

CyberSafe TopSecret User's Manual

© 2012 CyberSoft Ltd

CyberSafe TopSecret User's Manual

© 2012 CyberSoft Ltd

All rights reserved. No parts of this work may be reproduced in any form or by any means, whether in print, electronic, or mechanical, including photocopying, recording, taping, or any other information storage and retrieval systems without the written permission of the publisher.

Products referred to in this document may either be trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be held liable for any loss of profit or any other commercial harm caused or alleged to have been caused directly or indirectly by this document.

CyberSafe Certificate Authority

Special thanks to:

*The management and employees
of Dorf LLC, especially T.S Zhukova*

Publisher

*"CyberSoft", LLC
Eugene Zhukov*

Technical Editors

*Sergei Vasilchenko
Vadim Filatov*

Cover Designer

Alexander Vostrikov

Team Coordinator

Dmitry Belyaev

Production

Dmitry Sirotkin

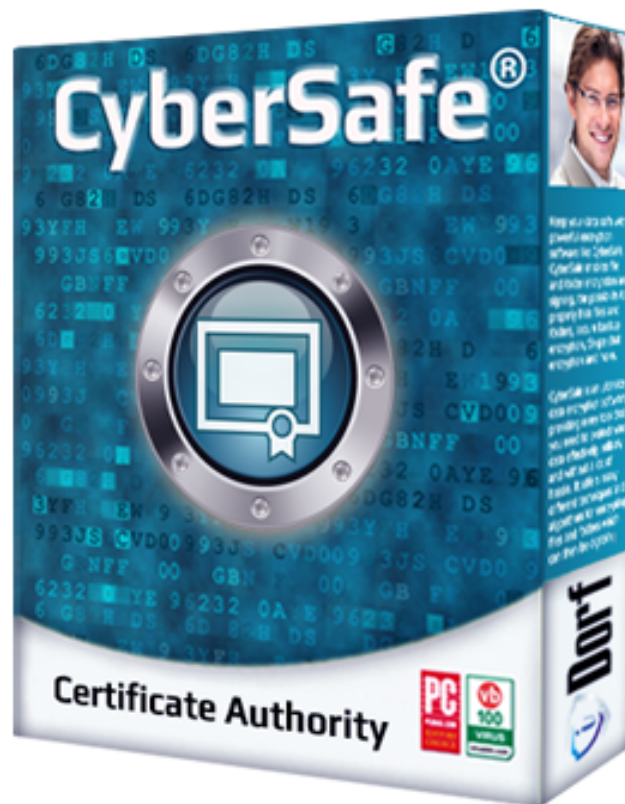


Table of Contents

Part I License agreement	5
Part II Installation	7
Part III Stealth mode	13
Part IV Working with ID	15
1 General information about ID.....	15
2 Import.....	19
3 .pid files.....	21
4 .id files.....	23
5 .pfx files.....	24
6 .skr files.....	26
7 .cer files.....	27
8 .asc files.....	28
9 Exporting ID.....	29
10 ID search.....	30
11 Features.....	32
Notation conventions	32
Change ID images	33
Allocate by default	33
Deleting an ID	34
Encryption by default	35
Signature by default	37
12 General principles of using CS with keys.....	37
Part V File Encryption	41
1 MS CSP.....	41
Auto - For official use	41
Auto - Secret	41
Auto - Top Secret	42
Manual - EFS	42
Manual - PKI	42
Manual - Blow Fish	43
2 GOST.....	43
Secret	43
Manual - PKI	43
Digital signature	43
3 OPGP.....	43
4 Data masking.....	43

5	Decrypting.....	44
6	Verifying a signature.....	44
Part VI CS explorer		45
1	Work with hidden objects.....	45
	Tag and running of files	47
	Disable masking	48
	Unmask all	48
2	Amazon S3.....	49
	Create a bucket	50
	Create a folder	51
3	Scheduler.....	52
Part VII Crypto disks		55
Part VIII Generating		57
1	Mounting.....	58
2	Auto-mount.....	59
Part IX E-mail encryption		59
1	Outlook.....	59
2	The Bat!.....	64
Part X Encryption of Skype		65
Part XI Methods of information theft		68
1	Trojan.....	68
2	Remote Desktop.....	68
3	Seizure of PC by law enforcement authorities.....	70

1 License agreement

License agreement

LICENSE AGREEMENT FOR PRODUCT USE.

1. Terms and definitions.

1.1. The present License Agreement is a general offer between "Dorf," OOO and the User, which can be an individual or legal entity. If the user does not refuse to agree within 7 days of the date of purchase, this License Agreement shall have the force of a contract, as set forth in Art. 433 of the Civil Code of Russian Federation.

1.2. The Product is a set of computer programs, including media and documentation, which is copyrighted and protected by law.

1.3. Throughout this text, the word "documentation" refers to printed materials and media contained within the documentation in electronic form. This documentation is an integral part of the Product.

1.4. The present Product (software), including media and printed materials are covered under the conditions of the License Agreement.

1.5. Subsequent installations of the Product shall be considered equivalent to acceptance of the conditions of the License Agreement and it therefore enters into legal force.

1.6. If the user disagrees with any of the conditions of this License Agreement, the User must return the complete Product, including the printed materials and packaging and media to the company that provided said product within seven days.

2. Scope of the Agreement.

2.1. The Scope of the present License Agreement is the compensated transfer to the User of rights to use and own the Product.

2.2. All conditions stipulated hereafter shall apply both to the Product in its entirety and all its component apart.

3. Copyrights.

3.1. The Product and all its components are the intellectual property of the developer and are protected by copyright law.

3.2. The right to use this Product is given only to the end User as the owner, and not to any other third parties, unless there is written consent from "Dorf," OOO stating otherwise.

4. Conditions of use.

4.1. The User can save, install and use only a certain number of copies of the Product. The user does not have the right to save, install or use (in the installed or uninstalled form) more copies of Product than given to him as determined in the relevant documents for the right to use the Product.

4.2. The user agrees not to distribute the Product. This includes access for third parties to reproduce the product in any form or aspect, by sale, rental, lease, and lend or any other method of transfer.

4.3. User does not have the right to undertake the following activities: ☐

- To allow people to use Product who do not have right to do so;
- To try to disassemble, decompile (convert compiled code into source code) the programs and other components of the Product;
- To make any changes to the compiled code of the programs except for those, which bring in programs, included in the set of the Product and listed in the documentation;
- To use the Products to perform any actions that violate Russian and/or international rules regarding copyright and use of software.

Note. The use of encryption tools for the cryptographic protection of information is subject to licensing in accordance with acting legislation of the Russian Federation.

5. Term of validity of the Agreement.

5.1. The present License Agreement shall enter into force upon opening the package with media or install software from the set of the Product and it shall remain valid throughout the term of the Product's usage.

5.2. In the case of a violation of the License Agreement or the inability to continue to fulfill its conditions, all components of the Product (including the printed materials, magnetic media, information files, archive copies) must be destroyed.

The user must confirm the destruction of the Product in writing. At this time the License Agreement shall no longer be in effect.

6. Liability.

6.1. The user purchases the product and is liable to insure that it is used in accordance with the stated recommendations in the maintenance documents.

6.2. Illegal use, distribution, reproduction for the third parties or copying of the software is a violation of the Law of the Russian Federation "Legal protection of programs for computers and databases" and it will be prosecuted to the full extent of the law.

6.3. In the case of a violation of this License Agreement, the User shall not be entitled to use the Product and the warranty for the service of the Product will be void.

7. Manufacturer's (supplier's) warranty.

7.1. The manufacturer guarantees the working ability of the Product in compliance with the requirements for operation, transportation and storage, with proper use and use of the Product in a "non-viral environment".

7.2. In the case of detection of defects in the programs not related to a violation of the rules of operation,

transportation and certificate storage, the product is subject to reclamation within 10 days from the time of detection, and the manufacturer shall undertake on receipt of notice of a claim as soon as possible to eliminate defects at its own cost, up until the delivery of a new product, as well as to take measures to avoid these defects in all other copies of the product.

7.3. The warranty period is set at 12 months.

7.4. The initial date for the calculation of the warranty period is the date of delivery of the product, which is recorded on the form.

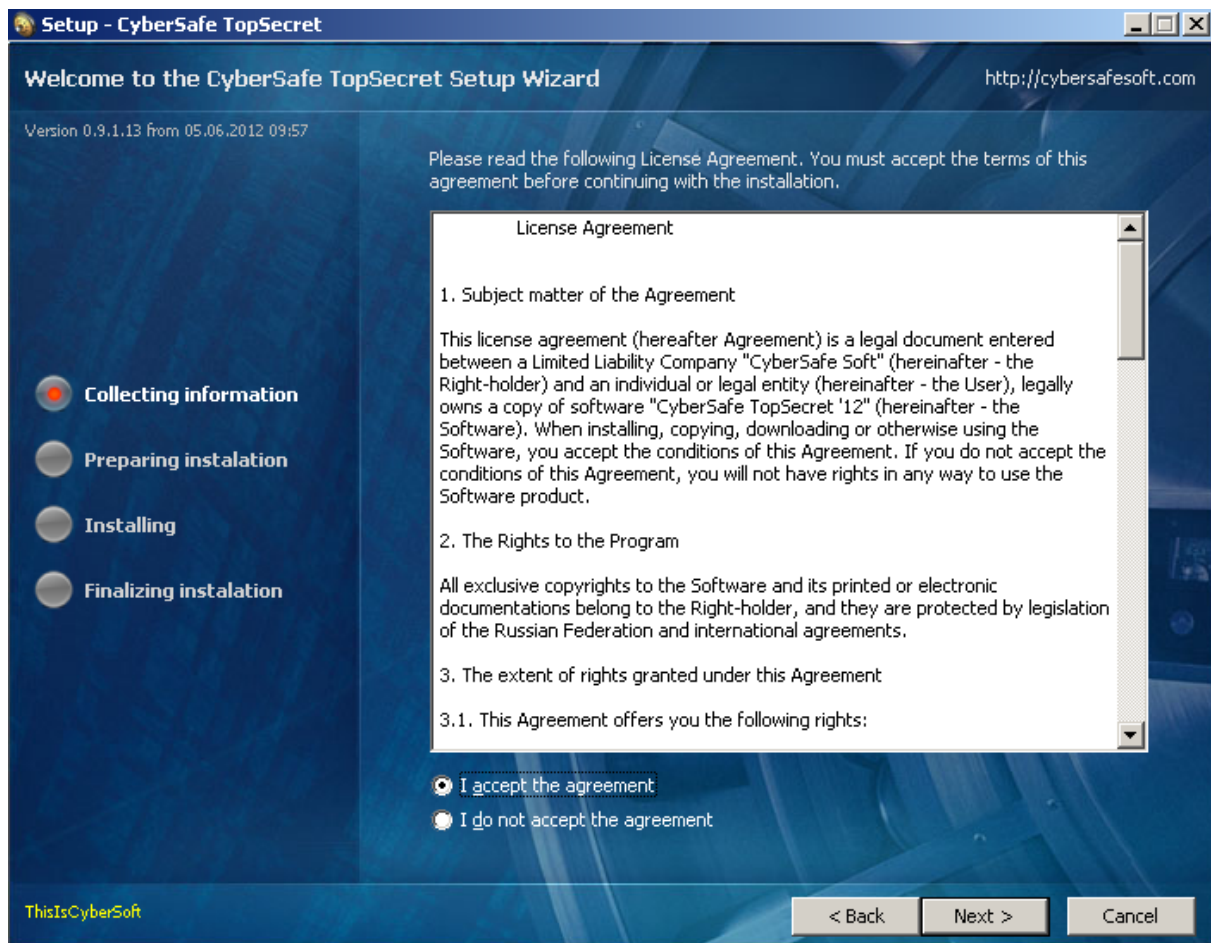
7.5. The manufacturer (supplier) shall accept claims concerning the quality of delivery of Product within thirty days of the date of delivery.

