Protect for Windows™

Protect™ is an easy to use yet complex security solution designed for protection of sensitive company and personal data.

The security functions of **Protect**™ consist of the following modules:

- Encryption module
- Identification/Authentication module
- Digital signature module

Digital Signing Module

In the electronic world digital signature represents an equivalent of a signature written with your own hand. For a user it serves the same purpose: to verify authenticity of a document or data file. Only its form is slightly different. Digital signature is a number computed based on the undersigned data and therefore it cannot be even copied on another document. The role of digital signing has grown dramatically with the development of electronic banking, Internet payments, digital money and other areas requiring reliable transmission and authenticity of data in electronic networks.

DECROS®
Security to fit your Information System

Principle of the Digital Signature

Digital signing is a method to protect data authenticity by using asymmetric encryption. To function, asymmetric encryption not only requires a workstation on which the electronic documents may be signed, but also a functioning network environment with certification authorities, registration servers, directory databases etc. i.e. a system called Public Key Infrastructure (PKI).

Using the original file the author computes a short hash. Hash is a very complex one-way function which transforms content of the original file into a short block of data. Hash function has one unique feature causing that a single different bit in the original file will, with very high probability, result in a completely different output value of the hash function. On the other hand, there is no way to convert a hash back into the original document. The hash is then encrypted with a secret key by the data author. The resulting group of data is called a digital signature. Since this secret key is only known to the author of the original document no one will be able to create the same signature on the original document. The signature is enclosed to the file and dispatched to the addressee.

The addressee shall know the author's public key. Using the public key the addressee will decrypt the received file and get to the original hash. This hash is then compared with a hash computed by him from the received file. If the two values are equal the data have been authenticated with high probability.

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. Individual files in the archive may be also signed with a digital signature.

DECROS SAPI CSP (Crypto Servis Provider) signed by Microsoft

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 (as 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

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.

Contact:
DECROS Ltd.
J. Š. Baara 40
370 01, České Budějovice
Czech Republic

Tel: +420 - 38 731 28 08
Fax: +420 -38 731 14 80
Sales@decros.com
http://www.decros.com

DECROS®
Security to fit your Information System