

NetCrypt

CLIENT SERVER CIPHERED SHARE

CONFIDENTIALITY, SECURITY AND PRIVACY

The confidentiality of data is a subject of great interest for companies and professional people, both due to the extreme vulnerability of computer systems, that are constantly under the dangers of the net (virus, worm, dealer, spam, etc.), and due to the increased value that business data have achieved for companies' competitiveness.

Moreover, the law on privacy has added precise obligations for the treatment and ciphering of personal and sensitive data.

CIPHERING: THE SOLUTION

The ciphering system is made up of a server module, installed on the computer server, that allows to do the ciphering of the folders you want to make reserved, and of a client module, that allows the users to have access to the ciphered documents. The product is based on the AES 256bit motor of symmetric ciphering, which does the ciphering and deciphering of files of different format and size. The access to ciphered information is protected by Strong Authentication (password + USB key): if someone had access to the server, the ciphered information would be completely unusable. Even if the server and the USB ciphering key were stolen, the access would be protected by the deciphering password.

Advantages

- It supports all Windows system files (FAT, FAT2, NTFS) and other file-sharing record (Samba, Novell, etc.)
- Strong Authentication with USB token
- File ciphering on any memorisation support
- The client-side ciphering guarantees the confidentiality of the file transport on the net
- Multi-user access to ciphered documents
- It can be integrated with Windows log-in user
- It is clear to backup procedures
- Recovery procedure for any document in case of loss or break of the USB key

NetCrypt server

- AES 256bit motor of symmetric ciphering (ciphering of any file format)
- Access to the server console with administrative USB key
- "Click&Crypt" quick selection of folders
- Timer for automatic disconnection
- Files automatic ciphering in the clear
- Importation and exportation of certificates
- Interface of USB client key programming and certificates administration

Technical data

- Cryptographic protection of local files and in the net
- AES 256 bit ciphering algorithm
- Management of the ciphered files share
- Management of ciphering multiple certificates

NetCrypt client

- Clear opening of ciphered files (double click)
- Safe deletion of temporary files (Wipe Delete)
- Ciphering function integrated in the contextual mouse menu