7.6. The validity of warranty obligations shall be terminated after expiration of the warranty period.

2 Installation

Installing CyberSafe included of the following steps:

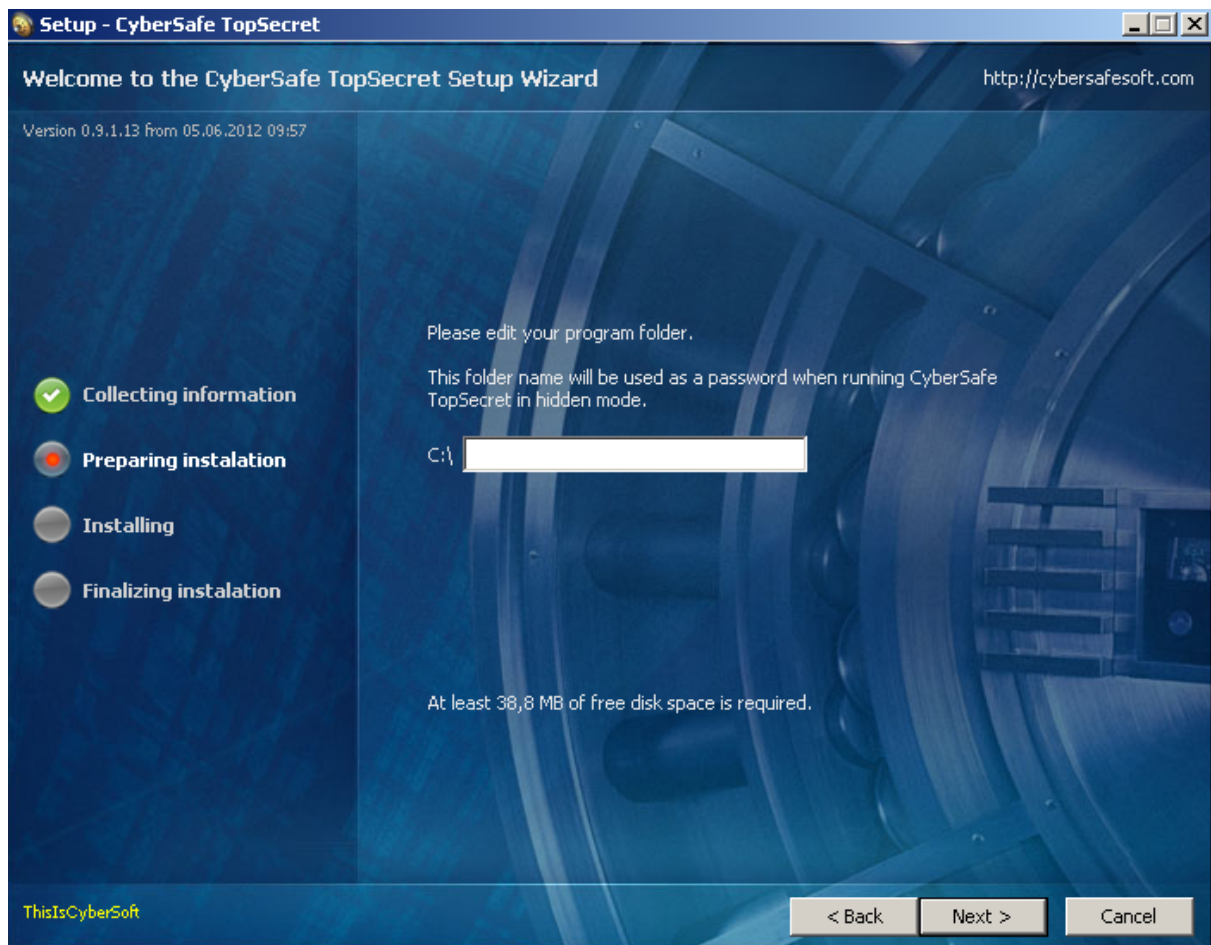
1. Download the installer, "cs_setup.exe" at <https://cybersafesoft.com/cssetup.exe>.
2. After you save the installation file on your PC run it. To install the CS will require administrator rights.
3. After reading the license agreement, tick the "I accept the agreement" and click "Next".



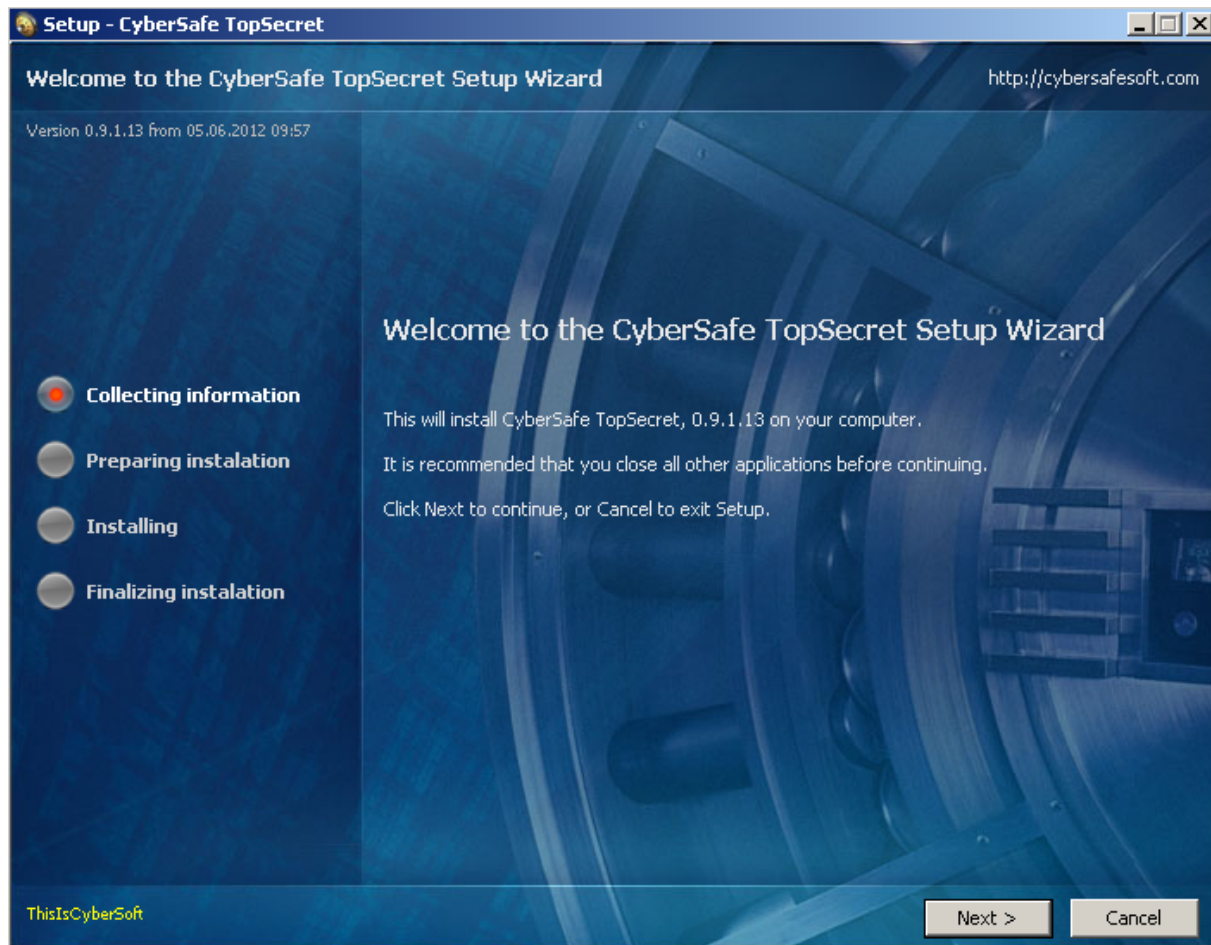
The version of Top Secret contains a "Folder - password" field in the stealth mode. Stealth mode is designed to ensure that CS cannot not be found, except by the user of PC. The existence of CS itself is hidden on the PC. Therefore, to run CS you should know the folder in which the CS is installed. Thus, the installation folder is the password to run CS. More information about how to run the software in stealth mode see the "Stealth mode".

4. Put desired password in the field. The password is represented in the form of the folder that's why there is a characters restrictions for the directories of Windows.

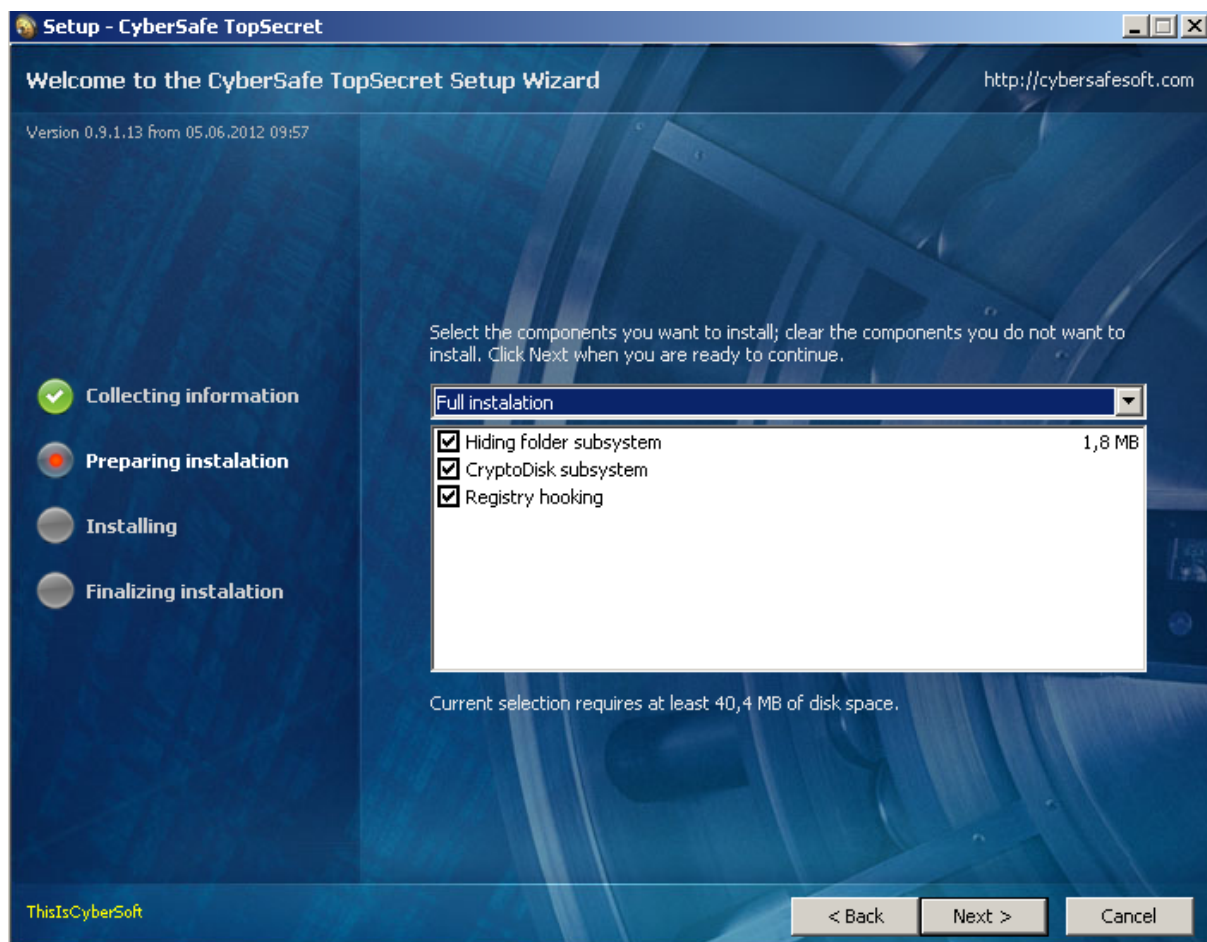
By default, the software will be installed on the C: drive, but the user can select another disk.



