dekart
MAKE IT SECURE

Dekart Solutions

The following *information security threats* comprise ¾ of the financial damages suffered by various businesses in the course of 2005.

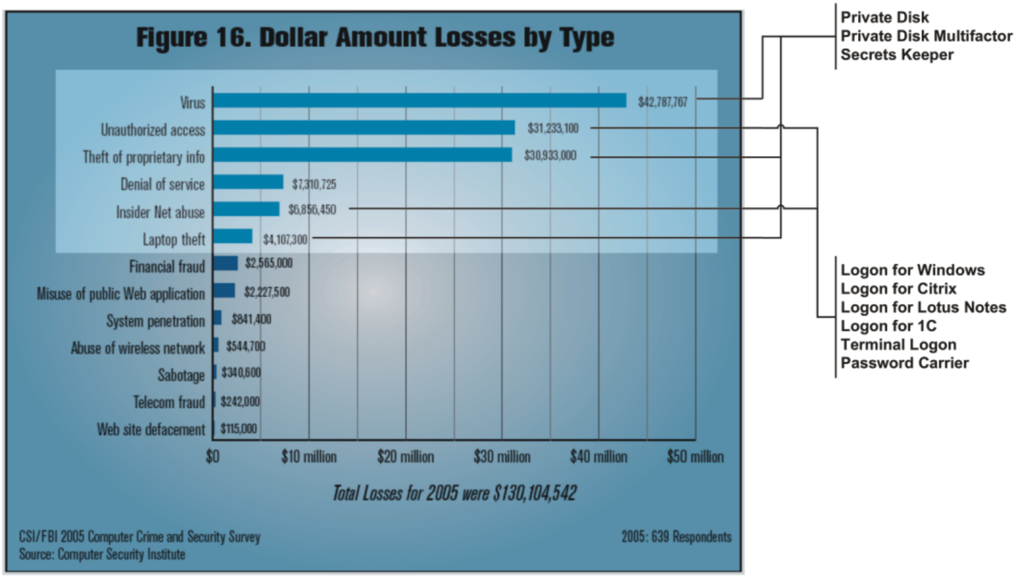


Figure 16. Dollar Amount Losses by Type

Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Private Disk
Private Disk Multifactor
Secrets Keeper

Logon for Windows
Logon for Citrix
Logon for Lotus Notes
Logon for 1C
Terminal Logon
Password Carrier

Dekart provides intelligent security software that aims to resolve the highlighted issues, requiring a minimal amount of time, investments, and changes in the existing infrastructure. Our products rely exclusively on **NIST certified** cryptographic modules, and they are successfully deployed in a great number of private and government organizations around the globe.

Dekart's end-to-end solutions are designed to *shift the responsibility off the shoulders of the end user*, which allows administrators to *strictly control* data flows and ensure the infrastructure's security is never breached as a consequence of misuse.

Our products can be *naturally integrated* into business environments that are made up of workstations running different versions of Windows, on different platforms. *64-bit* architecture support makes Dekart software ready for the future, while *Active Directory* and *Novell eDirectory* compatibility allows the applications to be easily deployed across a network domain.

Standards compliance makes it possible to use Dekart software with a broad range of *PC/SC smart card readers*, and biometric devices.

Dekart solutions work together tightly, solving multiple problems in one move. Private Disk's *proactive defense* technology – Disk Firewall, makes it possible to protect mission-critical data from unknown viruses and malware, while the top-notch encryption algorithms combined with biometric authentication make your data theft-proof. As a consequence, a single product shields you from *viruses*, *identity theft*, and *theft of proprietary information*.

Secure password storage and *user authentication* is achieved by applying products from our Logon series. These can be used to log on to Windows workstations, Active Directory or Novell eDirectory domains, terminal servers, Windows applications, web-sites, Citrix servers, as well as Lotus Notes.

Dekart offers a cost-effective solution to a set of multiple threats that exist in IT. The reliability of our products has been confirmed by reputable institutions such as NIST, and by a great number of organizations and individuals worldwide.

Secure password storage and multifactor user authentication

Our Logon series can be applied within infrastructures that are in the need to easily store the passwords of a great number of users, and authenticate them, without accepting the risks of *unauthorized access* or *identity theft*. This is achieved by combining *smart card technologies* and *biometric devices*, resulting in a *two-* or *three-factor authentication* mechanism that cannot be compromised.

- *Logon for Windows*: the supported versions are 9x/ME/NT/2000/XP/2003; the functionality of the program is consistent within each version of the OS. Domain logon is also supported, allowing users to log on to *Active Directory* or *Novell eDirectory* automatically.
- *Password Carrier*: a password storage solution that automates the process of logging on to web-sites, web-based business services, as well as Widows applications. The passwords are stored in encrypted form on a removable disk, which can be used on any Windows-powered PC, without the requirement of having administrative privileges. The program comes with a built-in backup routine.
- *Logon for Lotus Notes* and *Logon for Citrix ICA Client*: offers secure password storage and multifactor authentication to those who work with Lotus Notes, or remote Citrix servers.
- *RSA Cryptographic Service Provider*: moves digital certificates to a smart card, token, or a removable disk, making it possible to use the certificate on another workstation without having to locally install it, not even temporarily.
- *Terminal Logon*: provides the network administrator with the ability to use smart cards or tokens to securely store the credentials, which are needed when establishing *SSH* and *Telnet* sessions.

Our authentication solutions make the infrastructure *immune to keyloggers*, and to *social engineering* attacks, because the role of the end-user is that merely of connecting the token and authenticating themselves. The contents of the password storage device are encrypted, and may be kept secret from the end-user, allowing the enterprise administrator to ensure that *insider attacks* are simply impossible. Sticky notes cannot compromise corporate security anymore.

Disk encryption solutions

Every data encryption solution developed by Dekart relies on cryptographic libraries that were *certified by NIST*. The applications comfortably integrate into an existing environment, due to the full transparency of data encryption. The programs create multiple virtual volumes, to which any application can write data. This allows Private Disk and Private Disk Multifactor to be used as a secure layer, on top of which any running application becomes able to process encrypted data.

Dekart's innovative *Disk Firewall* feature is a *proactive defense* mechanism, which restricts access to the protected data, shielding the files from viruses or other malware that managed to get past the antivirus. Now you can beat the virus writers, getting ahead of the game by not having to constantly update your virus definitions.

Private Disk can run directly from a removable device, allowing it to be used with USB flash disks, or flash memory cards. The built-in encrypted backup procedure makes it easy to make copies of data, therefore theft of storage media will never result with *theft of proprietary information*.

Private Disk Multifactor extends Private Disk's feature set with the ability to use smart cards and biometric authentication mechanisms. This addition makes brute-force attacks literally impossible; further, it allows the enterprise administrator to control who can access sensitive data by issuing and revoking smart cards or tokens.

dekart
MAKE IT SECURE

Multifactor Authentication

Something you **know**
password or PIN

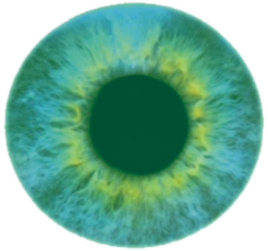
+

Something you **have**
USB key,smart card...

+

Something you **are**
voice,fingerprint,eye...

****



Password management

Sign-On services

- Active Directory
- SAMBA
- Lotus Notes

- Windows (local)
- Encrypt data
- Novell eDirectory

- Telnet, SSH
- Citrix Server
- Digital signature

- Application data
- Encrypt email
- Website forms

and a lot more...

Dekart Hardware Solutions

Dekart Secure Identity Storage is a smart card reader which also has a built-in 256MB flash memory module. This highly portable USB stick is designed to access SIM-sized smart cards and is ideal for security applications, card management and data storage. Combining flash drive encryption, smart card authentication, password and identity storage, Dekart Secure Identity Storage is an all-in-one solution to address endpoint security challenges of an enterprise.

Being combined in one small and strong case, both functions make it possible to apply the unit in many activities, which were previously unavailable, or required a significant effort to be deployed. Secure Identity Storage comes with software solutions which work tightly together, and help you resolve the problem of secure password storage, reliable user-authentication, and unauthorized access.

