PROTECT for Windows™

Version 3.x

Product Description

DECROS®

PROTECT for Windows™

Version 3.x

Basic Functions

- Software Windows superstructure to protect files by encrypting
- modular architecture (three modules):
  - **Protect Encrypt for Windows**- encryption module
  - **Protect Sign for Windows**- asymmetric encryption and signing module
  - **Protect Logon for Windows**- log-on module
- module to boost authentication with HW security tokens (log-on, workstation locking/unlocking)
- transparent file encryption on local discs, portable media and networks
- protection during transfers on a network
- encryption of electronic mail

- selectable symmetric encryption algorithms
- optional storage of encryption keys in HW security tokens
- new concept of an encryption archive
- controls fully integrated in the Windows user environment (Explorer)
- recording of certain operations (EventLog)

Products Description

The Protect system consists of separate modules that some of them may be installed and used independently. It is naturally possible to use any combination of the modules. Currently, the Protect system is divided into the following modules:

- **Protect Encrypt for Windows**- encryption module
- **Protect Sign for Windows**- asymmetric encryption and signing module
- **Protect Logon for Windows**- log-on module

Protect Encrypt for Windows

The module offers transparent on-line encrypting, irreversible deleting of files, support for HW tokens to keep encryption keys, protected archive and recording of performed operations (EventLog)

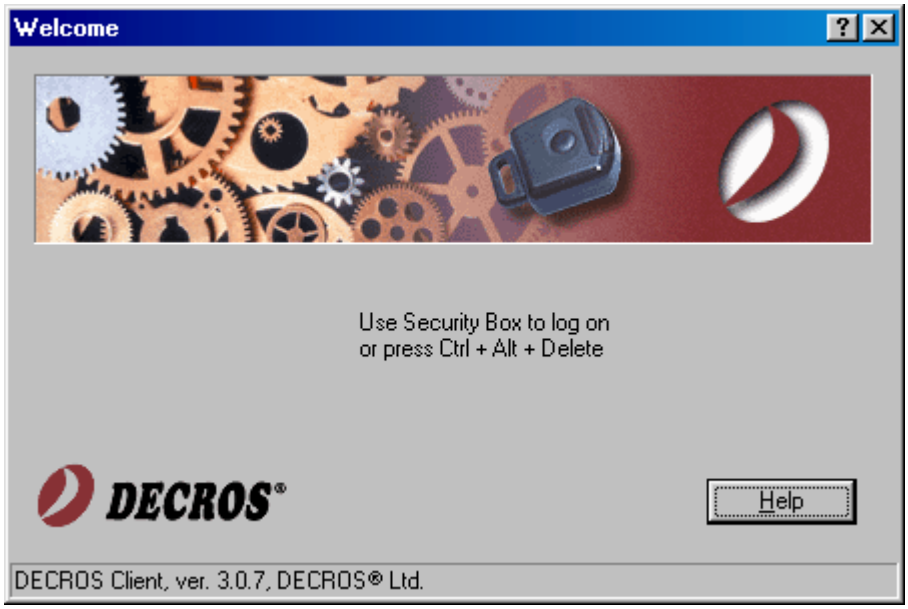
Protect Sign for Windows

The module is identical with the encryption one, while the protected archive of the Protect system is provided with a digital signing option.

Protect Logon for Windows

This module includes:

- log-on into the I&A operating system
- safe lock for the station
- system protections
- support for HW tokens to keep encryption keys and recording of performed operations (EventLog)