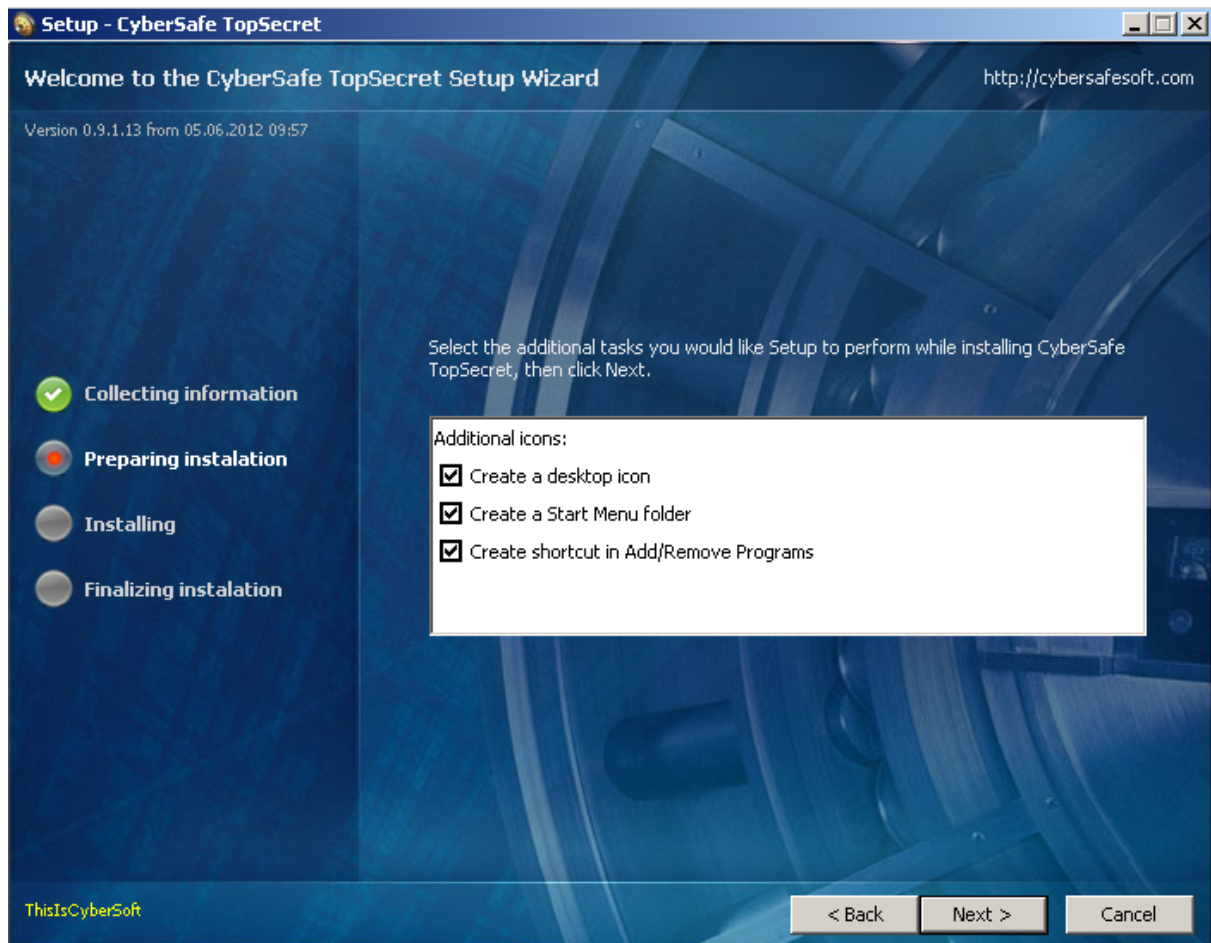
The beginning of CyberSafe installation:



5. Next step, select the components which you want to install.



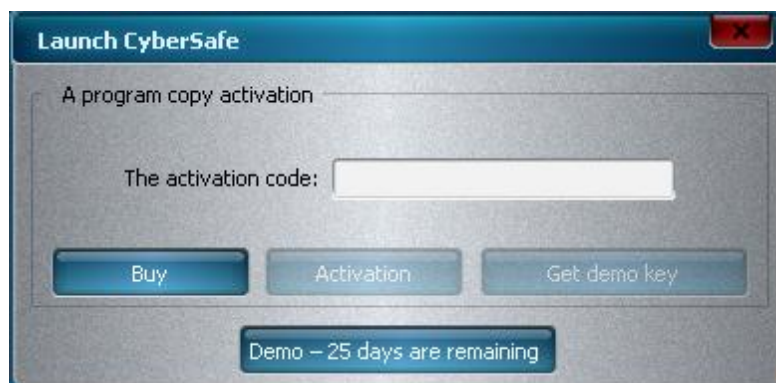
6. Select the additional tasks, that must be performed during installation CyberSafe.



After you click "Next" copies of files and registration of libraries will be made. Also the changes will be made to the parameters of EFS. To apply these parameters you will need to restart your PC. However, without restarting all the features of the software will be available, except for EFS encryption.



***If you purchased the CS, enter the received license key
otherwise, press the "Get Demo Key." In demo mode, CS has no functional limitations,
however, the term of the trial, limited to 30 days.***



3 Stealth mode



The fact that the PC has the encryption programs, encrypted files, and programs to hide files and so on is a fact that is suspicious in itself. The best information protection comes from hiding the very fact of protection.

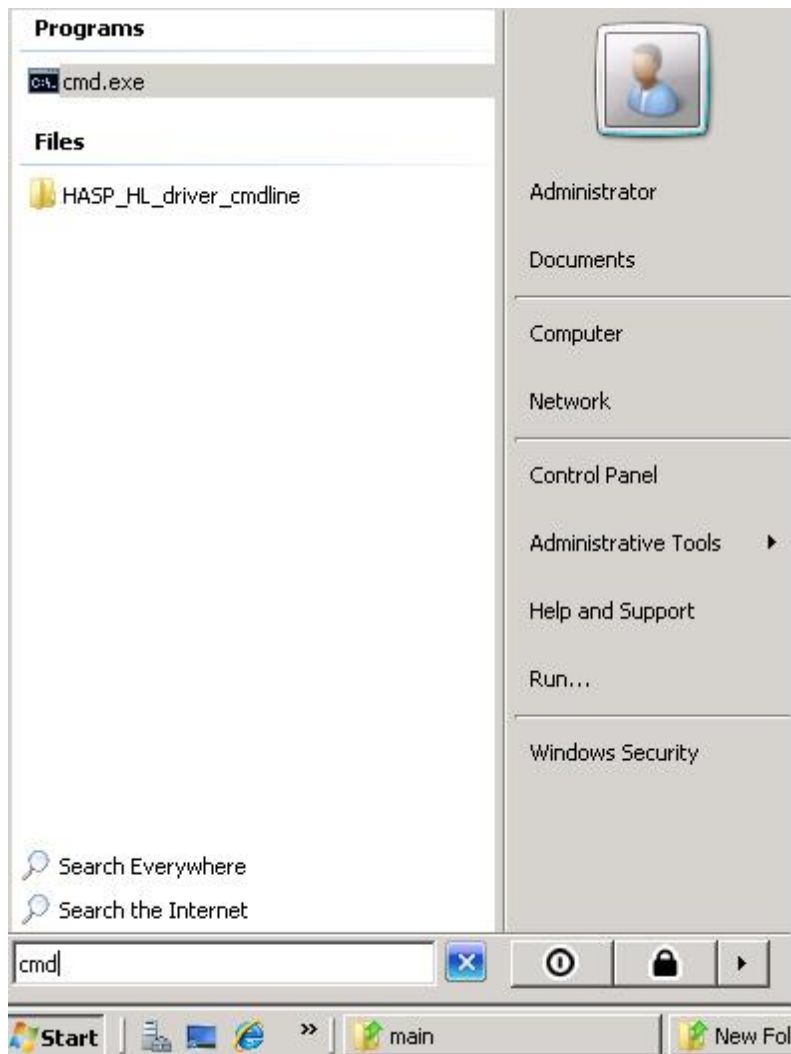
To these ends, CS Top Secret can operate in stealth mode. There are no traces of CS having been installed in the registry, control panel or system processes, or on the drive. The installed encryption keys are never left in certificate storage. The existence of CS is not hidden after it has been started or during its operation, otherwise the user would not be able to work with the program. However, before it is started, the existence of installed CS on your PC can be detected only using circumstantial evidence, and only by specialists who know the features of CS. To achieve optimal operation it is recommended to not leave encrypted files in a visible state in stealth mode.

For instructions, see the chapters "For official use ", "Secret" and "Top Secret ".

How to run the software in the hidden mode:

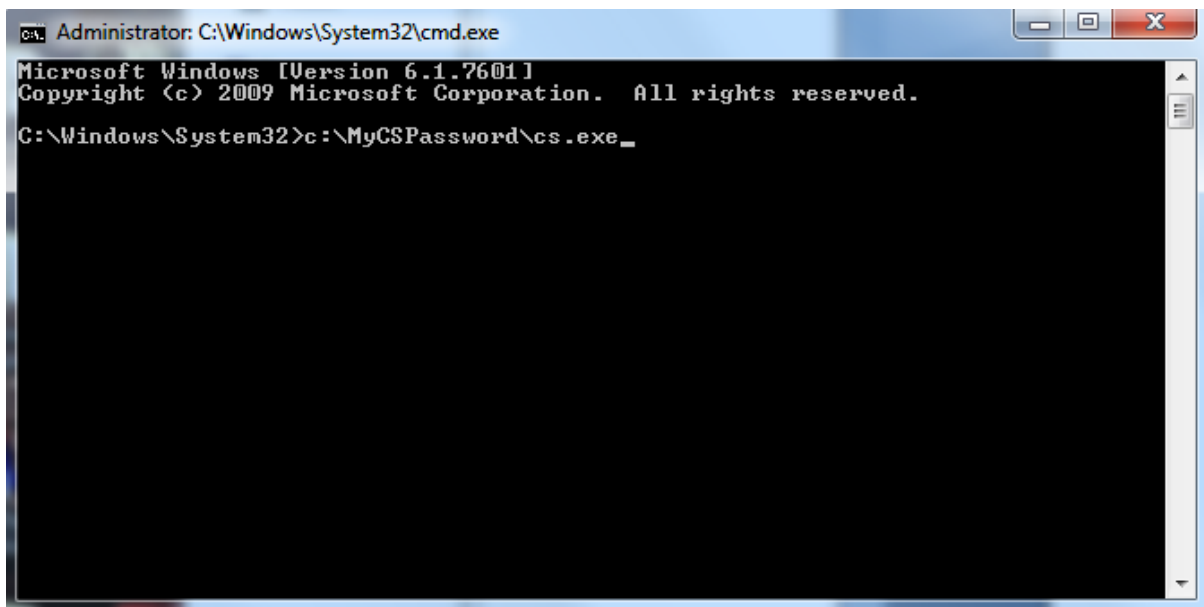
1. You need to enter a command line as an Administrator.

The easiest way to do this is clicking "Run" and typing «cmd» (without the quotation marks) in the search bar, (do not confuse this procedure with the procedure to run («Windows-R»)) and then pressing CTRL-SHIFT-ENTER.



You could also make a shortcut to cmd.exe, which is located in c: \ Windows \ System32 \ and run it as an administrator.

2. After you run the command line, enter the password that the user chose during the installation of the CS in hidden mode as follows: c: \ MyCSPassword \ cs.exe where "MyCSPassword" is the password selected by the user.



