe logon

Dekart RSA Cryptographic Provider - SSL, S/MIME, encryption and digital signature for Microsoft Outlook, Outlook Express, Novell GroupWise 6.5 and higher, TheBat! 2.0 and higher and other email clients.

Dekart Private Disk - employs the AES standard encryption algorithm. This technology ensures a high level of encryption, and does not hinder the computer's performance in any way. Private Disk allows you to store your information on a host of media such as HDD, FDD, CD, CD/R, CD/RW, MO, MD, ZIP-disks, flash drives, flash memory cards, PDAs, and even digital cameras (memory sticks). You have the flexibility to allow multiple users to share a single PC. Each user will then have their own secure area, with an individual hardware key.

Dekart Secrets Keeper - a security solution for the Windows Explorer and Microsoft Office environment. Secrets Keeper enables you to encrypt and decrypt any type of files including Microsoft Word, Excel and PowerPoint documents in order to keep the information safe from unauthorized access and manipulation. Encrypted information can only be accessed by entering the correct password, or PIN if you are using the hardware key feature.

Dekart Logon - provides an additional level of security for authenticating to the Microsoft Windows operating system, Samba (Linux).

Dekart RSA Cryptographic Provider - integrates into the Windows operating system and enables you digitally sign and encrypt/decrypt Microsoft Outlook and Outlook Express emails, as well as get access to protected web sites. Dekart RSA Cryptographic Provider's encryption keys can be stored within the Windows environment or on a key storage device, allowing access to and interoperability with encrypted emails, corporate Web sites and a host of other resources.