Distr.
GENERAL

CES/SEM.47/13
30 January 2002

ENGLISH ONLY

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE | **COMMISSION OF THE EUROPEAN COMMUNITIES**

CONFERENCE OF EUROPEAN STATISTICIANS | **EUROSTAT**

Joint UNECE/Eurostat Seminar on Integrated Statistical Information Systems and Related Matters (ISIS 2002)
(17-19 April 2002, Geneva, Switzerland)

Topic II: Secure communications and data confidentiality

ENCRYPTION ON LAPTOP COMPUTERS

Contributed paper

Submitted by Statistics Sweden [1]

Abstract: Today's world demands greater mobility and laptops are used more than ever. It only takes a moment for someone to pick up an unattended laptop. What if the thief is not interested in reselling your computer, but is interested in the sensitive information stored on its hard drive? The aim of this research is to scan through available encryption products (appendix I) on the market, choose a product that would satisfy the needs of Statistics Sweden, and implement the solution.

I. BACKGROUND

1. Today's world demands greater mobility and laptops are used more than ever. It only takes a moment for someone to pick up an unattended laptop. What if the thief is not interested in reselling your computer, but is interested in the sensitive information stored on its hard drive?

2. Office desktop systems are left unattended and anyone can come in and quickly steal information from an unattended computer.

3. The root of these security concerns is sensitive information, which typically exists as unprotected files on your hard drive.

4. Statistics Sweden has a lot of different sensitive registers such as:
   - Secret defense registers;
   - National registers covering the whole population, all enterprises and real estate;
   - Companies secrets;

[1] Prepared by Behzad Panahi (behzad.panahi@scb.se).

- Different surveys (health, income, family planning);
- Registers covering ill-treated children, drug abuse and criminals;

And the fact that people rely on SCB's statistics and information.

5. Laptops are used widely at Statistics Sweden and the need of encryption is quite evident. The aim of this research is to scan through encryption products and alternatives available and choose one suitable for the company.

II. INTRODUCTION

6. Cryptography has been used for thousands of years to keep information secret. There are two types of cryptography. Asymmetric cryptography and symmetric cryptography**.**

A. Symmetric cryptographic algorithms

7. Symmetric cryptography is the classic form of cryptography. People have relied on it for thousands of years to keep messages private.

8. Symmetric cryptographic works by transforming (encrypting) the plain text (the original data) to cipher text (the protected data) in a way that makes it infeasible to reverse the process without the full knowledge of the transformation function. For a number of reasons the secret information is split into a constant part, the cryptographic algorithm, and a variable part, the cryptographic key. The algorithm can be widely deployed in software or devices that use cryptography, and in general is not assumed to be a secret. Therefore, all security lies in keeping the key secret.

9. Symmetric keys are either random blocks of data or are derived from user passwords, and are usually 40 to 128 bits in length. Symmetric algorithms are symmetric keys and a bloc algorithm such as DES, DESX, RC2; or RC4 encrypt and decrypt data.

B. Asymmetric cryptographic algorithms

10. Asymmetric, or public key cryptography also turns plain text into cipher text using an algorithm and a key. The difference lays in the use of a different decryption key, hence the name asymmetric.

11. The decryption (private) key and the encryption (public) key are related to each other, but the former cannot feasibly be derived from the latter. Therefore, the encryption key need not be kept secret, and can be made public. Instead, users of public key need to trust that a given key does belong to a particular owner. The process of certification addresses this issue. Security lies in keeping the private key secret.

12. Asymmetric keys are randomly chosen from a set that has certain properties specific to the asymmetric algorithm, so that users are unlikely to generate the same keys. Key size commonly ranges from 512 to 4096.

13. Asymmetric cryptographic algorithms were the natural choice to pursue in order to meet the goal of this study, encryption on laptop computers.

III. ENCRYPTION PRODUCTS

14. There are thousands of products on the market for encryption purposes. Only products written for Windows 2000 were of interest for this study, as Windows 2000 would be the system running on these laptops. A short list of these products is available in appendix I.