Features

- USB full speed interface
- No need for separate power supply or battery – *Bus powered*
- *CCID* and *Mass Storage Device Class* compatible
- Automatic driver installation functionality
- USB Composite Device – works as Mass Storage and Smart Card Reader
- With protective USB cap, SIM card slot cover and Keychain loop
- Compliant with the following International Standards: *ISO7816, CE, FCC, PC/SC, and Microsoft WHQL*
- Smart Card Reader:
  - Reads and writes all microprocessor cards with T=0, T=1 protocols
  - Supports 5V MCU cards
  - Supports Plug-in (SIM-sized) smart cards, SIM cards for GSM phones, UICC cards for 3G phones and R-UIM cards for CDMA phones.
  - Short Circuit Protection
- Flash Drive:
  - Mass Storage Device Class compatible - no driver needed in Windows 2000 and XP
  - Built-in 256MB flash memory (higher memory size is available upon request)
  - Public *(free read/write area for data storage)* and Private *(protected area for pre-loaded applications)* zones

Dekart SIM Card Reader is one of the world's smallest, PC/SC-compliant smart card readers. With Dekart SIM card reader you can easily edit GSM SIM phonebook data and perform timely backups in case of mobile phone loss or upgrade. Dekart SIM card reader is a USB plug-in card reader for managing a mobile phone's SIM cards, including UMTS USIM cards for 3rd generation mobile communications.

It is also a full-featured PC/SC compliant smart card reader for PC security applications, compatible with all types of smart cards available on the market today.

Dekart SIM Card Reader comes with a free license for *SIM Manager*, a convenient SIM card management tool, which helps you organize the contacts of the address-book, make backup copies of the SIM card, and view detailed information about the card. SIM Manager is compatible with Nextel cards, as well as with the latest 3G cards that are becoming increasingly popular.

Features

- USB full speed interface
- No need for separate power supply or battery – *Bus powered*
- No need to run separate drivers on most Windows versions – *CCID compatible*
- Compliant with the following International Standards: *ISO7816, CE, FCC, PC/SC, and Microsoft WHQL*
- Smart Card Reader:
  - Reads and writes all microprocessor cards with T=0, T=1 protocols
  - Supports 5V MCU cards
  - Supports Plug-in (SIM-sized) smart cards, SIM cards for GSM phones, UICC cards for 3G phones and R-UIM cards for CDMA phones.
  - Short Circuit Protection

Password Carrier

Dekart Password Carrier *automatically* collects and *securely* stores the passwords and private details typed when logging on to web-sites or using Windows applications. Phishing protection, keylogger protection and strong password generation are just a few of the facilities offered by our product.

What makes Password Carrier better than other password management applications is its mobility. The program was initially designed to run from removable drives, which allows it to be used on *any* computer without sacrificing functionality or security.

Password Carrier stores the information in an encrypted form on the removable disk, the applied encryption algorithm is AES 256-bit, certified by NIST. This guarantees that if your USB disk was lost or stolen, nobody will be able to use it.

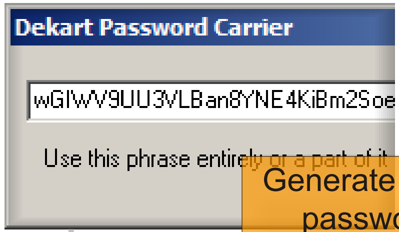
What else can Password Carrier do?

Besides automatically collecting passwords, storing them in an encrypted form, and transparently feeding them to the web-browser, Password Carrier provides other useful features:

- *Generate strong passwords*: the program can generate complex passwords that can be used in registration forms. Not only that it will make user accounts practically immune to brute-forcing, but it also guarantees that a person's accounts will have distinct passwords;
- *Easy registration of new accounts*: Password Carrier allows you to define a custom user profile, the data from which will be automatically filled in when signing up on a site. You are no longer forced to spend time entering details such as address, phone number or your name. This also helps you avoid accidental typos;
- *Freedom of movement*: this password management tool runs on *any* version of Windows which is in common use, and does *not* require administrative privileges. Users can stay connected to the world, regardless of their location;
- *Anti-phishing*: illicit sites that were designed to resemble authentic ones might fool the human eye, but they will *not* be processed by Password Carrier. Manually crafted Windows applications that mimic another application will not do the trick either;
- *Keylogger protection*: since form-filling is done automatically, no keyboard typing is required. Keyloggers *(being a common problem of public terminals or computers in internet cafes)* will no longer be able to memorize user credentials, making identity theft impossible;
- *Encrypted backup*: back yourself up by making an encrypted copy of the key, which can be used if the original key was lost or stolen. The data are encrypted with Dekart's NIST-certified implementation of the strongest algorithm available today – AES 256-bit;
- *Ease of use*: the program works in the background and doesn't get in your way. In addition, it can be temporarily disabled with only two mouse-clicks;
- *Easy customization*: Password Carrier can be trained to work with non-standard web-sites.

dekart
MAKE IT SECURE

Password Carrier

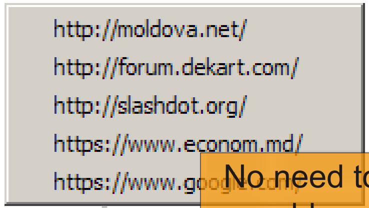


Dekart Password Carrier

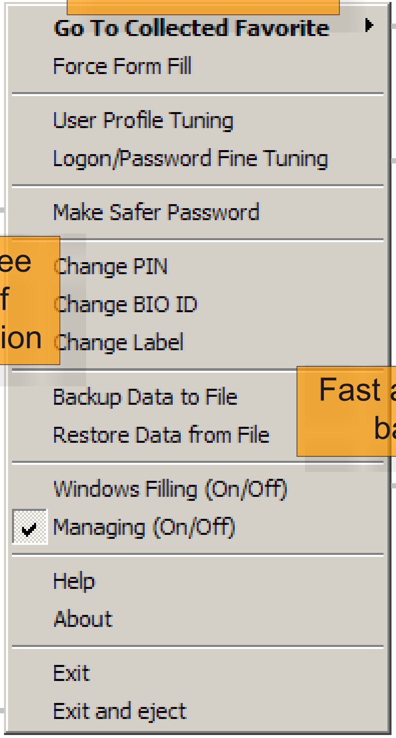
wGIWV9UU3VLBan8YNE4KiBm2Soe

Use this phrase entirely or a part of it

Generate strong passwords



No need to type addresses



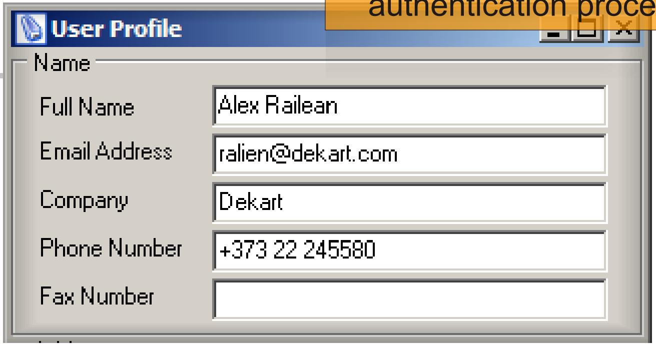
Two or three factors of authentication

Fast and secure backups

Automatic safe removal of portable media

Adjust your user profile by defining your personal details

This information will be used in the future, to automate registration and authentication processes



User Profile

Name

Full Name	Alex Railean
Email Address	ralien@dekart.com
Company	Dekart
Phone Number	+373 22 245580
Fax Number	

Automatically fill in the forms on web-sites and in Windows applications

Generate strong passwords

Easily register new accounts

Anti-phishing

Keylogger protection

Encrypted backups

Ease of use

Easy customization

Dekart Password Carrier *automatically* collects and *securely* stores the passwords and private details typed when logging on to web-sites or using Windows applications. **Phishing protection**, **keylogger protection** and **strong password generation** are just a few of the facilities offered by the software.

The collected credentials are encrypted with Dekart's *NIST-certified* implementation of **AES 256-bit**.

The program **does not require administrative rights**, and it runs directly from a removable disk, on any version of Windows which is in common use today.

Under the hood

- view and edit names and passwords
- define custom fields
- tweak program behavior
- ability to run off any removable storage device
- backup reminder

RSA Cryptographic Provider

This application makes it possible to use digital signatures and PKI-based mechanisms without being tied to a single computer. *Dekart RSA Cryptographic Provider* migrates certificates to a smart card, token, or a removable disk, making it possible to use the certificate on another workstation without having to locally install it, not even temporarily. This makes electronic document interchange a quick and safe procedure, protecting you from the risks of identity theft.