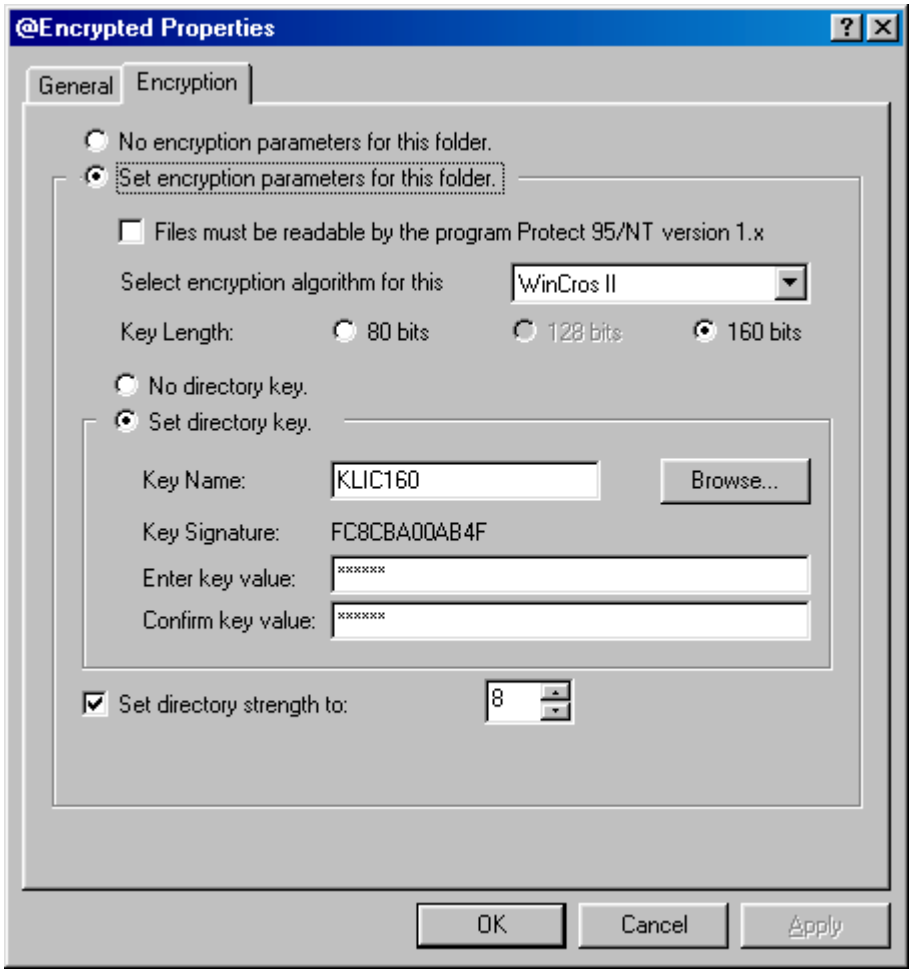
Encryption

The Protect system protects confidentiality of selected files and directories while enabling high-quality file encryption. The standard encryption options include a selection of symmetric encrypting algorithms (proprietory 80, 160 bits WinCros, WinCros II and public 80 and 128 bits algorithm CAST). Encrypting functions are implemented at the operating system core level and allow comfortable and entirely transparent work with encrypted files, high encryption speeds and high security standard. All controls of the encryption functions are fully integrated into the Windows user environment. There are two encryption methods available in Protect: transparent encryption and protected archives.

Transparent Encryption

Transparent encryption is performed in encrypted folders. By renaming any folder to a @folder (a folder whose name starts with @ character) an encrypted @folder will be created and encryption keys assigned to it in its attributes.

From this moment on Protect will encrypt all files stored or created in this @folder (including subfolders). When a file is created or when an already encrypted file in these @folders is accessed for the first time Protect will request an encryption key to be entered.



