PROTECT for Windows™

Main Advantages the PROTECT for Windows™ Technology in the Windows 2000 Environment

DECROS®

Table of Contents

Microsoft Windows 2000

By introducing Windows 2000 Microsoft has made another major step towards a next generation system of applications, much more open for users and administrators.

The particularly praised qualities of the new operating system include:

- its advanced architecture, offering more stable and more reliable operation, with the option of dynamic configuration of the system;
- easier administration of the system, in terms of installation, configuration, as well as maintenance;
- maximum compatibility with Internet and intranet applications;
- application of the most advanced computer technologies (PnP, USB, IrDA, ...);
- full-scope localization

The open nature of Windows 2000, however, will also mean the necessity to increase the security level which has, in comparison with Windows NT, acquired new dimensions, especially in the following areas:

- data encryption at the file system level
- use of chip cards for identification and authentication of users
- central administration using Active Directory, Microsoft Management Console and Group Policy Editor

DECROS has prepared Protect also for Windows 2000 and this document outlines basic assets of the said technology in the Windows environment.

Encrypting on various files servers

A novelty in Windows 2000 is the function enabling to encrypt sensitive data, as set up by the administrator. This function represents a major plus compared to Windows NT or Windows 98, as it gives you the additional opportunity to protect information whose disclosure might be of strategic importance to you or your organization.

File encrypting in Windows 2000 is based on an improved EFS (Encrypted Files System), a part of NTFS 5.0. The encrypting process has been programmed in manner so that the authorized user is not bothered by the encryption process course, encryption keys or other encryption parameters.

A certain disadvantage of this security function is its linkage with EFS, as it is impossible to work with the sensitive data safely as long as they are stored on a medium which does not support EFS, e.g. on a diskette or a ZIP driver. Naturally, this type of protection cannot be used on different files systems, such as FAT, FAT32, NTFS, EXT2 (Linux), now quite widespread.

It should be also noted, that encrypting only concerns the local disc (with EFS) or network disc (with EFS), as long as Windows 2000 Server has been installed.

PROTECT for Windows and a Files Server

The Protect application offers a well-tried encryption technology, based on transparent symmetric encrypting on the files system level. Encrypting with Protect is not limited by any files system: a file may be transparently encrypted in any location where the user may store it via the Explorer in Windows

This means Protect enables protection of sensitive data on diskettes and other replacement media, including CD-ROM, on files systems FAT, FAT32, NTFS and, of course, on all Files Servers supporting Windows
- e.g. Unix, Linux, Novell etc.

Naturally, the sharing of sensitive information is also possible in peer-to-peer networks made up of, e.g. Windows 98.

File encrypting on a server and performance distribution

As described in the chapter above, integrated encryption in Windows 2000 is a new security feature. The encryption is transparent, at the files system level. Physically, the encryption is performed by the station in which the file is stored.

Encryption of sensitive information stored on a Windows 2000 server is performed by the server, which results in two effects:

- The loading of the server increases. As a result, any information sharing may dramatically increase demand for the server's system capacities. This effect may be eliminated by increasing further the server's technical capacities.
- During communication between the station and the server the information remains unprotected.

PROTECT for Windows in a network

The Protect application, on the other hand, always provides for physical encryption on the very station where the user is working. The sensitive information is decrypted only into a protected memory of that particular station. The information is first encrypted in the station and only then, already encrypted, it is stored into the server. This method in no way increases the server's loading and still it enables full-scope services to the user, including sharing of the protected information.

Moreover, Protect protects the information during its transmission, since the information travelling in communication channels is already encrypted. As a result, it is no more important whether a particular communication channel is secure or not. Without the secret value of the encryption key no information protected in this way can be disclosed.

Files Sharing

Similarly as other Windows systems, Windows 2000 also offers the option to share information in the form of files.

However, when the files sharing feature is used, EFS have demonstrated some problems for users and administrators.

First of all it should be noted, that in the current version of Windows 2000 (with integrated EFS in version 1) the sharing feature is quite limited as one file may be shared only by two users: as a standard, one of the users shall be the file owner and the other one shall be the so-called Key Recovery. Due to this fact it is not suitable to apply EFS protection for the shared information.

Unlike this, Protect has been designed for sharing of files protected by encryption. Protect uses symmetric encryption which enables files sharing and processing by all users who are “holders” of the encryption key.
To become such a “holder” , the user shall either know the secret value of the encryption key (and enter it via keyboard) or hold a personal security token (e.g. Security Box, Smart Cards etc.) containing the secret value.

Another major feature of Protect, if compared to encryption within Windows 2000, is that a user logged on into Windows 2000 may immediately access all sensitive data, which may pose higher risks of data damage by e.g. „Trojan horse “ or viruses. In case of Protect the user may log on independently (with a personal security token) and then work with the system. No “Trojan horse” or viruses will be able to attack or disclose the encrypted data because they are not accessible; such infiltrations may be even exposed in this way as their activities may result in a request for the encryption keys. The access to sensitive data is provided to the user only at the moment the information is needed for work.

Data Protection Against Technical Personel

A number of Windows NT users and administrators have encountered the requirement to protect sensitive information against the administrator. The requirement is in many cases beneficial for both sides, in particular if strategic information or secret information under Act 148/1998 Coll. is involved.

Although the Windows 2000 operating system brings new features in the data security field, the system of data protection against administrator has not changed significantly. In Windows 2000 each encrypted file has the so-called Key Recovery, a special key by which the station or server administrator may decrypt and read the encrypted information. The security of such sensitive data then again depends on the administrator's credibility.
Also in this system, all any potential attacker needs to do is to sneak into position of an administrator of the station or the server.

PROTECT for Windows as a Protector

In terms of protection against technical personnel, Protect offers a different security level. It provides not only protection to the organization but also to the administrators who are able to prove their non-involvement in data abuse as they have no access to the information. Usage of your own encryption keys is easier with security tokens and their central administration.

Moreover, in case the secret value of an encryption key is disclosed, either accidentally or on purpose, only the information protected by this particular encryption key will be at risk while the remaining secret data will be safe.

Various Security Tokens

As mentioned above, encryption is not by far the only new security feature. There is also identification and authentication of the user with a personal security token, called Smart Card.

The Smart Card may store a personal user's certificate to be used after log-on. Subsequently, a PIN code is requested and verified by the system, to check authorization of the security token holder.

DGINA

This method has been used by DECROS for a number of years in Windows NT, Windows 95 and Windows 98 and based on Microsoft sources, DECROS was the very first company to create its own log-on module for Windows NT, the so-called dGINA.

Other Tokens

Thanks to the openness of the DECROS system, also fully integrated in the Protect application, other physical tokens may be used as well, including Security Box Infrared, Security Box Serial, Security Card, Touch Memory and Smart Cards.

What is more, using our specifically developed SAPI (Security API) interface, it is possible to integrate new tokens into the system, such as those already in use in your company for doors opening, electronic purses, etc. SAPI also offer another exclusive opportunity – the integration of physical tokens function into key software applications used by the company; e.g. access into the company's economic agenda will be enabled only to the user with a Smart Card specifically identified by the company.