4 Working with ID

4.1 General information about ID

The electronic IDs of CS are encrypted zip archives, which contains the following elements:

- .pfx File(s). (for MS CSP certificates, the public and private keys)□
- .cer File(s). (user's certificates)□
- .jpg File. (graphic form of authenticator with full details and photo of the owner)
- .p7m File. (DS for jpg that makes it impossible to fake a picture)□
- .skr, .pkr File(s). (OPGP public and private keys)□
- .gsec, .gpub File(s). (GOST public and private keys)

Personal identifiers contain both public and private parts of the key and they have the extension of .id. The public identifiers are the only open parts of the key and they are not encrypted and have the extension ".pid".

IDs are stored in the Private and Public folders in the working directory of the software. For greater security, IDs can be stored on a flash drive or a FrontLine biometric token (<http://cybersafesoft.com/frontline/>).

Creating a new ID

1. It is recommended to fill out all the fields that the user wants to be included in the ID.

The screenshot shows the 'Creating identification' window in the CyberSafe software. The window has a title bar with 'CyberSafe' and 'Version: 0.9.0.3'. Below the title bar are tabs for 'Identifications', 'Explorer', 'CyberSafe', and 'Settings'. The main content area is titled 'CyberSafe ID' and contains a sidebar on the left with 'INFORMATION', 'SETUP', and 'ISSUE'. The main area is titled 'Personal data for identification' and contains the following fields:

- Password for ID*: [Redacted]
- Name*: [Tester]
- Email*: [tests@cybersafesoft.com]
- Company: [CyberSafe]
- Unit: [IT]
- City: [Ontario]
- Photo: [C:\Documents and Settings\1\Desktop\myphoto.JPG]

There is a 'Browse' button next to the Photo field. At the bottom of the window are 'Cancel' and 'Next' buttons. A note at the bottom left says '*- Required data'.

2. On this screen, the size of the keys should be selected, as well as the crypto providers, with which the user is going to use it. MS CSP cannot be disabled. The GOST crypto provider is available only after installation of Crypto-PRO CSP.



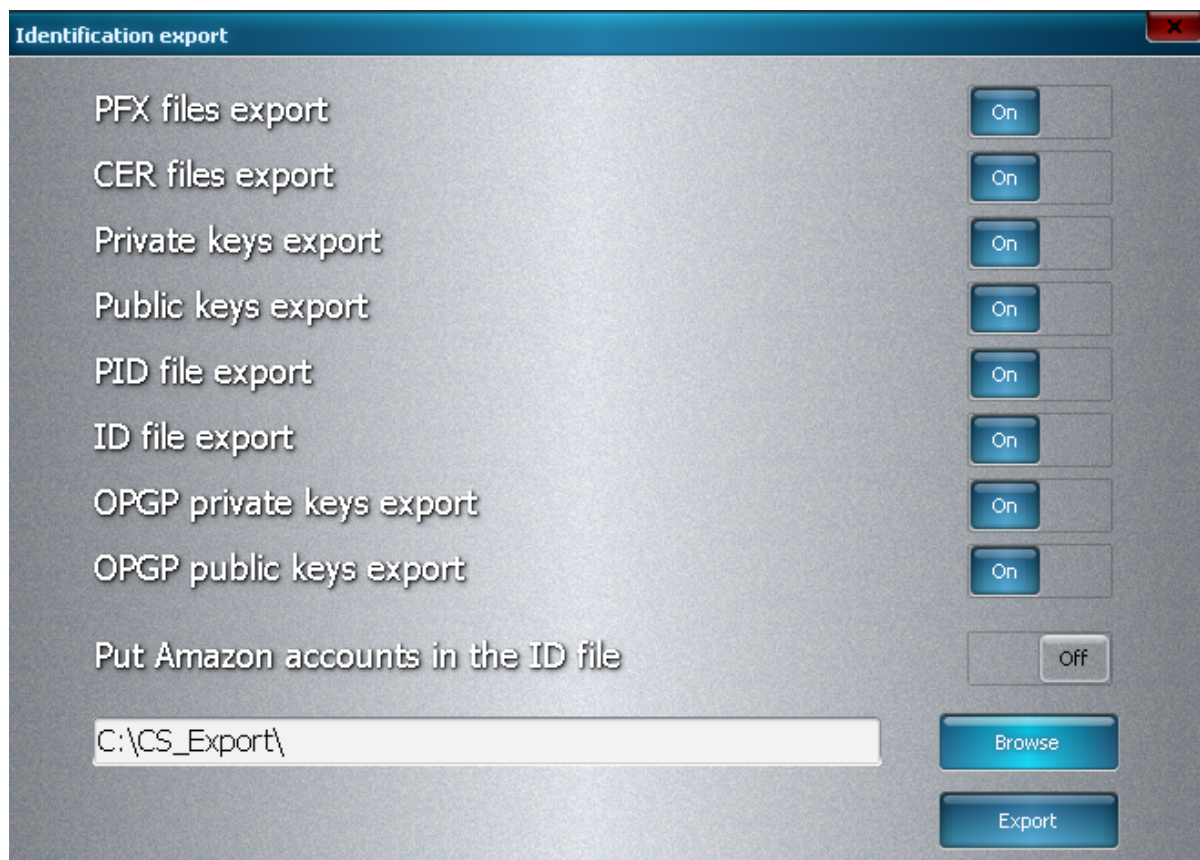
The larger the key size, the longer it will theoretically take to issue, as well as the time spent on the data encryption. That said, this will also increase the degree of complexity your data will need to be decrypted. However, in practice the time spent issuing and encrypting, even with key 4096 on a modern PC is insignificant, while the reliability of the encryption increases substantially. In 2011, the most guaranteed encryption is encryption by a RSA 2048 bit key and AES 256 bit algorithm.

The option "Publish on the server" allows the user to upload the public ID on the server so everyone could encrypt the data for him.

3. After clicking "Next" CS will generate keys, create certificates, graphic files, digital signatures and place them in the archive, which will be encrypted by password and will have the name of user's e-mail with id extension. The chosen password should be as long as possible. If the user is not going to keep the certificates on a flash drive or token to remember the password is not required. However, we strongly recommend making a backup copy of the ID and putting it in a safe place with the indicated password. In the case of recovery or transfer of CS a password will be required for id.

Exporting ID

In the export form, the user selects the desired items for .ID export and the directory to where they will be exported. The password for all elements of the hidden parts of the keys corresponds to the password, which was specified during the creation of the ID:



The export of an ID and all of its elements are required to backup your personal ID and to exchange the public keys with other participants of the encryption process.

All the elements of ID will be more particularly described in the chapters called **"Compatibility"** and **"E-mail protection"**.

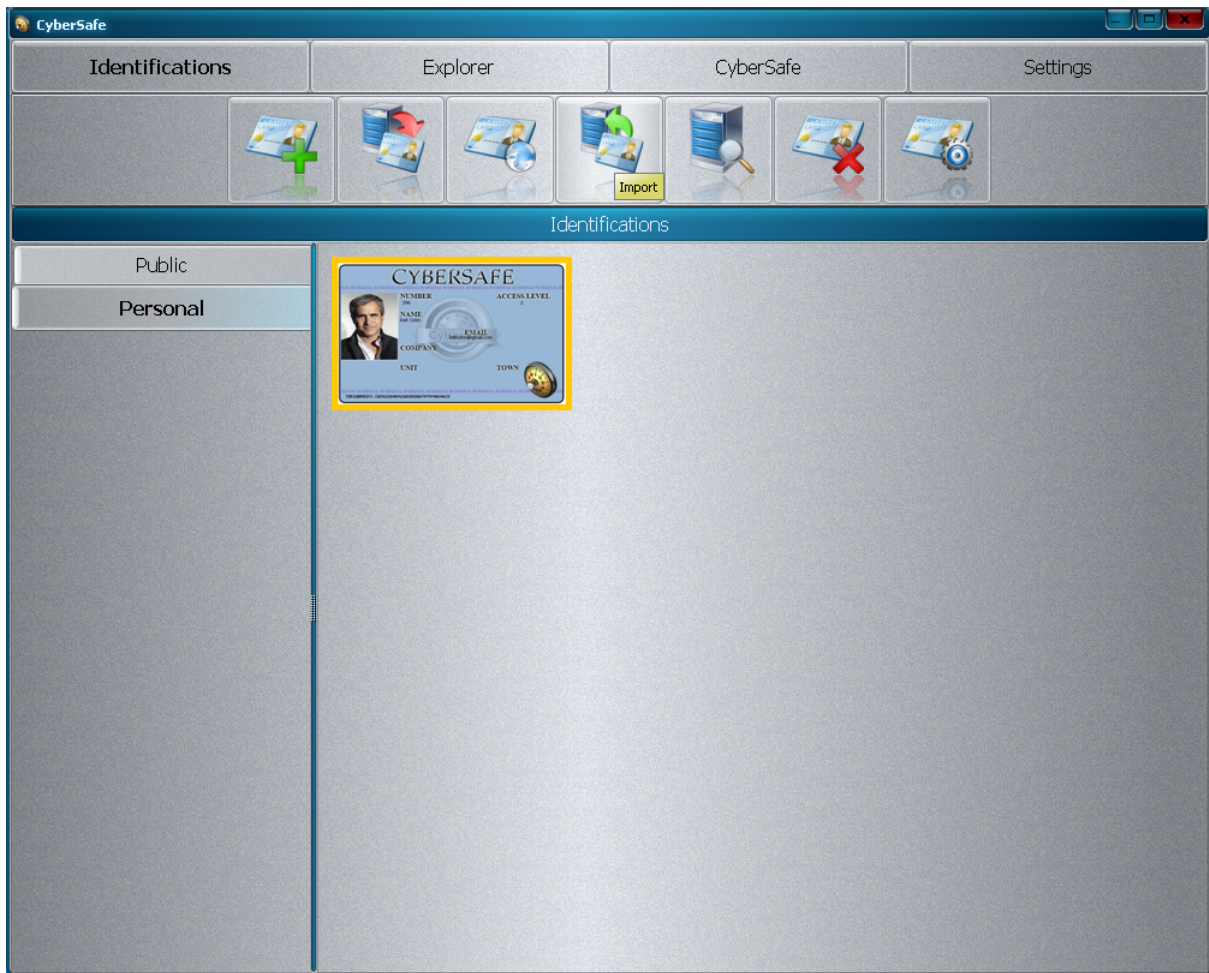
Publishing IDs

For convenience the public part of the ID is published on our server, where everyone can get such an ID and begin the process of data encryption.

The ID is published in the .pid format, which has no encryption and contains the above-mentioned public parts of the keys. You can only publish your own personal ID's public part.