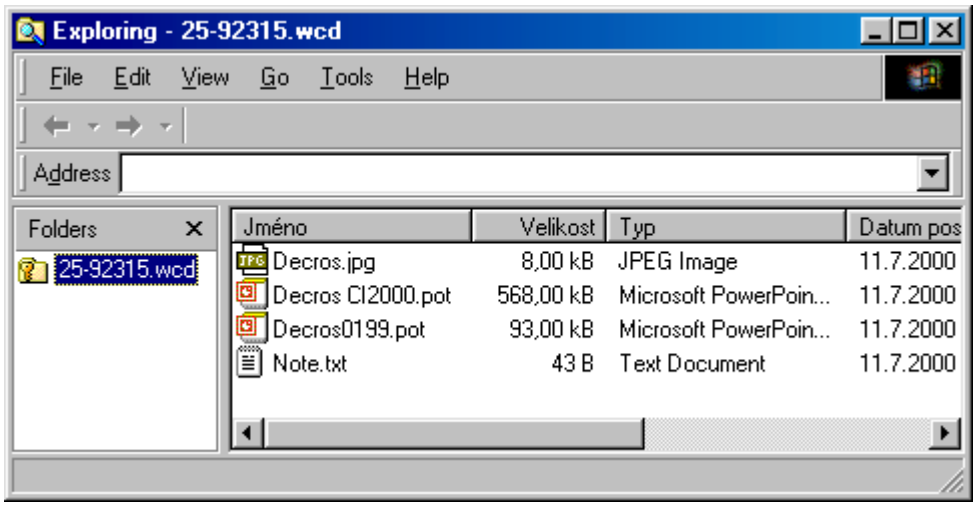
Once the key is entered (either through the keyboard or with a HW token), the file will be opened and the key remembered and consequently any work with the encrypted file will be completely transparent until the key is removed from the Protect memory. Transparent encrypting/decrypting then occurs unnoticed on the background while the user is working with encrypted data that remain permanently encrypted on a disc or net. Transparent encrypting enables easy protection of all working and data directories of the user.

Encrypted @folders may be created on local discs, as well as networks (MS, Netware, UNIX etc.) and portable and back up media (FDD, CD-ROM, ZIP). If @folders are on a network then all transfer of files within the network is also encrypted, independently of the employed protocol. Encrypting/decrypting always occurs only on the client workstation, while Protect need not be installed on the file server. By sharing the respective encryption key encrypted files may be shared by an unlimited number of users.

Protected Archives

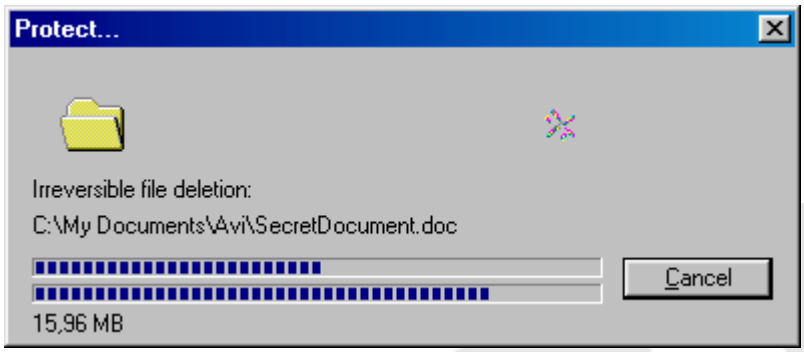
Protected Archive is an application enabling to insert a big number of files into a single encrypted file, the so-called Protected Archive (file .wcd). The file is internally

encrypted with a selected encryption key from the Protect system and it may be safely stored outside the encrypted @folders, backed up or sent by e-mail as an attachment. An archive created in this way may be opened again only by a person knowing or holding the applicable encryption key. It is possible to add or remove files from the Protected Archive, or to open and modify files directly in the archive (similarly as in other programs, e.g. WinZip or WinRAR). Protected Archive may be used even if it is desirable to conceal names of the files.



Irreversible Deleting

Once you select the option “delete irreversibly” the file will be first rewritten with a selected sample of characters and only then the applicable reference will be deleted. There is no way to retrieve a file deleted irreversibly.



Protect Sign for Windows

Digital Signature Module

A client of the digital signature module Protect Sign for Windows becomes an integral part of the Protect for Windows system providing an ideal combination of confidentiality (encryption) and authenticity (digital signature). Any file can be signed

within archives of Protect for Windows system. Encrypted and signed files can be stored anywhere in the file system, sent via e-mail or backed up in the form of optionaly encrypted archives.