Highlights:

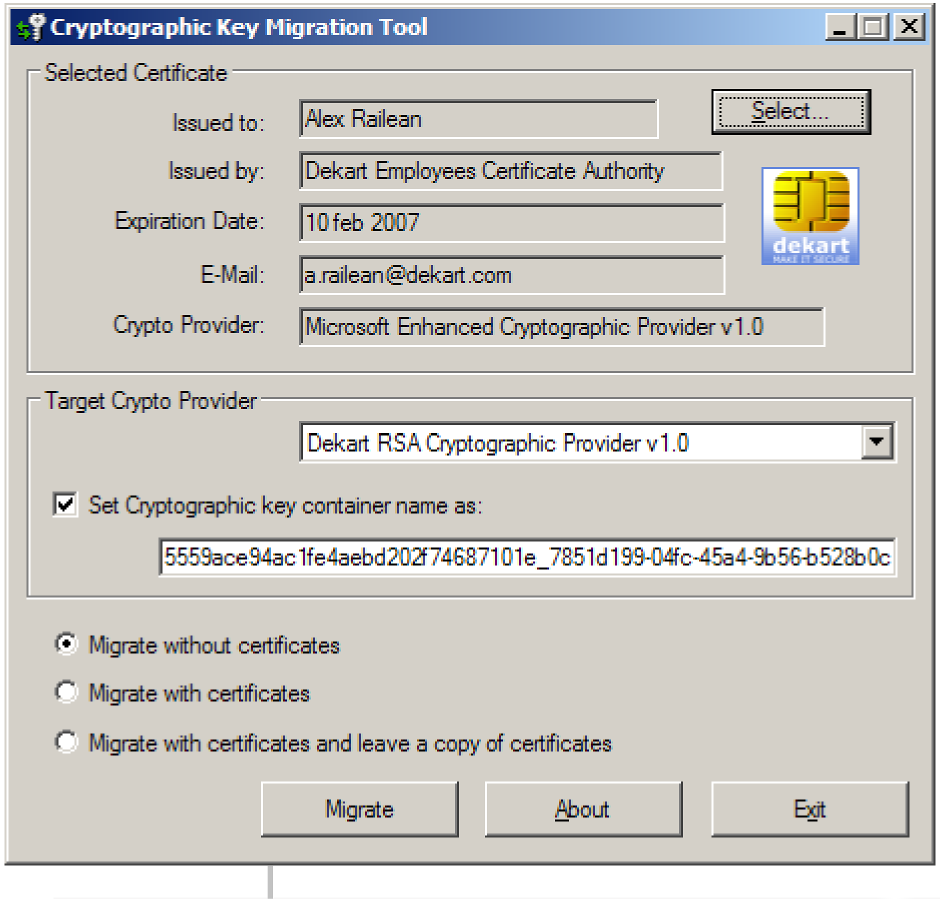
- the certificates are not stored locally, therefore a lost or stolen PC will not compromise one's digital identity;
- the vault on which the data are stored is secured with AES 256-bit encryption, thus only the true holder *(i.e. the person that knows the protection PIN)* can use it;
- identity theft attempts are literally impossible, because brute-forcing a smart-card will permanently block it, while unauthorized copies of a smart card cannot be made. This guarantees that the credentials are safe;
- a simple backup procedure allows you to quickly recover from situations in which the card is lost, without disrupting the rhythm of the business;

The above mentioned advantages make *Dekart RSA Cryptographic Provider* a popular tool among banks, and other institutions that heavily rely on the public key infrastructure. It guarantees that the person that uses the certificate is unable to accidentally compromise their own security, or that of the organization. This *shifts the responsibility off the shoulders of the end user*, allowing administrators to strictly control data flows and ensure the infrastructure's security is never breached.

The solution is also suitable for individual use, it can be applied in conjunction with the free digital certificates (http://www.dekart.com/home/free_digital_id/) issued by Dekart, making digital signatures and email encryption accessible to the general public.

dekart
MAKE IT SECURE

RSA Cryptographic Provider



Cryptographic Key Migration Tool

Selected Certificate

Issued to: Alex Railean

Issued by: Dekart Employees Certificate Authority

Expiration Date: 10 feb 2007

E-Mail: a.railean@dekart.com

Crypto Provider: Microsoft Enhanced Cryptographic Provider v1.0

Target Crypto Provider

Dekart RSA Cryptographic Provider v1.0

☑ Set Cryptographic key container name as:

5559ace94ac1fe4aebd202f74687101e_7851d199-04fc-45a4-9b56-b528b0c

● Migrate without certificates

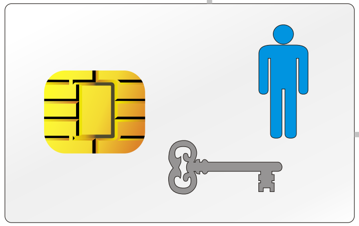
○ Migrate with certificates

○ Migrate with certificates and leave a copy of certificates

Private, protected and personalized computing from any PC – no matter where you are - simply migrate certificates to a smart card, token or USB flash drive. Use the certificate on any PC without having to locally install it, not even temporarily.

The product ***shifts the responsibility off the shoulders of the end user***, which allows you to strictly control data flows and ensure the infrastructure's security is never breached.

Digital certificates can be migrated to smart cards, tokens, removable drives, and flash-memory based storage devices



The smart card or token can hold both: the *encryption keys*, and the *digital certificate* itself, leaving absolutely **no traces** on the computer

	Windows CSP	Dekart CSP
Certificate storage media	Hard disk	Smart card, token, USB flash disk
Certificate mobility	**Restricted**: a certificate can be exported to a .PFX file and installed on another	**Unrestricted**: certificates are stored on the key and read directly from it; local
Possibility of cloning a certificate illegally	**Yes:** one can clone the entire disk on which the CSP stores its data	**No:** a smart card or token cannot be cloned without knowing the PIN
Potential dangers	**Yes:** a certificate imported on another system can be forgotten there, thus used	**None**: certificates are never stored, nor cached on the computer itself
Protection measures	The data are encrypted, a brute force attack **is possible**	The data are encrypted, a brute force attack **is not possible**
Backup possibility	No	Yes

Private Disk

Dekart Private Disk is a solution with a *unique* feature set, combining strong, NIST-certified AES 256-bit encryption with the best tools needed to build a protected infrastructure, where information can be processed in a secure way. Private Disk is compatible with virtually any version of Windows, including the latest 64-bit releases of Windows XP and Windows 2003.

Simple, reliable, and versatile, Private Disk allows you to create multiple encrypted disks that contain confidential information. Your files and documents are hidden from unwelcome eyes, while *Disk Firewall* ensures that undetected Trojans, viruses or spyware will not get access to your data.

Using Private Disk does not require any particular actions or changes in your routine activities, all the applications will be able to operate with the encrypted disks as if these were usual ones. Data encryption happens automatically, and in a transparent way: files are encrypted on the fly when they are written to the disk, and decrypted when read from the virtual disk.

The contents of the disk are well protected by *Disk Firewall*, a unique mechanism that guards your data from Trojans, viruses or other types of malware. Disk Firewall controls which applications are allowed to access the disk. If a specific application is not found in the white-list of programs, it will be unable to read or alter the contents of the private disk.