A. Security considerations at Statistics Sweden

15. All these products offer relatively good encryption possibilities. Considering:

- That the enemy is an individual, not a foreign power.
- The company's policy is relying on products from Microsoft.
- The company has contracts with IBM as well.

16. Due to the uncertainty about the lifetime and future support of the security products, it was mutually decided that the Encrypting File System for Windows 2000 would be chosen as the product to be thoroughly investigated and properly implemented on laptops.

B. Security considerations using encryption

17. There are many issues and questions that should be dealt with and investigated, among them are:

- How does the encryption work and where does it take place?
- What would happen to the temporary files that are created by the system?
- What happens if an employee leaves? Is it possible to retrieve the encrypted documents by a trusted party and how should it be organized?
- What happens to the encrypted files during a backup?
- What happens if a user changes her/his password?
- Would it take a long time to decrypt files that have been encrypted by the former password?
- Could an individual with physical access to the machine copy files to a floppy disc directly?
- How should encryption be implemented at the company laptops?
- Are there any complimentary products needed for encryption proposes?
- Does Microsoft have any products for auditing the encryption's success or failure?

IV. ENCRYPTION FILE SYSTEM FOR WINDOWS 2000

18. The following issues are addressed by the encryption File System for Windows 2000:

a) **Manual encryption and decryption on each use.** Encryption services are not transparent to the user in most products. The user has to decrypt the file before every use and re-encrypt it when finished. If the user forgets to encrypt a file, the file is unprotected. And, because the user must go to the trouble of specifying that a file be encrypted (and decrypted) on each use, it discourages the use of encryption.

b) **Leaks from temporary and paging files.** Many applications create temporary files while a user edits a document (Microsoft Word for one). These temporary files are left unencrypted on the disk, even though the original document is encrypted, making data theft easy. Application level encryption runs in Windows NT user mode. This means that the user's encryption key may be stored in a paging file. It is fairly easy to gain access to all documents encrypted using a single key by simply mining a paging file.

c) **Weak security.** Keys are derived from passwords or pass-phrases. Dictionary attacks can easily breach this kind of security if easy to remember passwords are used. Forcing more complicated passwords makes for more complicated usability.

d) **No data recovery.** Many products do not provide data recovery services. This is another discouragement to users especially ones who do not want to remember another password. In the cases where password-based data recovery is provided, it creates another weak point of access. All a data thief needs is the password to the recovery mechanism to gain access to all encrypted files.

A. How does the EFS encryption work?

19. EFS is based on public-key encryption, using CryptoAPI architecture in Windows -Microsoft® Cryptographic Application Programming Interface- (CryptoAPI). Each file is encrypted using a randomly generated key, called *the file encryption key*, which is independent of a user’s public/private key pair; thereby stifling many forms of cryptanalysis-based attack on the encrypted files.

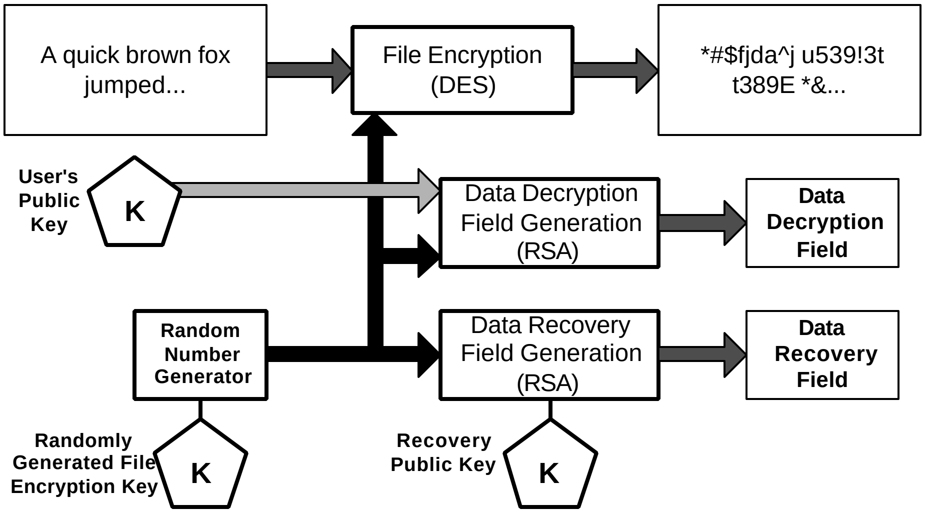
20. File encryption can use any symmetric encryption algorithm. The first release of EFS exposed DESX as the encryption algorithm. Future releases would allow alternate encryption schemes. EFS also supports encryption and decryption on files stored on remote file servers.

