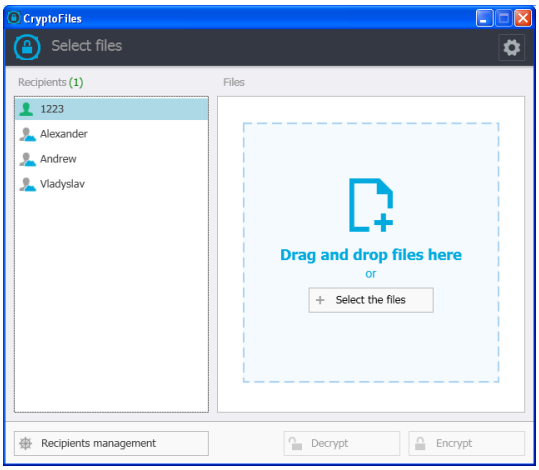
"AVTOR" LLC.
Smolens'ka St., 31-33, Kyiv, 03005
T/f (+380 44) 538 00 89
author@author.kiev.ua
author.kiev.ua

Software "CryptoFiles"



Software "CryptoFiles" is designed for encryption and exchange of all types of files.

"CryptoFiles" provides the ability to share files by sending an encrypted container (file) to the recipient via the cloud storage, e-mail or on any storage device.

Software "CryptoFiles" provides:

- ✓ safe and secure storage of important files in an encrypted form, including files in the public cloud storage;
- ✓ exchanging files in encrypted form between the different user devices (work and home computer, laptop, tablet, mobile phone);
- ✓ sharing files in encrypted form with other users with the ability to group and individual addressing;
- ✓ ability to store various user files in one encrypted container , including structured in different folders;
- ✓ ability to create fully protected logical drive.

Security

Secure storage and transmission of encrypted files is provided by reliable cryptographic system with public keys and is determined by the following basic principles:

- ✓ each user has two related keys – public and private;
- ✓ public key is used to encrypt the file which have to be transferred to the owner's of private key (public key is not secret);
- ✓ users must first exchange public keys between each other in any convenient way for opportunities to exchange of encrypted messages(by e-mail, transmit on Flash-drive, or use the cloud service provided by the program);
- ✓ private key is located only at its owner and only with it help files can be decrypted;
- ✓ to store the private key user can use a secure repository software or hardware devices;

- ✓ software repository provides storage of the private key in encrypted form in the computer memory;
- ✓ hardware devices provide maximum protection for the private key. As hardware devices are used smart card or USB-tokens. They provide key generation in the device, wherein the private key never leaves the device and extract it therefrom is not possible. Decryption key for each file is unique and is formed inside the hardware device using a private (secret) user's key.

Specifications

Specifications of used cryptographic algorithms:

- ✓ generation of key information in accordance with DSTU 4145-2002 (key length - 163-509 bits) and RSA (key length - 1024-4096 bits);
- ✓ encryption/decryption of files in accordance with DSTU GOST 28147:2009 and AES (256 bit key length).

Advantages of software "CryptoFiles":

- ✓ optimized algorithms of encryption large amounts of data;
- ✓ support for working with cloud services;
- ✓ support for hardware storage of key information;
- ✓ convenient and intuitive graphical user interface;
- ✓ ability to export/import settings and the list of recipients;
- ✓ exchange and synchronization of public key certificates by using "CryptoFiles" cloud service;
- ✓ embedded system of updates;
- ✓ support of all Microsoft Windows operating systems.

For free download **software "CryptoFiles"** please visit the company "AVTOR" site: http://cryptofiles.author.kiev.ua/setup.exe.

You can purchase hardware devices for secure storing of key information (smart card "CryptoCard-337", USB token "SecureToken-337" or "SecureToken-337F" with FLASH-memory) in the online store of the company "AVTOR": http://www.author.platimo.ua/index.php?categoryID=8.