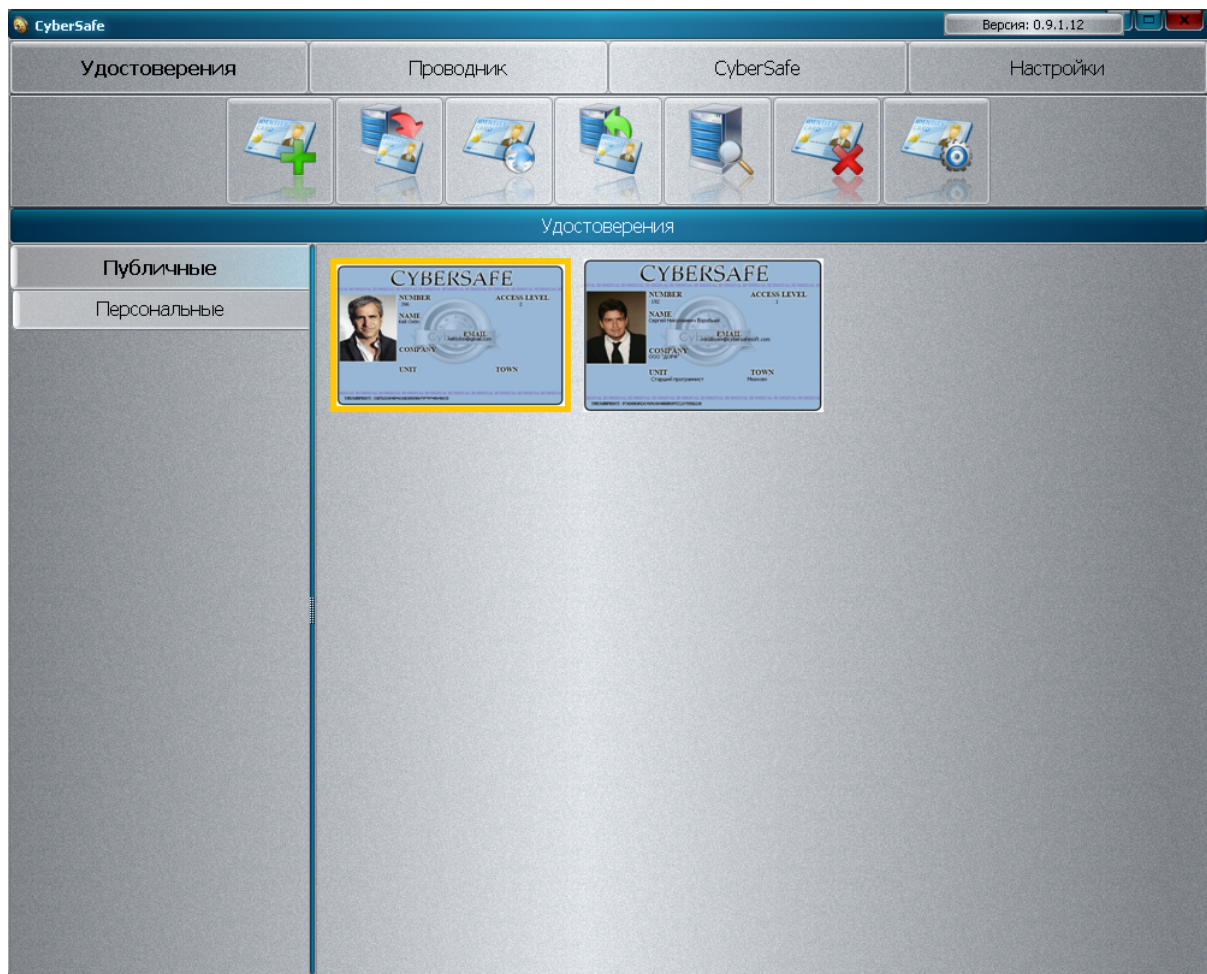
4.2 Import

You can import a new ID, and its elements by using the "Import" button:

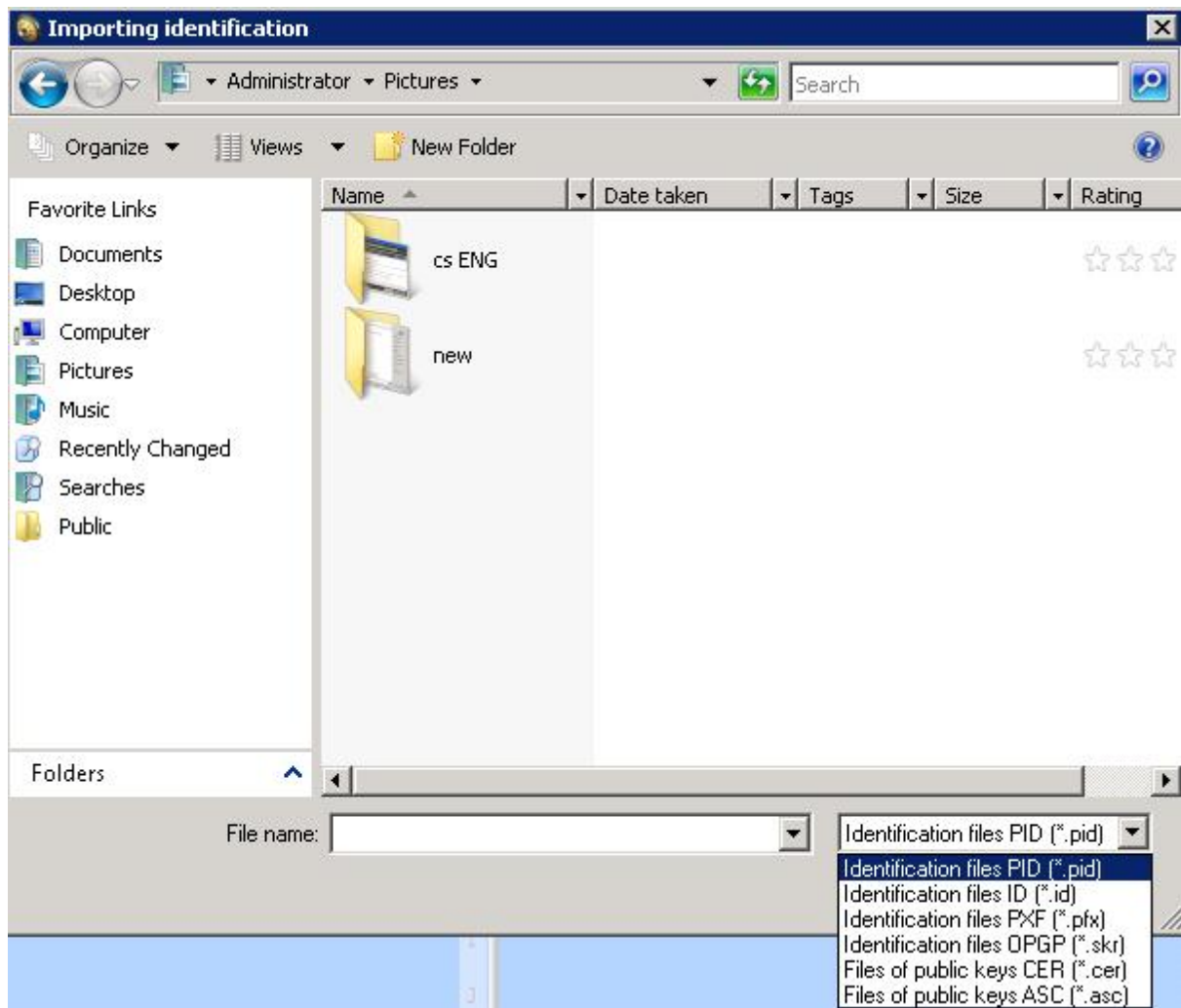


Your personal ID, unlike to the public one is marked with the CyberSafe logo.

Public ID:



CS has the ability to import any elements of ID:



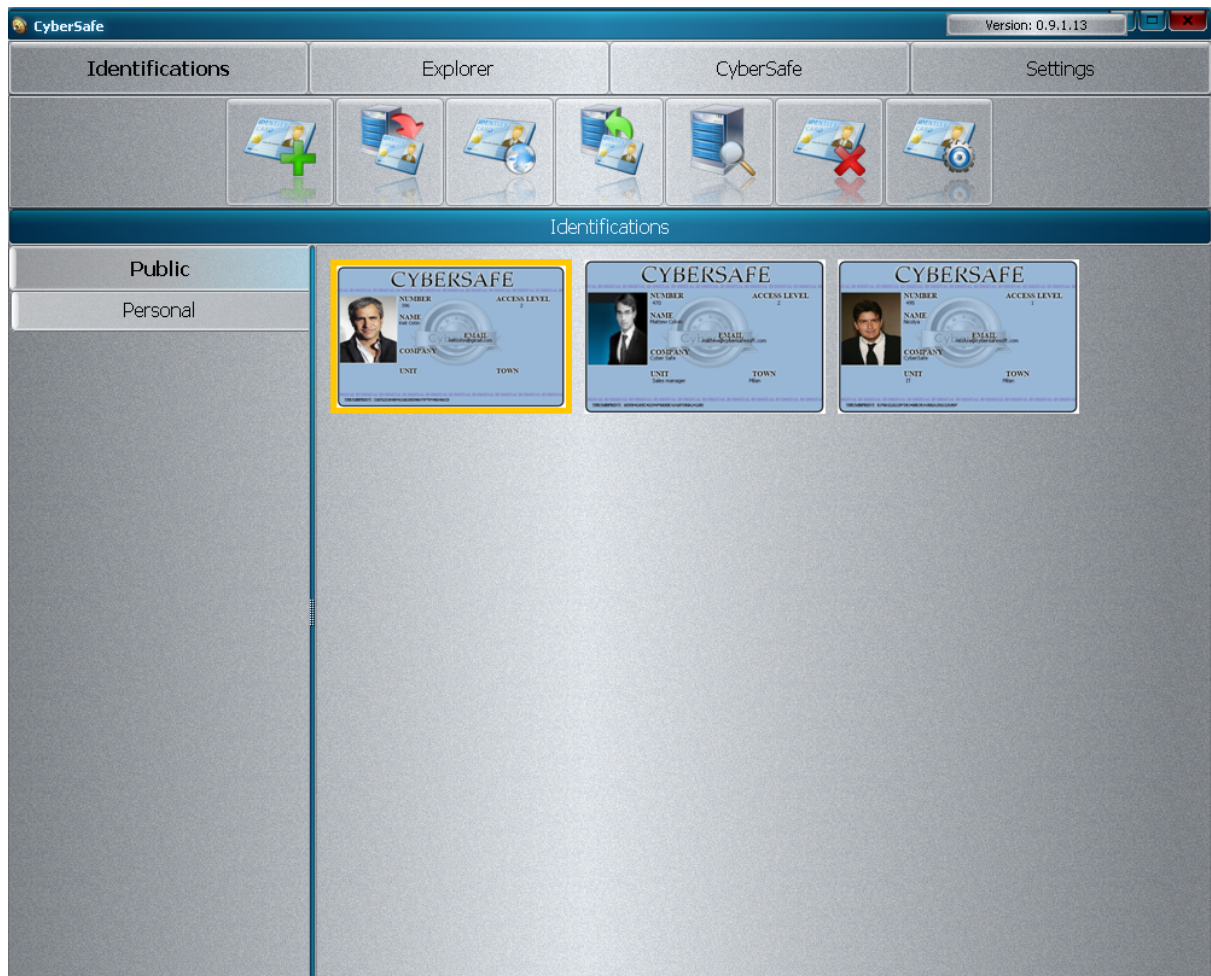
You get the added ability to import from file and from storage, with CryptoPro installed.

4.3 .pid files

.pid files are files of CS, meaning they contain all the necessary keys for encryption to the recipient.

After importing .pid it will appear in the "Public" area of the "Identification" submenu.

If necessary, you can change the image on a public ID, for more details, see the "Properties" of ID section.