Main features

- the module consists of two basic parts: DECROS SAPI CSP (Crypto Service Provider) and Protected Archive
- CSP may be used for digital signing and asymmetric encrypting in all applications supporting Crypto API (MS Outlook 2000, MS Outlook 98, MS Internet Explorer)

Advantages

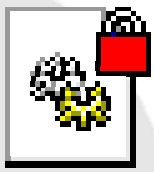
- guarantees authenticity of your signed data
- uses security tokens (Smart Card, Touch Memory, Security Box, etc.) to protect the secret key
- support for more algorithms with sufficient key length
- quality random numbers generator

Protected WCD archive

The Protected Archive application enables to keep a high number of files in a single encrypted file, the so-called „Protected Archive“ (file .wcd). This file is internally encrypted with a selected Protect for Windows encryption key and it may be safely stored, backed up and sent by e-mail as an attachment. Only a person who knows or holds the respective encryption key may open an archive created in this way. Files may be added or removed from the Protected Archive and while in the archive the files may be opened and modified (similarly as in WinZip or WinRAR). The Protected Archive may be used even if the user wants to keep the file names hidden. Individual files in the archive may be also signed with a digital signature.

DECROS SAPI CSP signed by Microsoft

(Crypto Service Provider)



The SAPI-CSP module in the system works as a provider of quality cryptographic services, capable of using all applications compatible with the CryptoAPI technology. In addition to quality and secure implementation of well-tried cryptographic methods, SAPI-CSP is also closely tied to physical security tokens available via the SAPI security subsystem. The items are used here to achieve high level of protection for the private keys.

Services provided by the SAPI-CSP module:

- electronic signature (RSA)
- asymmetric encryption of symmetric keys (RSA)
- symmetric encryption (3DES, RC2, RC4)

- hash function (SHA-1, MD5, MAC)
- random numbers generator

Parameters of the SAPI-CSP module:

- operating systems: Windows NT 4.0, Windows 95/98, Windows 2000
- supported client applications (selection of the most important ones):
  - MS Outlook 2000 SR1, MS Outlook 2000, MS Outlook 98
  - MS Internet Explorer 4.01, MS Internet Explorer 5.0, MS Internet Explorer 5.01
  - Protect 3.0
- length of the RSA module: 1024 to 4096 bits with granularity 64 bits

HW Tokens Support & PKI

Obviously, a digital signature can hardly work without its network counterpart, a so called „Public Key Infrastructure“ (PKI). DECROS is flexible in supporting most common PKI standards. The advantage of the DECROS digital signature module is the support of hardware security devices such as Smart Card, Security Box, or other smart devices for storage of user credentials.

Apart from storing information on the user and encryption keys, HW tokens are also used to protect private keys. The information is then available to the token holder, based on PIN. The tokens used most frequently by DECROS include Smart cards (DECROS Card PKI, DECROS Card Dual, DECROS Card Memory), Security Boxes - infrared or serial and Touch Memory. For more information read our leaflet with detailed information on the identification and authentication module. On request the series may be complemented with USB tokens and biometric readers.

Support for HW Security Tokens

While reducing your worry about confidential data exposure Protect will on the other hand result in a new concern about encryption keys, in particular their safe keeping. If you loose or forget the encryption key your data will be lost for good. There is no method to retrieve data from a Protect encrypted file without knowing the encryption key. An encryption specialist may attempt to decrypt the file, however, a high quality algorithm with suitably selected encryption power and key value may resist for a practically unlimited period of time. Therefore it is essential to keep the encryption keys in a safe place. The key value shall not be accessible for unauthorized persons and shall be always easily available for the data user.

The most obvious method to keep the key is to remember it. Then at any first access to the data the key value needs to be entered. The problem of this method is

that you may forget the key (particularly when you use a number of different or long key values). This results in a practice of writing them down in unsafe places or selecting key values that are easy to remember or short, thus making them vulnerable (it is easy for an attacker to guess such keys or identify them by trial-and-error method).

Still, this is not a truly efficient method for keeping, sharing and managing of encryption keys. Our company offers a number of hardware accessories enabling a truly efficient and practical keeping of encryption keys. In these tokens the keys are stored securely, however in case of loss or destruction you should think of a suitable back up, either in another token or a written record kept in a safe place.