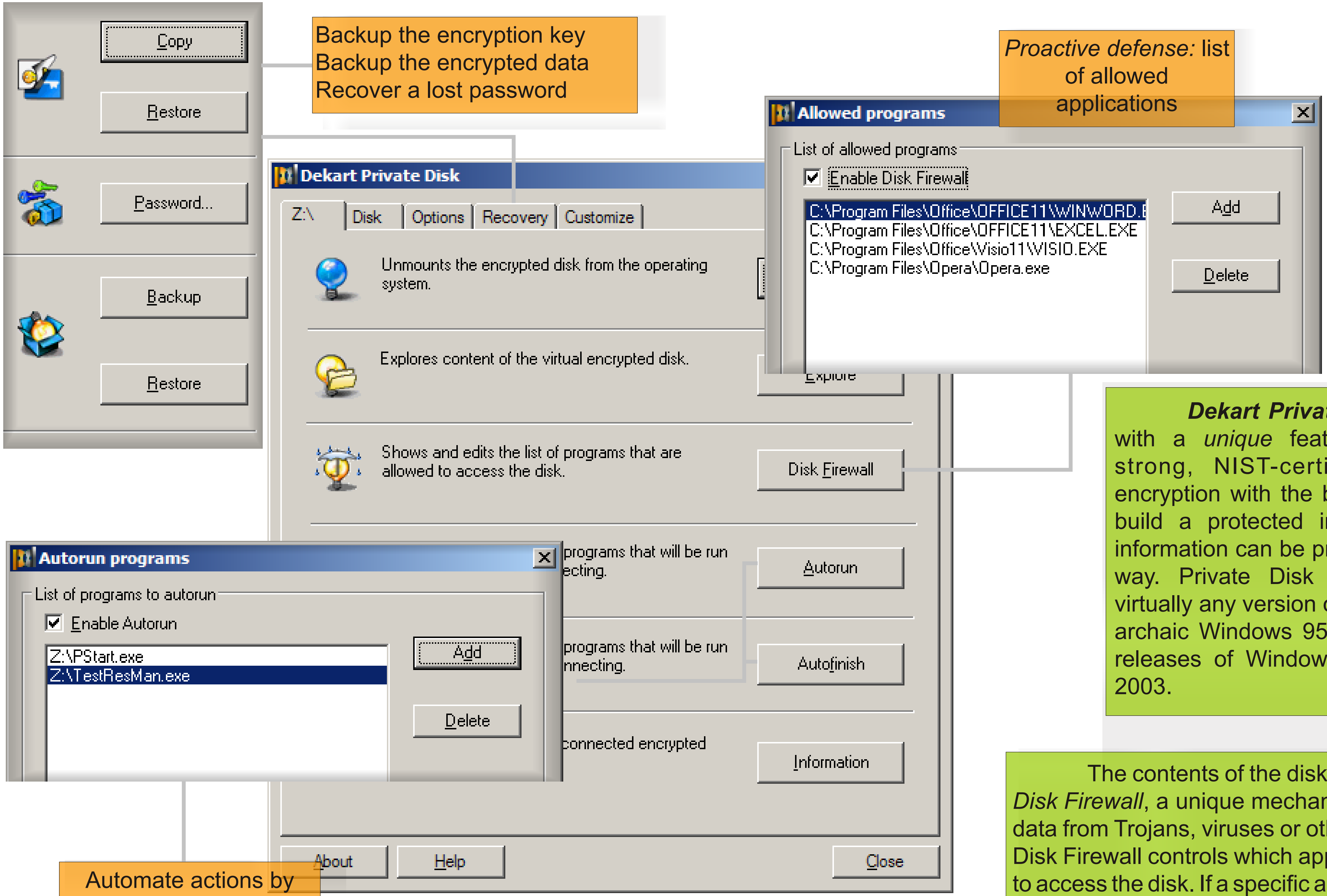
Private Disk's mobility allows it to be used in conjunction with a broad range of portable media, for instance: USB flash drives, external hard disks, flash memory cards, DVDs, or digital mp3 players, such as the iPod. Private Disk can be launched directly from the removable media, without having to be installed on the computer, meaning that you can work safely with your data, no matter where you are. The program will automatically invoke the safe hardware removal dialog when you close it – which will protect you from accidental data loss.

Highlights:

- *Disk Firewall*: protects your data from illegal copying, viruses and spyware by maintaining a white-list of applications which are allowed to access the encrypted disk;
- *64-bit platform compatibility:* Private Disk works with Windows x64, on AMD64 and IA-64 systems. At the same time, the program is able to run on older versions of Windows, including Windows 95;
- *NIST certification* of all the cryptographic components applied in the software: *AES 256-bit* encryption and *SHA-2* hashing;
- *Portability* allows you to open your protected files on other computers by running Private Disk directly from a removable drive, without having to install it locally. The program can be migrated to a USB disk or flash memory card with a single click, while the built-in *safe hardware removal* routine will help you disconnect a removable disk quickly and safely;
- *Encrypted backups*: create compressed encrypted backups of your private data, making disaster recovery an easy process. Backups are also a common corporate policy;
- *Autorun and Autofinish applications*: simplify your tasks and save your time by automating the execution of specific applications located on the encrypted drive;
- *Data wiping*: securely erase your encrypted data, making sure that recovery tools will fail to obtain fragments of your encrypted files.

dekart
MAKE IT SECURE

Private Disk



Unmounts the encrypted disk from the operating system.

Explores content of the virtual encrypted disk.

Shows and edits the list of programs that are allowed to access the disk.

programs that will be run
ecting.

programs that will be run
nnecting.

connected encrypted

List of allowed programs

☑ Enable Disk Firewall

C:\Program Files\Office\OFFICE11\WINWORD.E
C:\Program Files\Office\OFFICE11\EXCEL.EXE
C:\Program Files\Office\Visio11\VISIO.EXE
C:\Program Files\Opera\Opera.exe

List of programs to autorun

☑ Enable Autorun

Z:\PStart.exe
Z:\TestResMan.exe

Backup the encryption key
Backup the encrypted data
Recover a lost password

Proactive defense: list of allowed applications

Automate actions by defining *Autorun* or *Autofinish* applications

SC MAGAZINE RECOMMENDED
★★★★★

Dekart Private Disk is a solution with a *unique* feature set, combining strong, NIST-certified AES 256-bit encryption with the best tools needed to build a protected infrastructure, where information can be processed in a secure way. Private Disk is compatible with virtually any version of Windows, from the archaic Windows 95, to the latest 64-bit releases of Windows XP and Windows 2003.

The contents of the disk are well protected by *Disk Firewall*, a unique mechanism that guards your data from Trojans, viruses or other types of malware. Disk Firewall controls which applications are allowed to access the disk. If a specific application is not found in the white-list of programs, it will be unable to read or alter the contents of the private disk.

File and folder encryption software, that combines hardware and biometric authentication with 256-bit AES encryption to protect users' important documents and files on hard drives and portable media.

With Secrets Keeper companies eliminate data theft possibilities while meeting federal compliance regulations like Sarbanes-Oxley, GLBA, HIPAA. Tailored to satisfy an increasing global demand for encryption of endpoint equipment, such as desktop PCs, notebooks, USB flash drives, and different portable storage devices, Secrets Keeper protects sensitive data without long deployment procedures or personnel training.

Secrets Keeper is the quickest, most secure, most simple, and the most cost effective method of email attachment encryption when PKI is not an option. The program may also be applied in the cases in which files must be transferred via an untrusted third-party. The solution is moderately priced, which means that the strongest encryption tools available today can be afforded by the general public.

Security-conscious users will get the peace of mind that their confidential files and important documents are protected. If your notebook or portable drive gets lost or stolen, you can rest assured that all your files remain protected with unbeatable AES 256-bit encryption. Dekart offers the only solution on the market today that combines the industry's best-of-breed NIST-certified encryption, portability and two- and three-factor authentication technologies into a low-cost and easy-to-deploy solution. Secrets Keeper is intuitive to use, and is backed by Dekart's exceptional, personalized customer service.

Secrets Keeper is a file encryption program that enables PC users to protect/encrypt their files without any special knowledge. You do not have to waste time learning how the application works – you start protecting confidential information immediately after installing this file encryption software. Users can easily encrypt their documents directly from Microsoft Word, Microsoft Excel and Microsoft PowerPoint applications, as well as enjoy fast and convenient encryption of all types of files using Windows Explorer.

What sets Dekart Secrets Keeper apart from competitors' products is its ease of use combined with a wide range of professional security capabilities. You may simply lock your files by setting a strong password or you may use a security token and a fingerprint scanner to strengthen your data protection with two and three factor authentication. You may select from the widest range of hardware devices to store your cryptographic keys, including various smart cards, USB tokens, USB flash disks, iPods, memory sticks etc.

dekart
MAKE IT SECURE

Secrets Keeper

Data wiping assures that the deleted files cannot be recovered

Relies on implementations of *AES 256-bit* and *SHA-512*, certified by NIST

Creates *standalone*, *self-extracting* encrypted archives

File-based encryption tool which relies on **NIST-certified AES 256-bit** encryption.

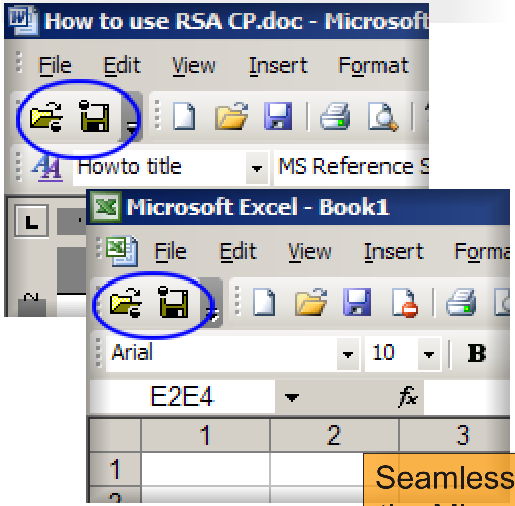
Secrets Keeper makes it easy to handle protected data, by allowing you to encrypt and decrypt files using a key.