21. If the original file is encrypted, EFS encrypts its temporary copies when attributes are transferred during file creation. EFS reside in the Windows 2000 kernel and use the non-paged pool to store file encryption keys, ensuring that they never make it to the paging file.

22. File encryption and decryption is supported on a per file or entire directory basis. Directory encryption is transparently enforced. All files (and subdirectories) created in a directory marked for encryption are automatically encrypted. Each file has a unique encryption key, making it safe for rename operations. If you rename a file from an encrypted directory to an unencrypted directory on the same volume, the file remains encrypted.

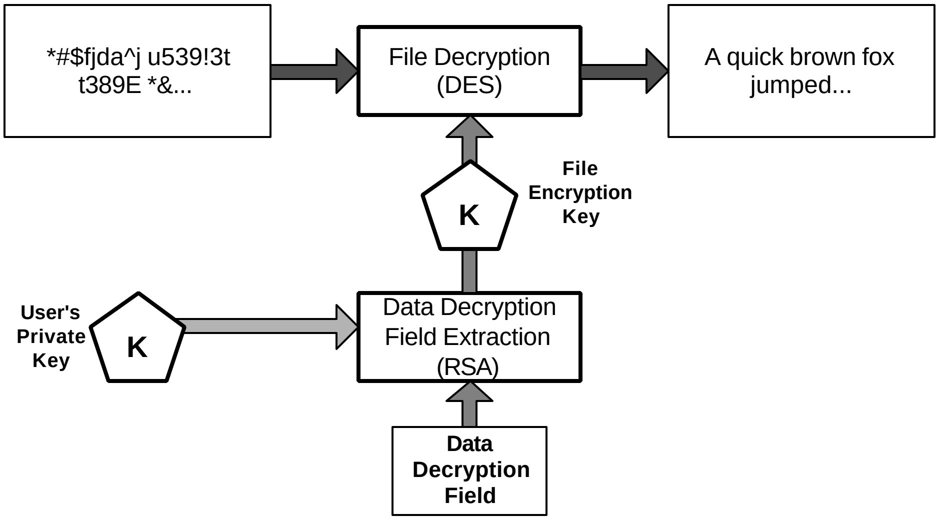
23. A file need not be decrypted before use (encryption and decryption is done transparently when bytes travel to and from the disk). EFS automatically detects an encrypted file and locates a user’s certificate and associated private key in user’s certificate and key stores. Since the mechanism of key storage is based on CryptoAPI, users will have the flexibility of storing keys on secure devices, such as smart cards.