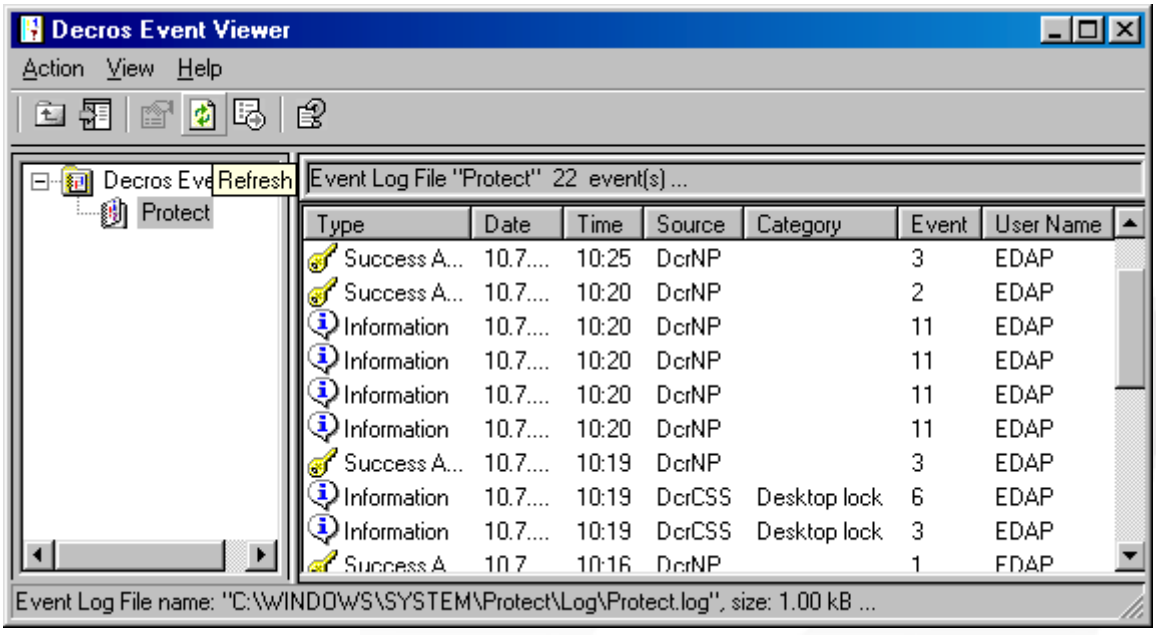
Currently supported tokens

Currently supported tokens include chip cards - **SmartCards** (DECROS Card PKI, DECROS Card Memory, ActivCard), **Security Boxes** (infrared and serial), **Touch Memory** (via serial port or via Security Card) and Security Card.

HW tokens are part of Protect Plus product series.

Recording of Performed Operations (EventLog)

Event Log is a means of record keeping about certain events in Protect for W95/98, WNT, W2000. Recorded events should help to look for conflicts, unclear issues, solutions of unexpected behavior of the system etc. Every module has a set-up group of events to be recorded. The set-up is fully manageable through a system policy and supplied templates for system policy. Each record includes time and name of the logged-on user . All events are recorded into a file protected against deleting and modification by the user.



The following may be recorded in the Protect EventLog:

- Shutdown
- Start of the encryption driver
- Driver deactivation/activation
- Encryption switching off/on
- Application for a key initiated by the user when opening the file (passed/failed /file name/process)
- Record of Protect.ini opening to make an entry
- Key/keys reading
- Keys deleting - reset
- Log-on (token, passed)/log off
- Locking/unlocking (token/passed)/automatic locking (timeout)
- Internal errors, error messages

Authentication to Windows NT/2000

Authentication to Windows NT/2000

The log-on module includes an identification/authentication module dGina, replacing the original Windows NT module and enabling to log on with HW security tokens, e.g. Chipcards DECROS Card PKI or BrainCard, infrared device Security Box or Touch Memory. Their principle is that user's name, password (or, if applicable, NT domain name) are kept in these tokens. A user wishing to log on does not need to enter the name and password via keyboard – but simply uses his personal security token (e.g. inserts a chip card or presses a button on the infrared Security Box). Thanks to this, it is possible to select powerful, random generated passwords since there is no need to remember them (the user even does not have to know the password at all). The user will use the keyboard only to enter his/her PIN designed to protect application of the security token.