A key is the most reliable way to store a password, and it eliminates the need to memorize complex pass-phrases.

Two- or three-factor authentication that employs *smart cards*, *tokens* and *biometric devices* increases the level of protection and makes unauthorized data access practically impossible.

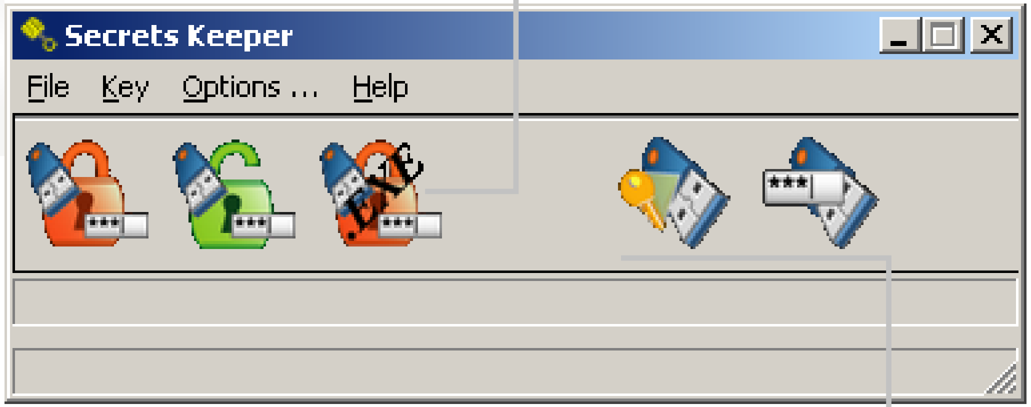
The risk of forgetting decryption passwords is entirely eliminated.

Secrets Keeper integrates with Microsoft Office applications and Windows Explorer, making it easy to exchange documents in a secure way, without having to acquire new computer skills.

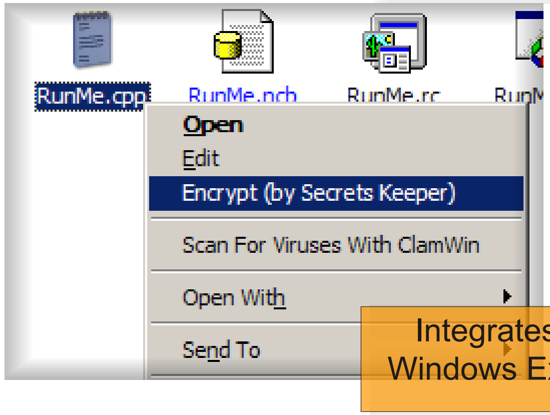


How to use RSA CP.doc - Microsoft
File Edit View Insert Format
Howto title
MS Reference S
Microsoft Excel - Book1
File Edit View Insert Forma
Arial
10
B
E2E4
fx
1
2
3
1
2

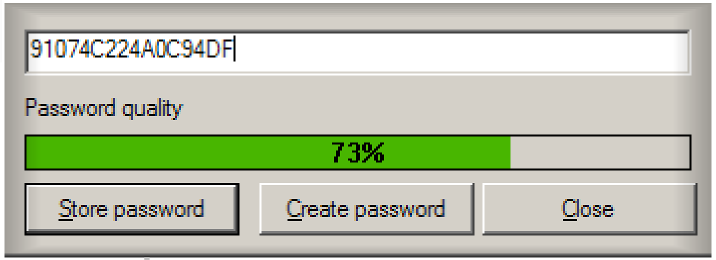
Seamless integration into the Microsoft Office suite



Two- or three-factor authentication protects the data



Integrates into Windows Explorer


91074C224A0C94DF

Password quality 73%

The password quality meter prevents weak passwords from compromising your data

Two- or three-factor authentication, using smart cards, tokens or USB flash drives with biometric devices

SIM Manager 2 is an advanced SIM card management tool, which provides an easy way to manage the address-book of a SIM card, as well as process other data (such as the SMS archive, the list of fixed dialing numbers, or the list of last dialed numbers, etc).

The new version is fully compatible with *Nextel* and *3G* SIM cards, while preserving the compatibility with older GSM cards.

SIM Manager works *directly* with the SIM card, using a PC/SC-compliant smart card reader. The program does not require a phone, therefore it is a fact that the solution will still be relevant after the phone is upgraded, or when a switch to a different mobile operator is made.

Some of the common tasks SIM Manager can handle:

- Synchronize contacts between phones within an enterprise, regardless of which carrier different persons use, or which phone brand or model they prefer;
- Synchronize the contacts of the SIM card with the contacts stored in the address book of an email client *(ex: Outlook, Eudora)* or a desktop PIM application *(ex: Palm Desktop)*, this is achieved by exporting / importing the data using CSV files;
- Backup a SIM card in order to easily restore the data if the card is lost, or if a copy needs to be made;
- Update multiple address book entries at once, by adding or removing a phone prefix when traveling from one country to another;
- Print out reports that contain the address book entries, and other information that is stored on the SIM;
- Change or disable the security codes (PIN1, PIN2), as well as unlock a SIM;
- Obtain detailed information about the SIM card, such as the IMSI, ICCID, the ATR, or the name of the mobile operator;

SIM Manager is a Unicode application, meaning that it can correctly process names and texts that contain characters other than the ones in the Latin alphabet, regardless of the current regional settings of Windows. This makes SIM Manager suitable for enterprises that have offices in different geographical locations.

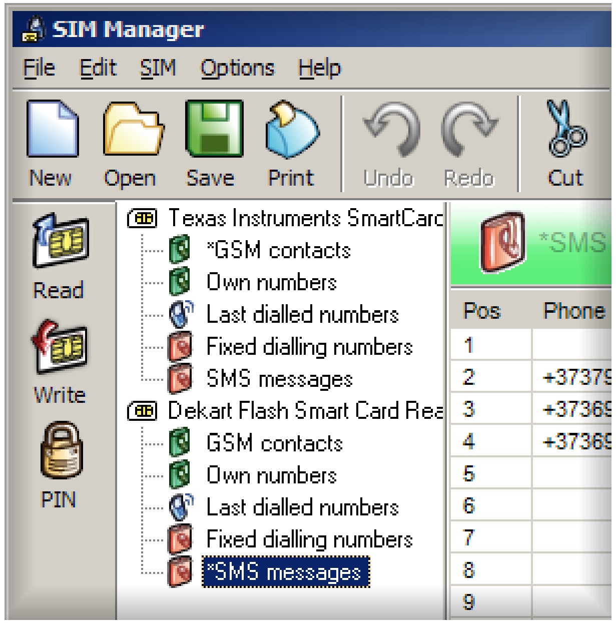
Coming soon - SIM Manager SDK

SIM Manager SDK is a library that allows you to create a custom SIM card management application that meets the needs of your business.