Double click on the ID to zoom in.:

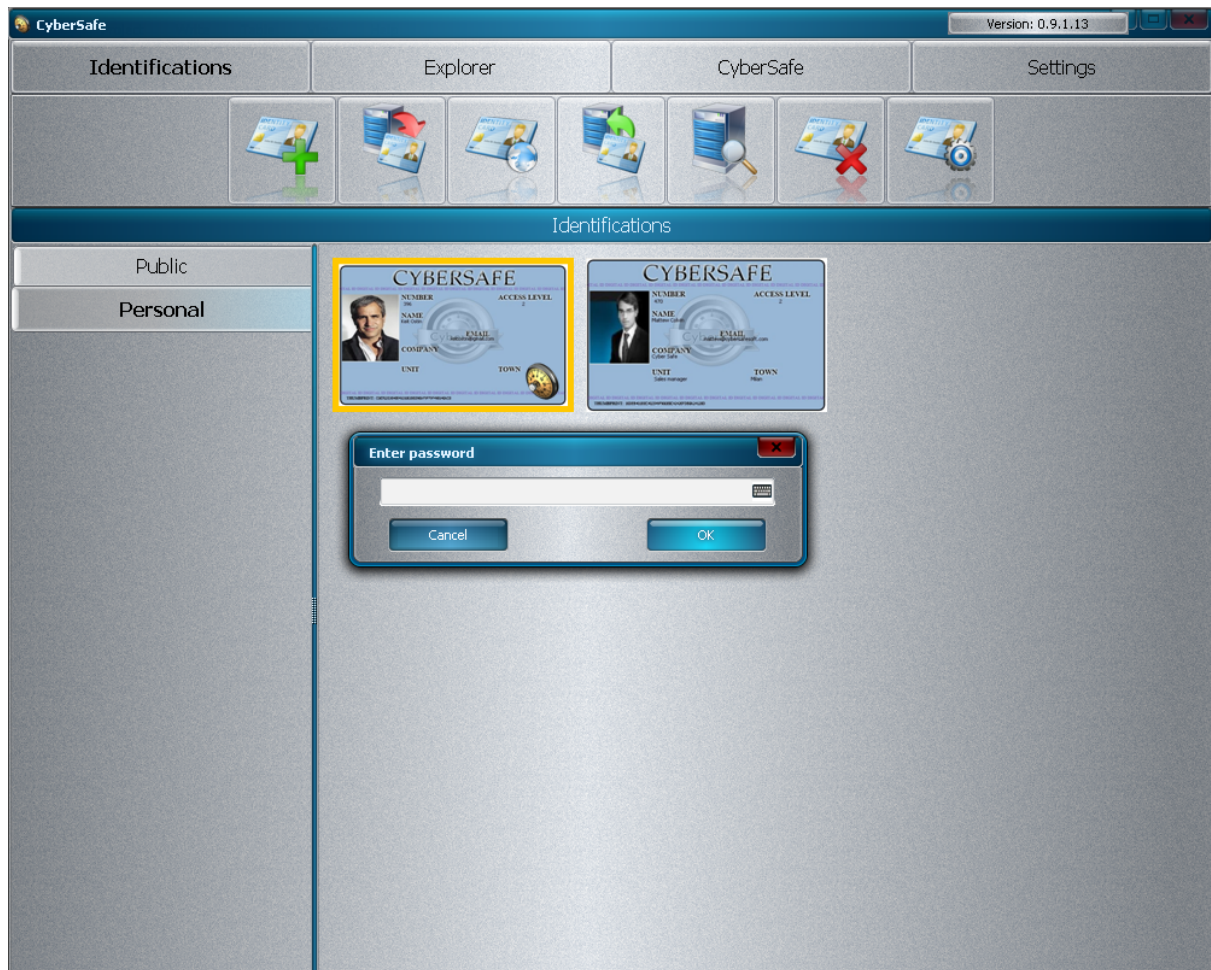


4.4 .id files

File id is also a CS file and contains all the elements of keys: both private and public.



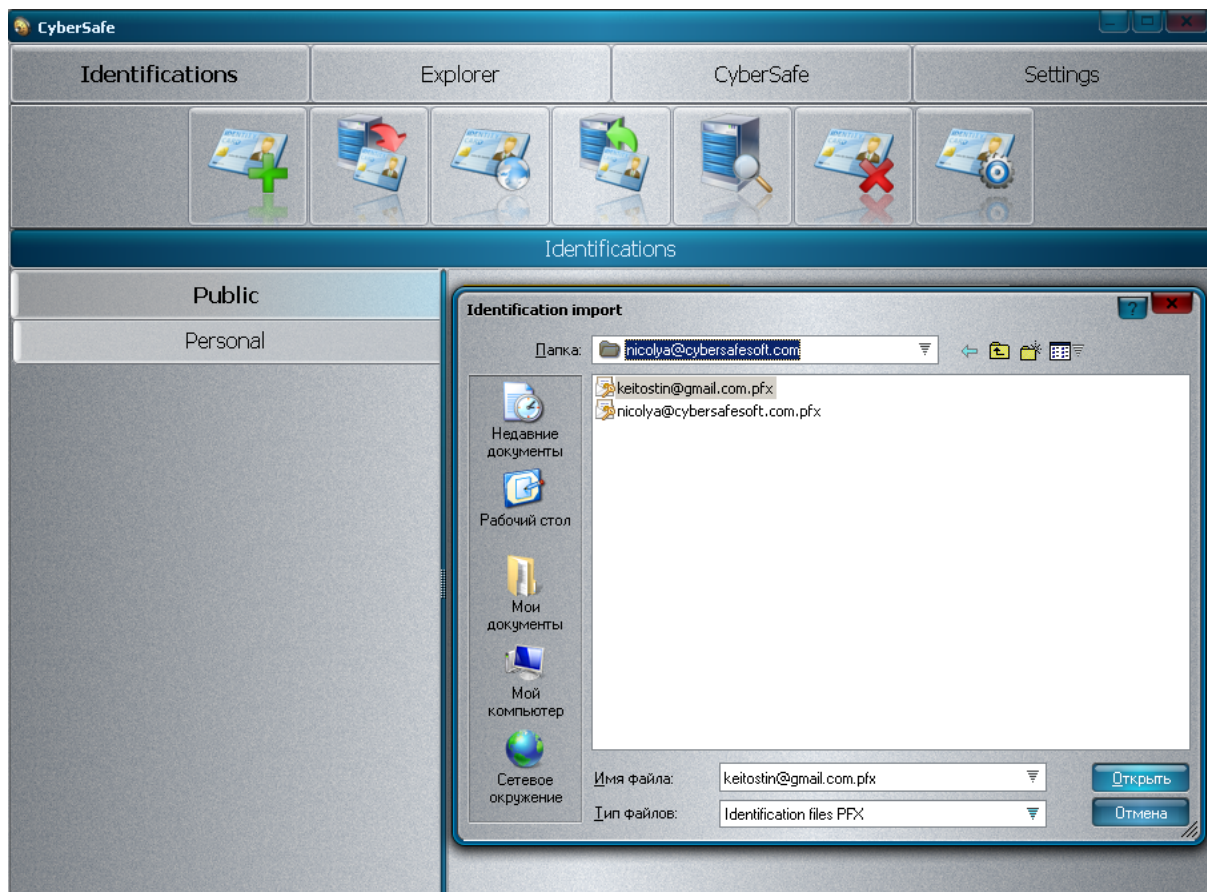
In order to import an .id, you need to know the password.



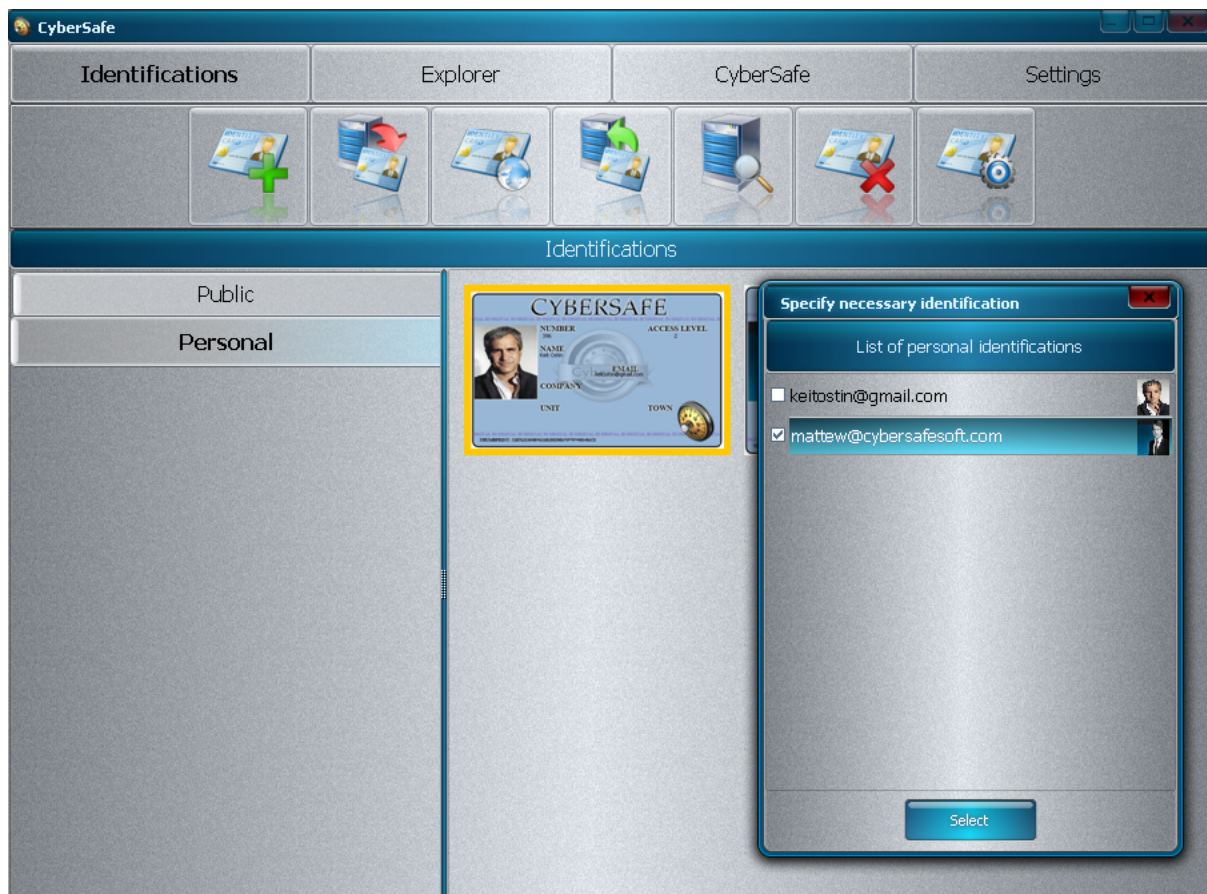
Imported IDs are placed in the "Personal" ID folder.

4.5 .pfx files

If the user already has a .pfx and it is necessary for him to work with already encrypted files or e-mail, the user can import these files.