The authentication module also enables to control the workstation lock with security tokens and timed set-off of the workstation lock.

Authentication to Windows 95/98

Unlike Windows NT, the log-on module for Windows98/95 includes the identification/authentication module DECROS Client that becomes a primary network client and enables to log on with HW security tokens (there is no option to avoid log-on with e.g. „ESC"). Other features and the application are identical with the WindowsNT/2000 log-on module.

Central Administration

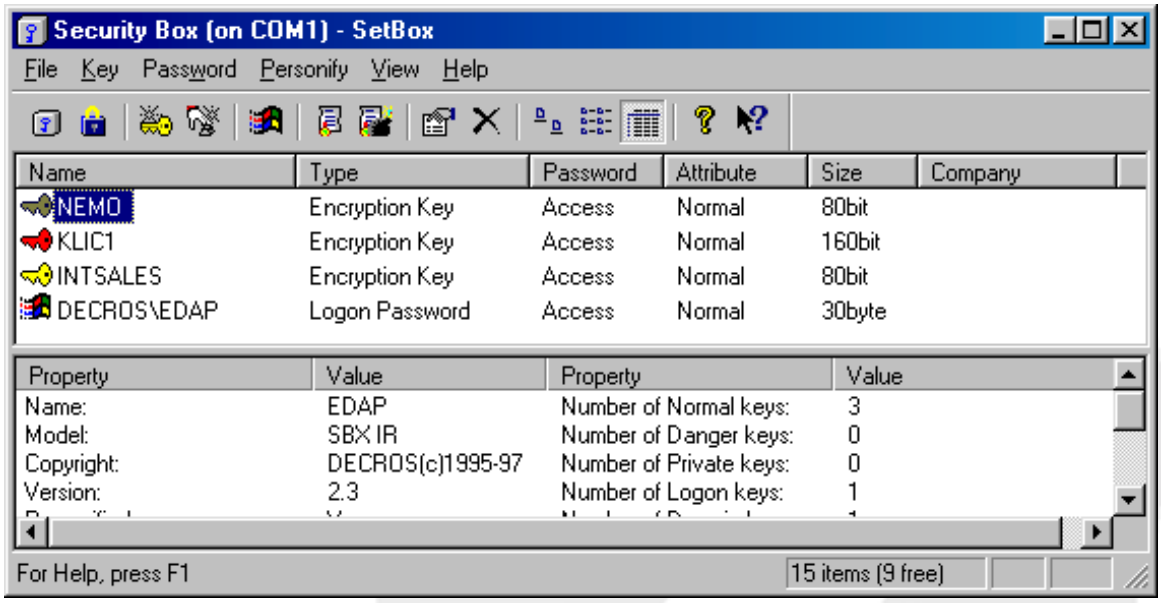
All set-ups of the Protect system are concentrated on the Protect panel and they may be remote – controlled with the system policy or available templates for system policies.

- SBXAdmin allows for the dynamic issuing and removing of cryptographic keys from one centre.
- SBXAdmin allows the key administrators to enter the company cryptographic keys and log-on information into the user Security Box without the administrator having to know the access code (PIN) for the Security Box.
- The administrator may deny the user write into the Security Box or limit the user's entry (for example to one private cryptographic key). The users may not rewrite or delete the company keys.
- SBXAdmin collects all company information entered in the Security Boxes into a single database and allows for the effective backing up of the company section of the Security Boxes.
- SBXAdmin allows for the transfer of responsibility for the content of the Security Boxes to the key management administrator, i.e. typically to an individual who is outside the circle of network administrators and who does not have access to the user data.
- The Security Box may be administered from a distance at the client's station. This means that the user does not have to physically carry the Security Box to the key administrator. The SBXAgent section of the central administration program serves this purpose. SBXAGENT_QUICKLY.

SetBox

Utility for HW token management:

- add/remove encryption keys
- store into HW token log-on information for Windows



Documentation

All modules naturally include documentation, in form of HTML help, divided into two sections – one containing basic information for users and the other for IT administrators.