The SDK includes the library, the documentation, and several samples that will help you get started.

dekart
MAKE IT SECURE

SIM Manager



Pos	Phone
1	
2	+37379
3	+37369
4	+37369
5	
6	
7	
8	
9	

Supports **3G** and **Nextel** cards

SIM Manager is now able to view and edit SMSes stored on the card

Backup a SIM card with just a few clicks

Add, delete, edit and move phone numbers with ease

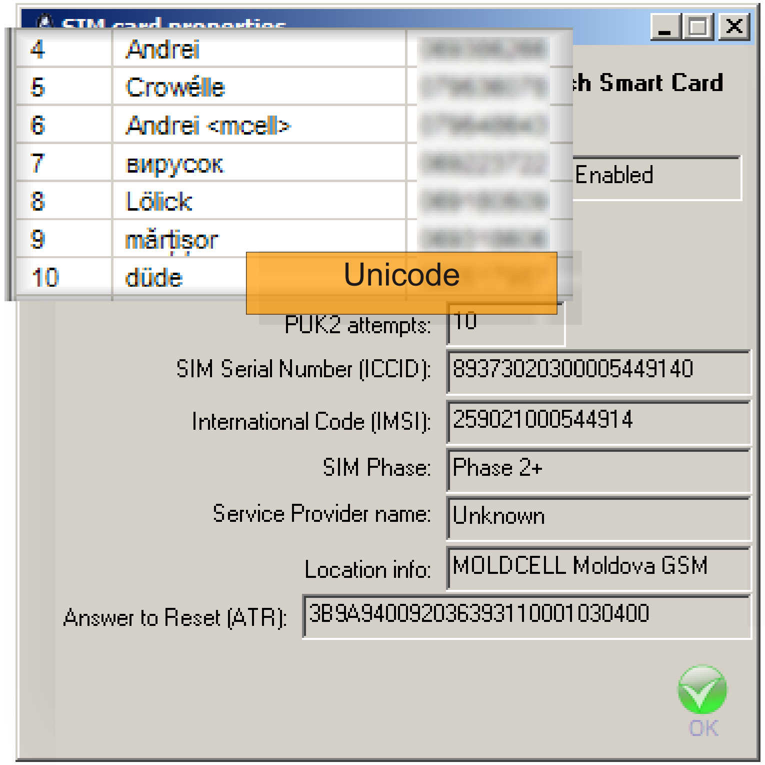
Convenient SIM card management solution, compatible with standard GSM SIM cards, as well as with new **3G** and **Nextel** SIM cards.

Easily manage the contacts within the enterprise, by merging contacts from multiple SIM cards, and synchronizing them with desktop applications such as Outlook, Palm Desktop, etc.

Full **Unicode** support guarantees that all the names will be displayed correctly.

Additional features

- *backup* the contents of the SIM card
- *synchronize* the address book with Outlook, Palm Desktop, and other applications on the desktop via the CSV format
- *print out reports* that contain your address book and other details
- retrieve detailed information about the SIM card
- *change PIN* codes
- *unlock the SIM* card
- *full Unicode support* ensures that all the names are displayed correctly
- *multiple card readers* can be used simultaneously



4	Andrei	[redacted]
5	Crowělle	[redacted]
6	Andrei <mcell>	[redacted]
7	вирусок	[redacted]
8	Lölick	[redacted]
9	mărțișor	[redacted]
10	düde	[redacted]

Unicode

Enabled

PUK2 attempts: 10

SIM Serial Number (ICCID): 89373020300005449140

International Code (IMSI): 259021000544914

SIM Phase: Phase 2+

Service Provider name: Unknown

Location info: MOLDCELL Moldova GSM

Answer to Reset (ATR): 3B9A940092036393110001030400

Compatibility with all GSM phones

Dekart SIM Manager supports all mobile phone models and does not require any additional cables, since it works directly with a SIM card using a PC/SC compatible smart card reader.

View detailed information about the SIM card

State of PIN1, PIN2, PUK1 and PUK2
ICCID (SIM serial number)
IMSI (International code)
SIM Phase
Service Provider name
Location information
The ATR of the SIM card
The total available memory on the card
The size and the number of free phonebook entries
The date and time of the received SMSes

Logon for Windows

Dekart Logon is a convenient password replacement solution, which enhances the standard logon procedure by adding the possibility to use *multiple authentication factors*. It allows you to securely logon to Windows PCs using smart cards, tokens or USB flash disks, while the third authentication factor – the *biometric verification*, further secures the process. The use of three factors of authentication eliminates the risks of *unauthorized access* and *identity theft*.

Domain administrators can issue keys to the end users, without letting them know what the actual passwords are. As a consequence, the security of the enterprise cannot be compromised by passwords written on sticky notes, or by people who deliberately share their pass phrases with another party.

The solution also makes the infrastructure *immune to keyloggers*, and to *social engineering* attacks, because the role of the end-user is that merely of connecting the token and authenticating themselves.

Logon for Windows makes it easy to follow the best practices of security, allowing the use of *strong passwords*, as well as their *change at regular intervals*. All of this happens without burdening users, thus the negative effects of the human factor are avoided.

It is now simple to achieve Sarbanes-Oxley (SOX), Gramm Leach Bliley Act (GLBA), Basel II and the Health Insurance Portability and Accountability Act (HIPAA) regulatory compliance without long deployment procedures or additional training costs.

The software supports a broad range of smart cards, tokens, and biometric devices, thus Logon for Windows will *naturally integrate* into an environment.

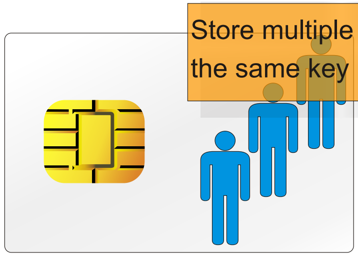
Dekart Logon offers native support for Microsoft Windows 9x/2000, XP, Windows Server 2003 and close integration with Microsoft *Active Directory* and *Novell eDirectory*.

Highlights:

- *Improved privacy:* nobody can peep over your shoulder as you type your passwords, because the process is fully automated. Besides giving you all the privacy you need, this feature takes off your shoulders the burden of remembering complex passwords;
- *Multiple factors of authentication* boost your security to an entirely new level, making identity theft impossible, even if your key was stolen and the protection PIN was compromised;
- *Easily follow the best practices of security*: the program will automatically lock or shutdown the workstation if the key is unplugged; while the optional *key removal reminder* will make sure that you never forget your key when you leave;
- *Save time:* the logon procedure allows you to authenticate locally, as well as remotely *(on an Active Directory or Novell eDirectory domain)* in a single move;
- *Scalability*: use the same key to unlock user accounts that exist on computers that are a part of a different infrastructure, without having to get yourself a new one.

dekart
MAKE IT SECURE

Logon for Windows



Store multiple accounts on the same key

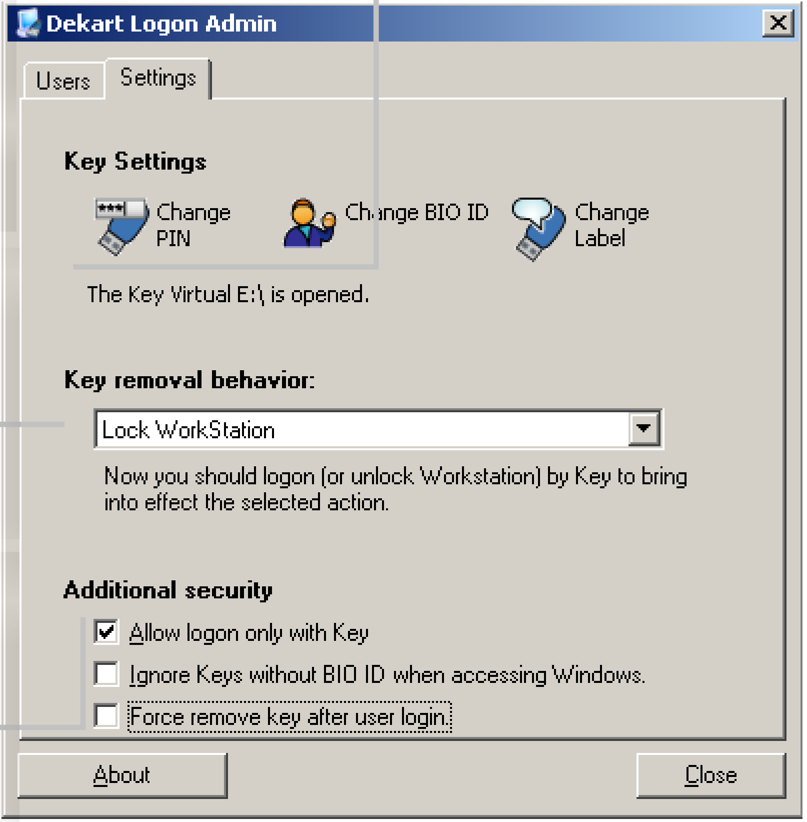
Two- or three-factor authentication, using smart cards, tokens or USB flash drives with biometric devices

The generated cryptographically *strong passwords* don't need to be memorized by humans anymore

Avoid *unauthorized access* by automatically locking the workstation or ending the current session when the key is removed

Flexible access control

Avoid *identity theft* by making it impossible to forget a key



Key Settings

The Key Virtual E:\ is opened.

Key removal behavior:

Lock WorkStation

Now you should logon (or unlock Workstation) by Key to bring into effect the selected action.

Additional security

☑ Allow logon only with Key

☐ Ignore Keys without BIO ID when accessing Windows.

☐ Force remove key after user login.