24. The following diagrams illustrate the encryption and decryption processes. The encryption process:


A quick brown fox jumped...
File Encryption (DES)
*#$fjda^j u539!3t t389E *&...
User's Public Key
K
Data Decryption Field Generation (RSA)
Data Decryption Field
Random Number Generator
Data Recovery Field Generation (RSA)
Data Recovery Field
Randomly Generated File Encryption Key
K
Recovery Public Key
K

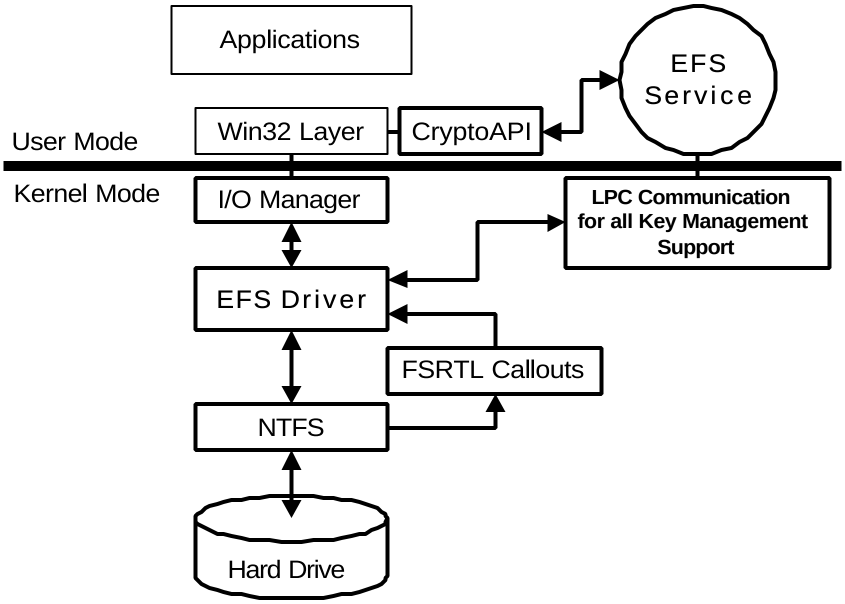
25. The user’s plaintext file is encrypted using a randomly generated FEK. This file encryption key is stored along with the file, encrypted under a user’s public key in the DDF and encrypted under the recovery agent’s public key in the DRF.

26. The decryption process:


*#$fjda^j u539!3t t389E *&...
File Decryption (DES)
A quick brown fox jumped...
File Encryption Key
K
User's Private Key
K
Data Decryption Field Extraction (RSA)
Data Decryption Field

27. A user’s private key is used to decrypt the FEK using the corresponding encrypted FEK item in the DDF. The FEK is used to decrypt file data reads on a block-by-block basis. Random access to a large file will decrypt only the specific blocks read from disk for that file. The entire file does not have to be decrypted.

28. Implementation: EFS architecture is shown in the figure below.



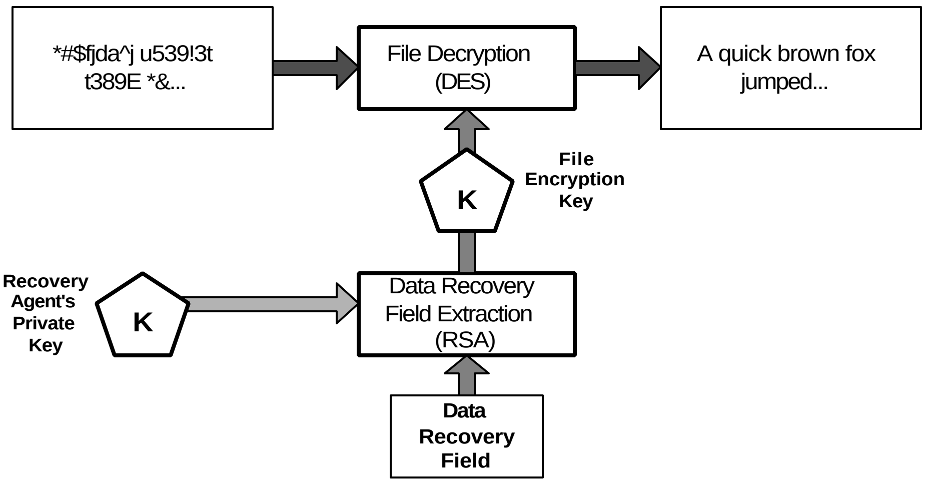
B. Data Recovery

29. EFS also provides built-in data recovery support. You can use file encryption only if the system is configured with one or more recovery keys. EFS allows recovery agents to configure public key certificates that are used to enable file recovery. Only the file’s randomly generated encryption key is available using the recovery key, not a user’s private key. This ensures that no other private information is revealed to the recovery agent accidentally (only the data that falls in the scope of influence of a recovery agent is recoverable by the agent).