When you import files the password should be specified for pfx and such file is then placed in an existing private ID marked as "Default":



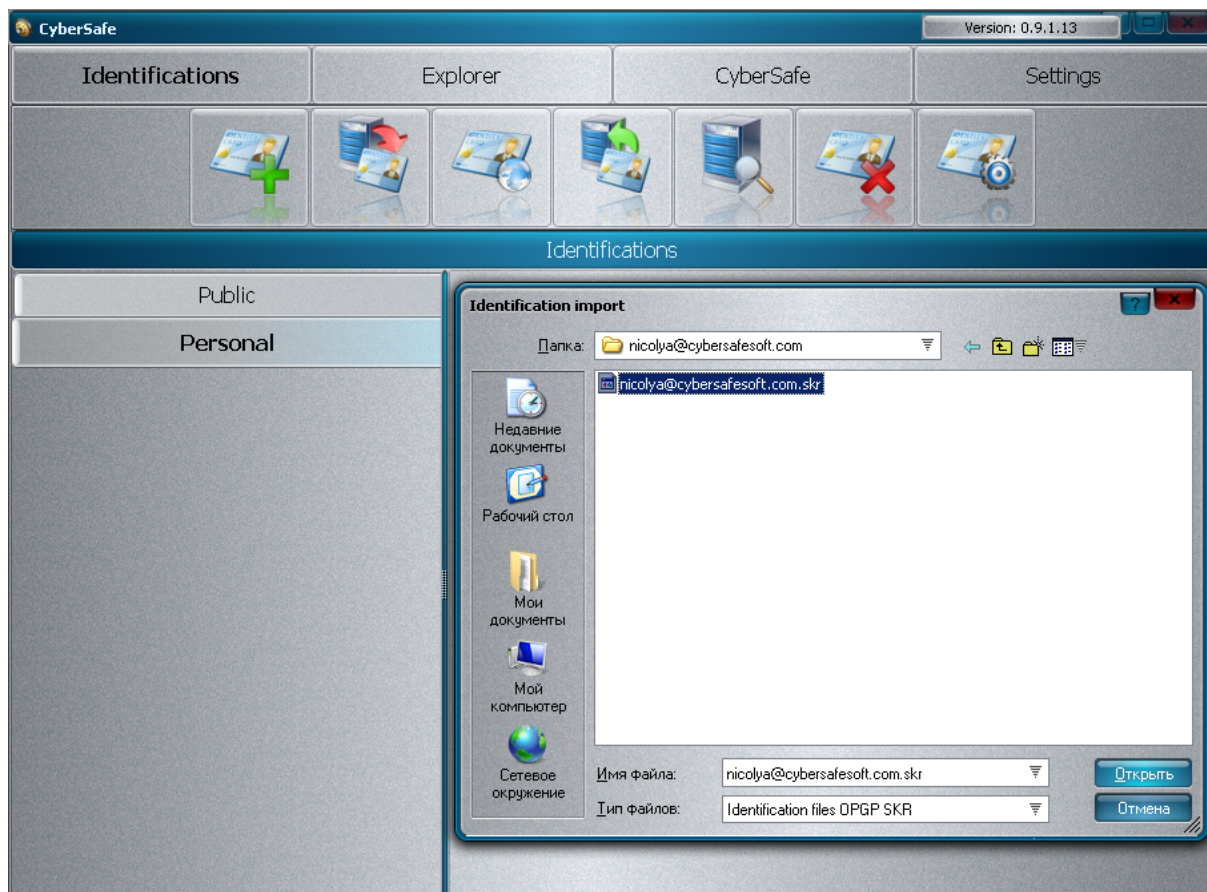
To use .pfx for encryption, signatures, and other operations, one should set .pfx as default for IDs (see "Properties" of ID).

Before the user can import a pfx a personal ID should be created!

4.6 .skr files

Skr. (Secret Key Ring) files are files which are PGP / Open PGP formatted and they are used in the programs such as PGP and WinPGP (Cleopatra).

If the user already has the keys and wants to use them in CS to import files, this can be done by specifying a password for them.

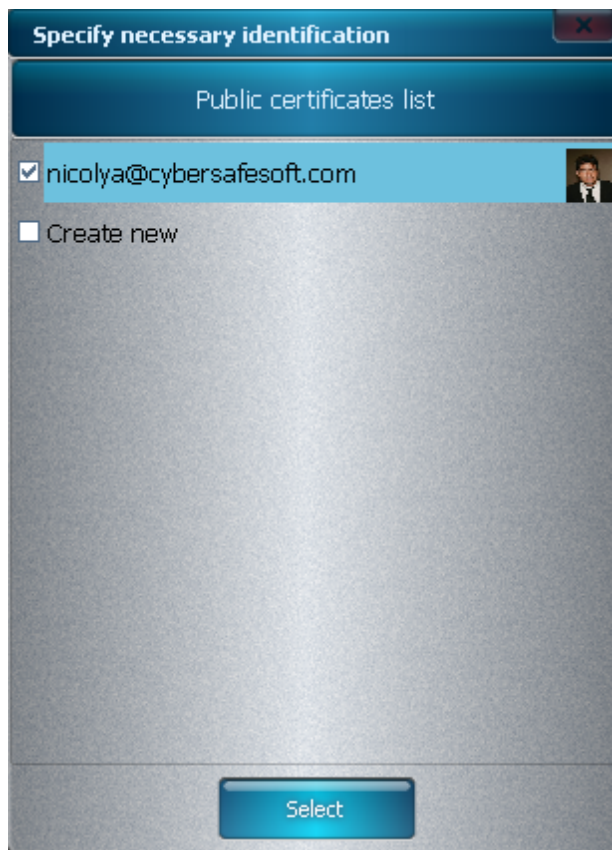


Keys are placed in a private ID by default similar to .pfx.

4.7 .cer files

.cer files are certificate files that contain the public key and are used to encrypt e-mail and files with CryptoARM, Outlook, The Bat!, and so on. When the user imports a .cer file, the user is offered the choice to place the certificate in an existing Public ID or to create a new .pid, which would be based on this certificate.

If the certificate is placed in an existing ID then the encryption certificate is replaced by the imported one.

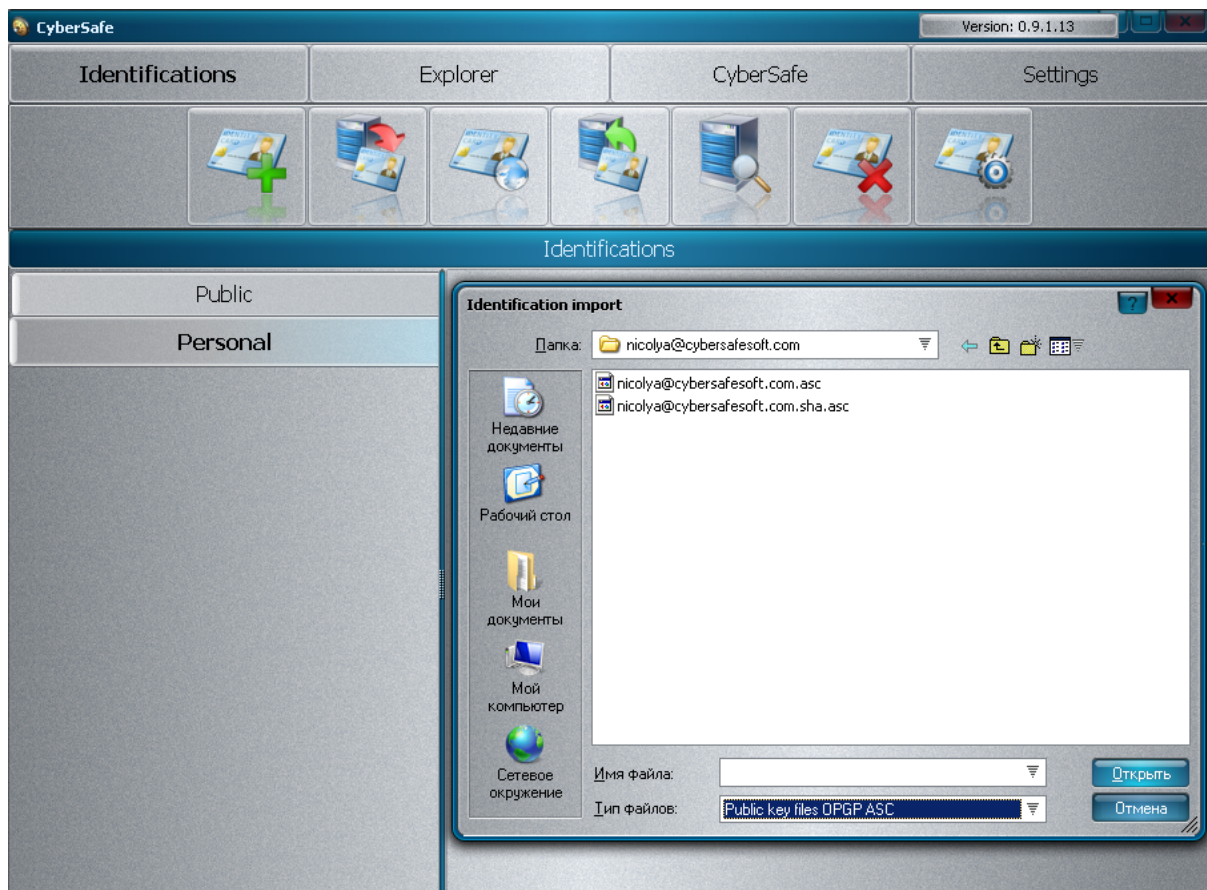


You can see which certificate is used for encryption in the "Properties" of the ID.

4.8 .asc files

.asc files are commonly used by programs which use the PGP standard for transmission of a public key.

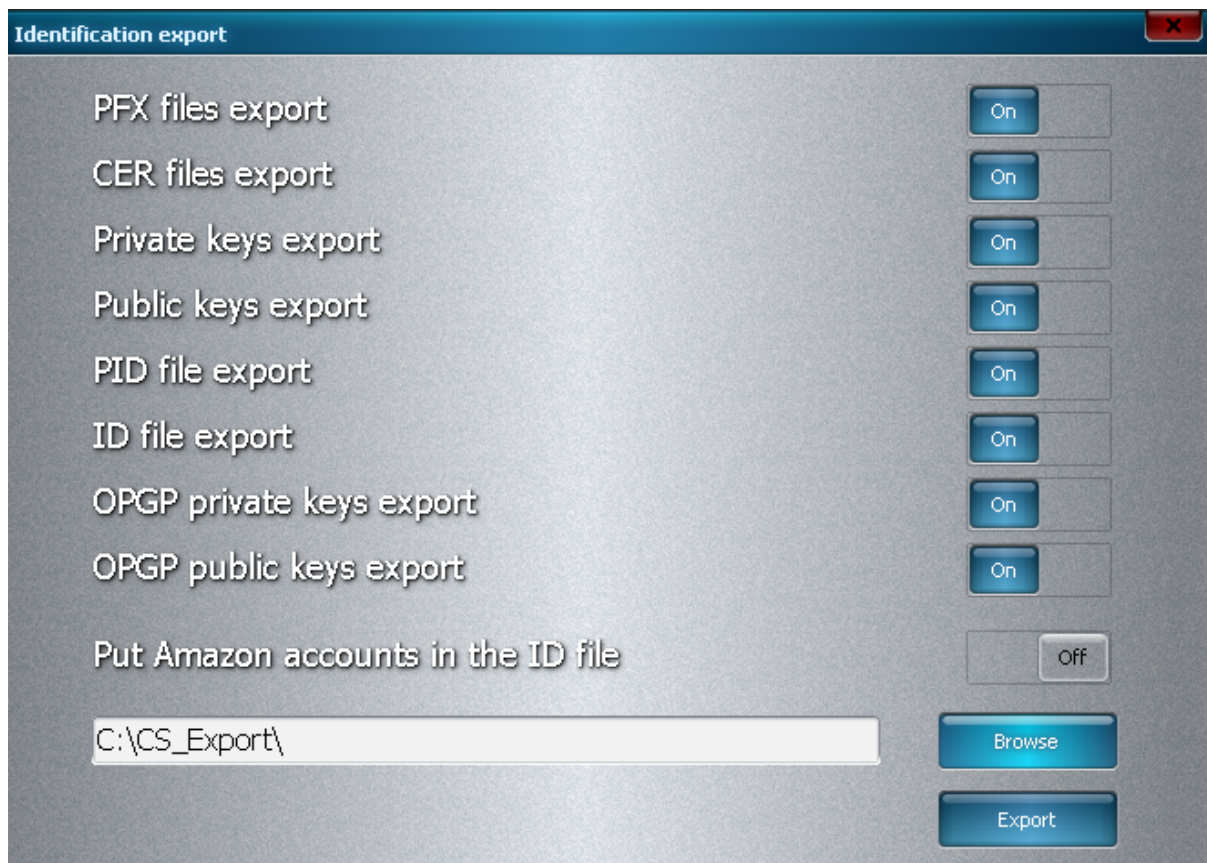
Importing these files is similar to the importing of .cer files.



4.9 Exporting ID

In the export form the user selects the desired items for ID export and the directory to where they will be exported. The password for all elements of the hidden parts of the keys corresponds to the password, which was specified during ID creation.

All the elements of ID will be described in greater detail in the chapters called "Compatibility" and "E-mail protection."