Dekart Logon is a convenient password replacement solution, allowing you to securely logon to Windows PCs using smart cards or USB flash disks.

The tool serves as a *secure password storage* mechanism, as well as a *reliable user authentication* tool.

The program offers native support for Microsoft Windows 9x/2000, XP, Windows Server 2003 and close integration with Microsoft Active Directory and Novell eDirectory.

Improved privacy: nobody can peep over your shoulder as you type your passwords, because the process is fully automated. Besides giving you all the privacy you need, this feature takes off your shoulders the burden of remembering complex passwords;

Multiple factors of authentication boost your security to an entirely new level, making identity theft impossible, even if your key was stolen and the protection PIN was compromised;

Easily follow the best practices of security: the program will automatically lock or shutdown the workstation if the key is unplugged; while the optional *key removal reminder* will make sure that you never forget your key when you leave;

Save time: the logon procedure allows you to authenticate locally, as well as remotely *(on an Active Directory or Novell eDirectory domain)* in a single move;

Scalability: use the same key to unlock user accounts that exist on computers that are a part of a different infrastructure, without having to get yourself a new one.

Two- or three-factor authentication, using smart cards, tokens or USB flash drives with biometric devices

Under the hood

- automatic logon to Active Directory, Novell eDirectory
- compatible with a great number of smart card readers and biometric devices
- the key can be used to contain data written by other Dekart applications

Logon Series

Dekart offers a series of cost-effective applications which are designed to enhance the security of businesses that rely on the following software and technologies: *Lotus Notes*, *Citrix* servers, *SSH* servers, *1C* accounting tools.

They enhance the standard logon procedures by adding the possibility to use *multiple authentication factors*, combining smart cards, tokens or USB flash disks with *biometric verification*. The use of three factors of authentication eliminates the risks of *unauthorized access* and *identity theft*.

The solutions also make the infrastructure *immune to keyloggers* and *social engineering* attacks, because the role of the end-user is that of merely connecting the token and authenticating themselves.

There is no need to remember user names, passwords and connection profiles, because all the credentials are securely stored on the smart card, hardware token or USB flash drive. It is now easy to achieve Sarbanes-Oxley (SOX), Gramm Leach Bliley Act (GLBA), Basel II and the Health Insurance Portability and Accountability Act (HIPAA) regulatory compliance without long deployment procedures or additional training costs.

Dekart logon applications come with a full automation mode: a connection can be initiated automatically, as soon as the smart card or token is plugged in. The software also assures there will be *no data leaks* if a computer is left unattended – connections are closed automatically when the key is unplugged.

Dekart Logon for Citrix ICA Client can act as an entirely self-contained bundle, by migrating the Citrix client itself to a removable disk, making it possible to keep everything on a single key, and never leave any traces on the local machine. This gives users all the mobility they could ask for; at the same time, the infrastructure does not become less secure, as the privacy of the data is protected by our *NIST-certified* implementation of *AES 256-bit*.

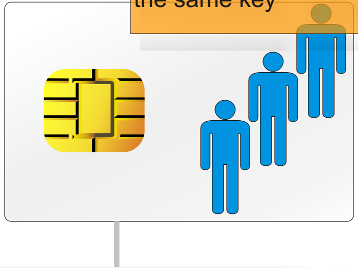
Highlights:

- *Improved privacy:* nobody can peep over your shoulder as you type your passwords, because the process is fully automated. Besides giving you all the privacy you need, this feature takes off your shoulders the burden of remembering complex passwords;
- *Multiple factors of authentication* boost your security to an entirely new level, making identity theft impossible, even if your key was stolen and the protection PIN was compromised;
- *Save time* by letting the software automatically establish or terminate the connections when keys are plugged or unplugged;
- *The natural integration* of the software makes it easy to use, because employees are not required to change their working habits, since the programs can work in the background and never get in one's way;
- *Cost-efficiency* allows you to combine multiple Dekart solutions and use them with the same token or smart card; this is very convenient if it happens so that your enterprise relies on more than one technology supported by our software.

dekart
MAKE IT SECURE

Logon Series

Store multiple accounts on the same key

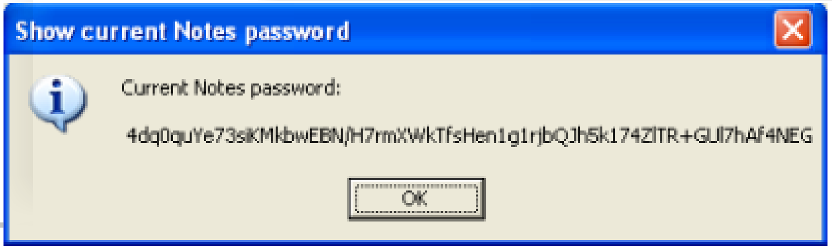


Portability

The connection profiles and the user credentials are stored entirely on the key, leaving no information on the computer itself

Logon for Citrix can store the Citrix client itself on a removable drive, meaning that the system is entirely self-contained

The generated cryptographically *strong passwords* don't need to be memorized by humans anymore



Show current Notes password

Current Notes password:

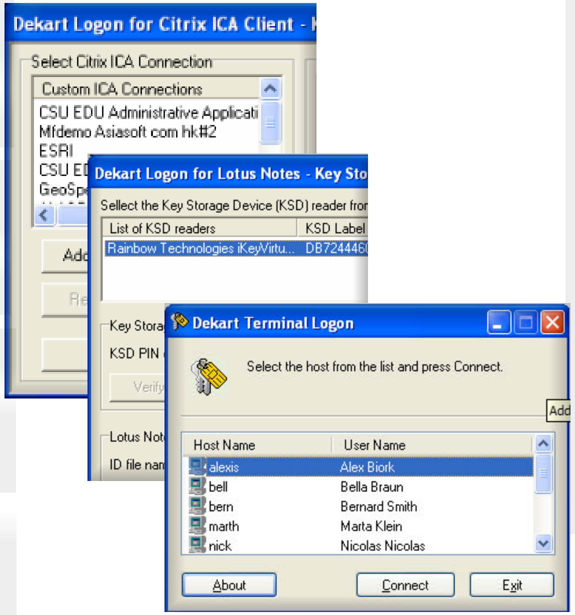
4dq0quYe73sIKMkbwEBN/H7rmXWkTfsHen1g1rjbQJh5k174ZlTR+GUl7hAf4NEG

Full automation
The program can be fully automated, initiating connections as soon as a key is plugged in, and terminating them when the key is removed

Work in the background
The software works in the background and does not interfere with the user

Easy backup
The keys can be quickly backed up, or multiplied if necessary

Flexible management of credentials
Authentication data can be stored on the key without being disclosed to the user, which makes insider abuse impossible



Dekart Logon for Citrix ICA Client - I

Select Citrix ICA Connection

Custom ICA Connections

CSU EDU Administrative Applicati
Mfdemo Asiasoft com hk#2
ESRI
CSU ED
GeoSp

Dekart Logon for Lotus Notes - Key Sto

Sellect the Key Storage Device (KSD) reader fron

List of KSD readers	KSD Label
Rainbow Technologies iKeyVirtu...	DB724446

Key Stora
KSD PIN
Lotus Not
ID file nan

Dekart Terminal Logon

Select the host from the list and press Connect.

Host Name	User Name
alexis	Alex Biork
bell	Bella Braun
bern	Bernard Smith
marth	Marta Klein
nick	Nicolas Nicolas

Dekart provides a series of solutions that bring multi-factor authentication and secure password storage to enterprises that use the following products:

- *Citrix client*
- *Lotus Notes*
- *1C* accounting software
- *SSH* or *Telnet* clients for remote server administration

These cost-effective solutions help companies achieve Sarbanes-Oxley (SOX), the Gramm Leach Bliley Act (GLBA), Basel II and the Health Insurance Portability and Accountability Act (HIPAA) regulatory compliance without long deployment procedures or additional training costs.

Improved privacy: nobody can peep over your shoulder as you type your passwords, because the process is fully automated. Besides giving you all the privacy you need, this feature takes off your shoulders the burden of remembering complex passwords;

Multiple factors of authentication boost your security to an entirely new level, making identity theft impossible, even if your key was stolen and the protection PIN was compromised;

Easily follow the best practices of security: the program will automatically lock or shutdown the workstation if the key is unplugged; while the optional *key removal reminder* will make sure that you never forget your key when you leave;

Scalability: use the same key to store user credentials for different accounts;

Reliability: the software relies on *NIST-certified* implementations of *AES 256-bit* encryption and *SHA-2* hashing algorithms;

Two- or three-factor authentication, using smart cards, tokens or USB flash drives with biometric devices

dekart
MAKE IT SECURE

Private Disk Multifactor

Dekart Private Disk Multifactor is a volume-based, *on-the-fly* encryption application, which enhances the strong, *NIST-certified* AES 256-bit encryption algorithm with a second and third authentication factor – a smart card or token, and a biometric device.