30. Data recovery is intended for most business environments where the organization expects to be able to recover data encrypted by an employee after an employee leaves or when encryption keys are lost. The recovery policy can be defined at the domain controller of a Windows 2000 domain.

31. By default, recovery policy is under the control of domain administrators. To reduce any need for administration, EFS automatically configures a default recovery policy making the domain administrator account the recovery agent for the domain. Domain administrators can delegate this to designated data security administrator accounts using Windows 2000 Directory Service delegation features. This provides better control and flexibility on who is authorized to recover encrypted data. EFS also supports multiple recovery agents, by allowing for multiple recovery key configurations.

The recovery process:


*#$fjda^j u539!3t t389E *&...
File Decryption (DES)
A quick brown fox jumped...
K
File Encryption Key
Recovery Agent's Private Key
K
Data Recovery Field Extraction (RSA)
Data Recovery Field

32. The process is similar to decryption except that it uses the recovery agent's private key to decrypt the FEK in the DRF. This simple scheme provides a strong encryption technology and the ability to let multiple users share an encrypted file, as well as allowing multiple recovery agents the ability to recover the file if so required. The scheme is fully algorithm agile and any cryptography algorithms can be used for various encryption phases. This will be very important as new and better algorithms are invented.

C. Encryption auditing and implementation

33. A pilot laptop was acquired in order to test and implement encryption. The following tools/programs were installed on the laptop.

- High Encryption Pack - The Windows 2000 High Encryption Pack upgrades Windows 2000 to use 128-bit encryption.

- Efsinfo.exe: Encrypting File System Information - Efsinfo.exe is a command-line tool, which displays information about files, and folders encrypted with EFS on NTFS partitions.
  The user can also encrypt or decrypt a file or folder by using the command-line tool *cipher* that is included with the Windows 2000.

Selecting the Advanced button on the folder property page exposes the following EFS features to the user

D. Multiple tests

34. An encrypted folder (folder E) was created according to instructions. Another folder (folder U) (unencrypted) was created containing one encrypted file and one unencrypted file. File attributes are shown for these files when clicking on these files/folders. Encrypted files/folders were marked encrypted. Furthermore were these files/folders audited using Efsinfo.exe. Efsinfo.exe showed the same information about the files/folders as above.

35. An unencrypted document was created. The file's attribute changed to encrypted when copying it to the encrypted folder.

36. A user account was created giving the user access to the encryption files. It was not possible to read the encrypted documents using the user account. Because, when a user attempts to open a file encrypted by another user, EFS attempts to locate the private key, which will decrypt the FEK (file encryption key) during the open. Since the calling user will not possess the key, FEK will not get decrypted and hence the attempt will failed with "Access Denied".

37. A backup copy of E and U folders was created.

38. A copy of the encryption key was produced using Windows 2000 facilities. Encrypted files/folders were restored using Windows Explorer to decrypt the folder by clearing the Encrypt contents to secure data check box. A dialog box confirmed that the operation had to be performed on just the folders, but any subfolders as well or not.

39. A number of encrypted files were created using a user account. These files were accessible by administrator logging in on the laptop.

40. Attempts to read the data by physically gaining access to the media failed. Files were encrypted and a successful process would require implementing EFS itself.

41. Another possible attack with physical access was to invalidate or delete the recovery portion on the encrypted file. This did not work either, because EFS recreate the recovery information when the file was successfully opened next time.

42. It was of interest to find out what would happen to encrypted files when a user changes her/his password. The user's password was changed and the encrypted files were accessed. Change of password didn't affect the encrypted files integrity and accessibility because, EFS determines if the key used to open the file is current. If not, the data decryption field is updated on the file using the user's current key.