Smart card and biometric technologies take data security to the next level, making it impractical to conduct brute-force attacks. A smart card or token will block itself after an incorrect PIN was entered multiple times; while biometric verification ensures that even if the PIN of a lost or stolen token is known, the data are still well-guarded. This makes Private Disk Multifactor the best tool to *prevent unauthorized data access*.

The contents of a virtual disk are additionally protected by *Disk Firewall*, a unique *proactive defense* mechanism that guards your data from Trojans, viruses or other types of malware. Disk Firewall controls which applications are allowed to access the disk. If a specific application is not found in the user-defined white-list of programs, it will be unable to read or alter the contents of the private disk.

Multifactor supports a wide range of smart cards, tokens, and biometric devices, making it easy to choose the hardware which suits your needs in a better way. This also allows you to build a cost-effective solution.

The software is compatible with virtually any version of Windows, including the latest 64-bit releases of Windows XP and Windows 2003.

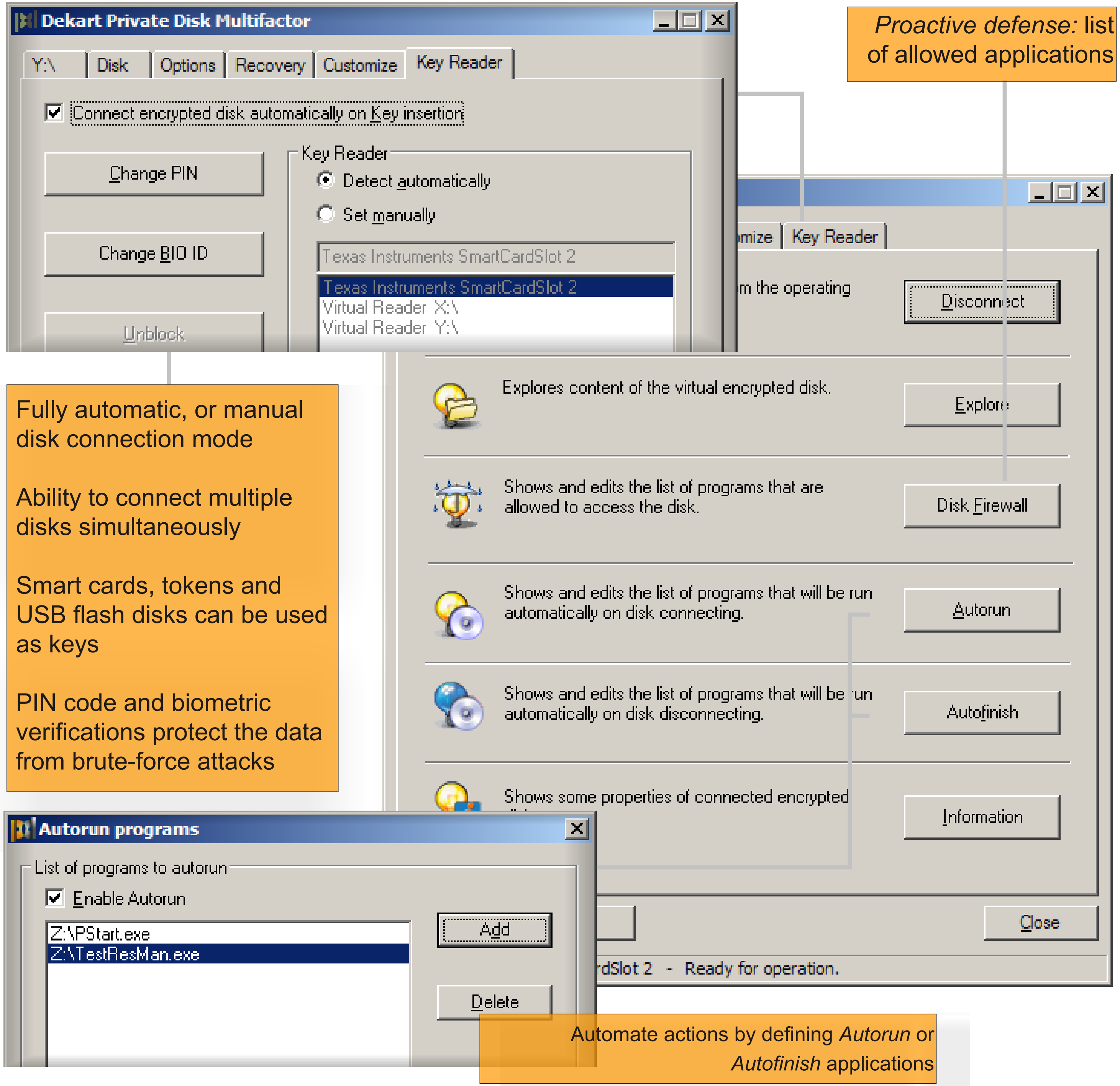
The program's mobility allows it to be used in conjunction with a broad range of portable media, for instance: USB flash drives, external hard disks, flash memory cards, DVDs, or digital mp3 players, such as the iPod. Private Disk Multifactor 2 can be launched directly from the removable media, without having to be installed on the computer, meaning that you can work safely with your data, no matter where you are.

Highlights:

- *Smart cards, tokens and biometric devices* of various types are supported, allowing you to build a custom, cost-effective solution which suits your needs best;
- *Disk Firewall*: protects your data from illegal copying, viruses and spyware by maintaining a white-list of applications which are allowed to access the encrypted disk;
- *64-bit platform compatibility:* Private Disk works with Windows x64, on AMD64 and IA-64 systems. At the same time, the program is able to run on older versions of Windows, including Windows 95;
- *NIST certification* of all the cryptographic components applied in the software: *AES 256-bit* encryption and *SHA-2* hashing;
- *Encrypted backups*: create compressed encrypted backups of your private data, making disaster recovery an easy process. Backups are also a common corporate policy;
- *Autorun and Autofinish applications*: simplify your tasks and save your time by automating the execution of specific applications located on the encrypted drive;
- *Data wiping*: securely erase your encrypted data, making sure that recovery tools will fail to obtain fragments of your encrypted files.

dekart
MAKE IT SECURE

Private Disk Multifactor



Dekart Private Disk Multifactor

☑ Connect encrypted disk automatically on Key insertion

Key Reader
● Detect automatically
○ Set manually

Texas Instruments SmartCardSlot 2

Texas Instruments SmartCardSlot 2
Virtual Reader X:\
Virtual Reader Y:\

m the operating

Explores content of the virtual encrypted disk. — Explore

Shows and edits the list of programs that are allowed to access the disk. — Disk Firewall

Shows and edits the list of programs that will be run automatically on disk connecting. — Autorun

Shows and edits the list of programs that will be run automatically on disk disconnecting. — Autofinish

Shows some properties of connected encrypted — Information

rdSlot 2 - Ready for operation.

Autorun programs

List of programs to autorun
☑ Enable Autorun

Z:\PStart.exe
Z:\TestResMan.exe

Proactive defense: list of allowed applications

Fully automatic, or manual disk connection mode

Ability to connect multiple disks simultaneously

Smart cards, tokens and USB flash disks can be used as keys

PIN code and biometric verifications protect the data from brute-force attacks

Automate actions by defining *Autorun* or *Autofinish* applications

Combine the strength of ***NIST-certified*** AES 256-bit encryption with the intelligence of ***smart card*** technologies.

The level of protection is further enhanced by applying ***biometric verification*** devices. This guarantees that the data will not become the target of a brute-force attack.

Multifactor 2 incorporates Dekart's new *Disk Firewall* technology, which is an efficient ***proactive defense*** mechanism. Now your data are well-protected even when your antivirus failed to detect the threat.

Easy and secure backup procedures are now a de-facto standard for each Dekart application; this, along with ***data wiping*** possibilities makes it easy to follow with the regulatory compliance laws such as ***Sarbanes-Oxley (SOX)*** or ***HIPPA***.

Two- or three-factor authentication, using smart cards, tokens or USB flash drives with biometric devices