V. CONCLUSIONS

43. It was concluded that Windows 2000 offers an acceptable degree of encryption, suitable for Statistics Sweden. It was decided that all newer laptop computers upgradeable to Windows 2000 would be upgraded, enabling users to use encryption on these laptops.

44. An instruction was written for IBM personal requesting installation of High Encryption Pack on all laptops upgraded to Windows 2000.

45. Microsoft claims that each document encrypts separately and decrypts just when accessing the document. It was not possible to verify this statement because, documents are decrypted when one tries to access it and it is fully readable if the same document is copied to a disc and viewed in another computer (the system allows you to copy the document to the disc as the owner of the document when logging onto the computer as the owner of the file).

46. The same procedure disables you to see the actual cipher text, as the whole idea is denying access to a file by the system, when one is not the owner of the encrypted file. At the same time the owner gets to see the decrypted document. So there is no way of monitoring the exact encryption process and see different cipher texts.

47. EFS works only on NTFS partitions. Encrypted files copied to other non-NTFS partitions on the same disc or other media will not be encrypted. The user password should not be compromised.

References

Microsoft Windows 2000 Professional Resource Kit
ISBN: 1-57231-808-2.

Microsoft Windows 2000 Security Technical Reference
ISBN: 0-7356-0858-x.

Microsoft Windows 2000 Professional Expert Companion
ISBN: 0-7356-0855-5.

Running Microsoft Windows 2000 Professional
ISBN: 1-57231-838-4.

http://www.absolutelock.de/
http://www.baxbex.com/
http://cryptomite.html
http://www.jetico.com/
http://inv.co.nz/products/kryptel/
http://www.secureaction.com/guidesx/
http://www.globesoft.com/
http://www.davecentral.com/
http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp
http://msdn.microsoft.com/library/default.asp

Appendix I

Encryption Tools

- 007 Write All Stored ...
- A-Lock
- ABI - Key Manager
- ABI-Coder
- Absolute Security
- AbsoluteLock
- Accent Access Passwor...
- Accent Excel Password...
- Accent Money Password...
- Accent Office Passwor...
- Accent Office Passwor...
- Accent Word Password ...
- Access Denied
- Access Password Recov...
- aCrypt
- AdvaCrypt Suite
- Advanced Access Passw...
- Advanced ACE Password..
- Advanced ACT Password..
- Advanced ARJ Password...
- Advanced Backup Passw...
- Advanced Excel 95 Pas...
- Advanced Excel 97 Pas...
- Advanced Lotus Passwo...
- Advanced Money Passwo...
- Advanced NT Security ...
- Advanced Office 2000 ...
- Advanced Office 2000 ...
- Advanced Office 95 Pa...
- Advanced Office 97 Pa...
- Advanced Outlook Pass...
- Advanced Paradox Pass...
- Advanced Password Enu...
- Advanced Password Gen...
- Advanced PDF Password...
- Advanced Project Pass...
- Advanced QuicBooks Pa...
- Advanced RAR Password..
- Advanced Security Con...
- Advanced VBA Password..
- Advanced Word 95 Pass...
- Advanced Word 97 Pass...
- Advanced Word 97 Pass...
- Advanced ZIP Password...
- AE-STED
- AE-STED
- BestCrypt
- Boot Guard Plus with ...
- bProtected 2000
- Bunker
- chiocec20
- CIA (Cryptography in ...
- Cipher Data Manager
- CipherPad
- Citadel
- CodedDrag
- Codepad
- ComShield VPN
- CoolFish
- CrackIt
- CRC32
- Crypt-o-Text
- CryptEon DES File Enc...
- Crypter
- Cryptext
- Cryptnotes
- Crypto
- CryptoMan
- CryptoMite
- CryptoPAD
- CryptWare 2000
- Crytpo Kong
- CT Attrib
- EldoS Keeper
- Encode It
- Encrypted Magic Folde...
- Encrypted Sanctuary
- Encryption Plus Folde...
- Encryption Plus for E...
- Encryption Plus for H...
- Encryption Plus Secur...
- Enigma (Vranjesevic)
- Enigma 98
- Entry LE
- EXE Protector
- ExpressLock
- EZ Encrypt
- Fastcode
- Figa
- File Buddy
- File Encryptor and De...
- File Locker
- File Protector
- File Shredder (Topstu...
- FileCryptor
- FlashLock
- Folder Guard
- Fortify
- Guaranteed Excel 97/2...
- Guaranteed Excel 97/2...
- Guaranteed PDF Decryp...
- Guaranteed Word 97/20...
- Gui4PGP
- Guideon
- GUIDESX Encryption 20...
- GUIDESX Encryption Pa...
- Hidden
- Houdini
- Hydrant Internet Secu...
- I.D.E.A. Encryption
- Icon Lock-iT 2000
- IF 2000 Pro
- INAS
- Info Keep
- Interscope BlackBox
- Invisible Secrets
- Invisible Secrets Pro
- iProtect
- Iron Key
- IsEncrypted
- IW Mail
- Jammer (Lee)
- Jaylock
- JS Encrypt
- KeyPack2000
- Kremlin
- Kryptel
- Link Protect
- Lock n Safe
- Locker4U
- LockTight
- MAILguardian
- MailPGP
- Mastercrypt
- MDBPassw
- Mince
- Mollusc
- Mouse Lock
- MP-Crypt
- My Personal Diary
- N-CAT
- Navaho Lock with Voic...
- Navaho Viewer
- Navaho ZipSafe
- Ncrypt
- Neocrypt
- nKrytpt-IT
- NovaLock
- Password Vault
- Passwords by Mask
- PATools Data Encrypte...
- PC Activity Monitor
- PC-ENCRYPT
- PCSafe
- Peekboo
- PGP Encryptor Interfa...
- PGPHTML
- Phoenix Sentry
- PhotoEncrypt
- PhraseCrypt
- Power Crypto
- Powercrypt
- PowerPGP
- PowerVault for AOL
- Pretty Good Privacy
- PrivaSuite
- Private Desktop
- Private Pictures
- ProtectShell 2000
- ProtectZ
- pTrack
- Puffer
- Pure Noise
- QDPGP
- QuantaCrypt
- Quick:Crypt
- Random Password Gener...
- RAR Password Cracker
- S to Infinity
- SafeDisk
- SafeHouse
- SafeIT e-mail encrypt...
- SChatBUDDY
- Scramdisk
- ScreenLock (iJen)
- SCUA Security
- Scytale
- Secret Info
- Secur-all
- SecuraSite
- SECURE
- Secure (Digital Terra...
- Secure Explorer
- Secure Image
- Secure Messenger
- Secure Note
- SecureExplore
- SecureOffice
- SecureSafe
- SecureViewer
- SecureWin Desktop Edi...
- Security Box Freeware
- SecurityPlus
- seNTry 2020
- Shroud III
- Shroud Security Syste...
- Silver Key
- SimpleCrypt
- Smart Crypt-It
- Software Safe
- SpartaCom CryptoGram
- Speedsafe Pro
- SSHPro
- Stealth Encryptor
- Stealth Keyboard Inte...
- Stealth Keyboard Inte...
- Stealth Logger Core
- Steganos
- StopLight 95 ELS
- StrongCrypt
- Super WinUUE
- Tangle-It
- tbCrypt
- Visual Encryption
- Visual Zip Password R...
- VoiceSecureIt
- wbStego
- WinChanger 2000
- WinCrypt
- Windows Security Offi...
- WinFile Vault
- WinSafe
- WinXFiles
- WINZAP
- WinZip Password Recov...
- WMVault
- WPGP
- Z-File
- zipPassword