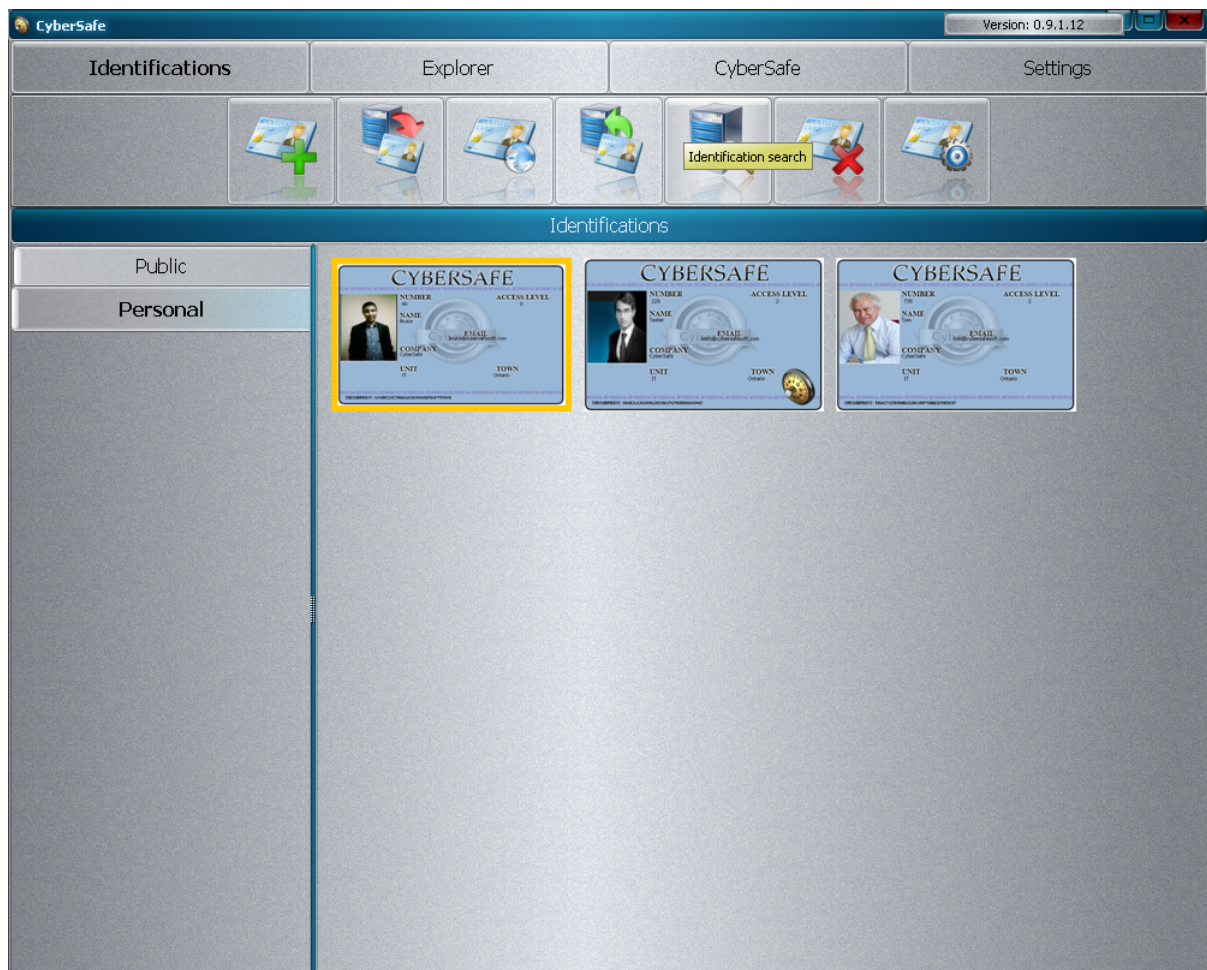


The export of an ID and all of its elements requires you to backup your personal ID and to exchange the public keys with other participants in the encryption process.

4.10 ID search

When several people perform an encryption, the easiest way to exchange their keys is to publish them on a server and give one another their e-mail addresses.

By pressing the search icon and entering an e-mail address the user can receive the requested .pid if it has been published previously.



4.11 Features



The main part of the form displays the ID. The CS icon means that the ID is used as the default for all operations in the use of Windows and CS.

On the right side of the form all the private keys, which are used in the ID are listed. Each key specifies the initial values of the serial number and the fingerprint that corresponds to the values in the certificate. Also, the crypto provider is indicated in square brackets.

4.11.1 Notation conventions

PK – PKI Public Key Infrastructure is a key for encryption of MS CSP

SH – SHA1 is a key for the signature of MS CSP

GE – GOST Encryption is an encryption key for GOST

GS – GOST Signature is a signature key for GOST

PE – PGP Encryption is an encryption key for PGP

PS – PGP Signature is a signature key for PGP

4.11.2 Change ID images

The user can change the picture on the ID.

How to change the ID image:

1. Open "Properties of ID".
2. Select the "Change Image" button.

Only jpg. files, are supported:



4.11.3 Allocate by default

The ID is installed as the ID for all encryption operations.

There is no need for decryption to set an ID as the default, CS selects a proper ID itself at the time of decryption, see the chapter called "Decrypt."

Choosing and setting a new "Default" identity:



4.11.4 Deleting an ID

Any previously imported into the key ID, you can delete the "Properties identity" section.

To do this:

1. Select the key in the "Properties ID" section.
2. Click on "Remove from ID" button

The key is deleted from the ID:



4.11.5 Encryption by default

The classic theory of cryptography assumes that different keys are used for the encryption and the signature. In practice, it is more convenient and easier to use one key for all operations. However, the user can use various keys for any encryption or signature. When the user selects a key and presses "Encryption by default," this key is set as the encryption key by the crypto provider to which the selected key belongs. When exporting, only this key (certificate) will be copied in .pid, and transferred to another party.

The certificate will be replaced by the default one:



4.11.6 Signature by default

The same situation with the signature (DS):



When checking, the digital signature will be checked against the signature with the certificate, which is set by default to be signed, but not to the one used for encryption, see the "Sign" section.



Important! When you change the default key you need to republish your ID or to pass it to the other party so there will be no confusion regarding the keys, otherwise the other party will encrypt certificate, with an outdated key.

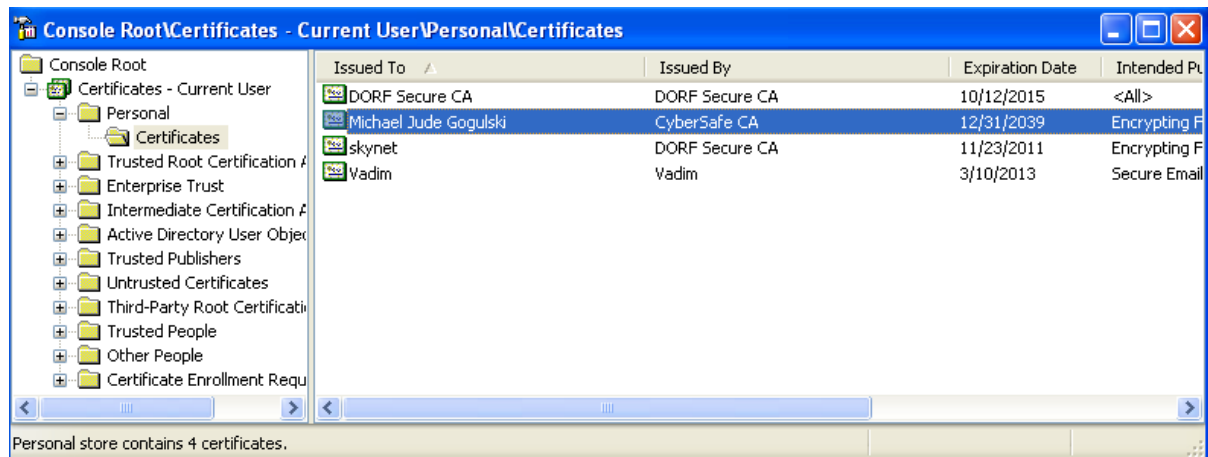
4.12 General principles of using CS with keys

For all asymmetrical cryptography it is crucial to understand how to work with keys. If this information is not well understood, the user cannot successfully use CS.

This does not exclude cases in which the encrypted data cannot be decrypted due to discrepancies between the public and private keys.

When you run CS, it loads all .pfx files in certificate storage without the ability to export them. The user can view them through the certificates snap in:

Windows-R-> mmc-> CTRL-M-> Certificate-> User-> Personal



After closing CS, all certificates and private key containers are removed from the system, because the password for a Windows account can be easily compromised and does not provide any protection for keys.

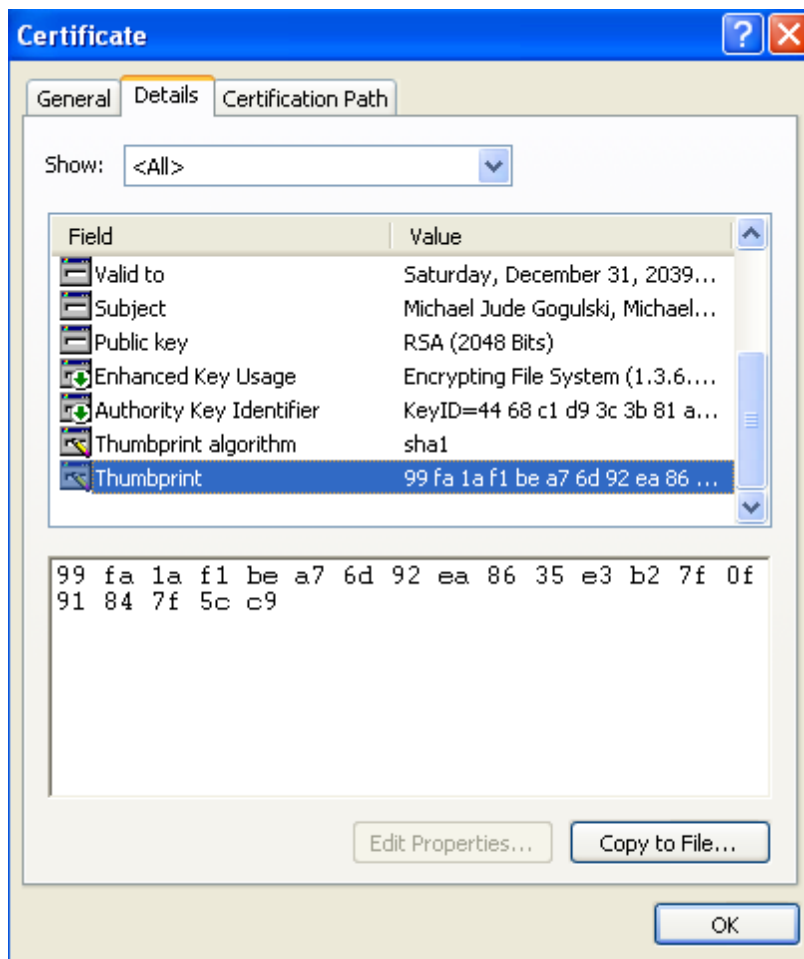
Crypto-PRO keys cannot be backed up in .pfx format. Therefore, GOST keys cannot be removed from certificate storage. Operations with them can be performed using a Crypto-PRO interface, see more details about Crypto-PRO on their official site: [http:// cryptopro.ru](http://cryptopro.ru).

PGP keys are taken from .pkr and .scr files. They are not stored in unprotected form, they are only stored in .id files, in protected form.

MS CSP certificates (.cer) are used to encrypt files, and GOST uses the certificates in the certificate storage. Therefore, when importing .pid or .cer files, GOST certificates are installed in certificate storage. To avoid confusion, it is not recommended to have 2 or more certificates with the same e-mail of the same crypto provider in certificate storage.

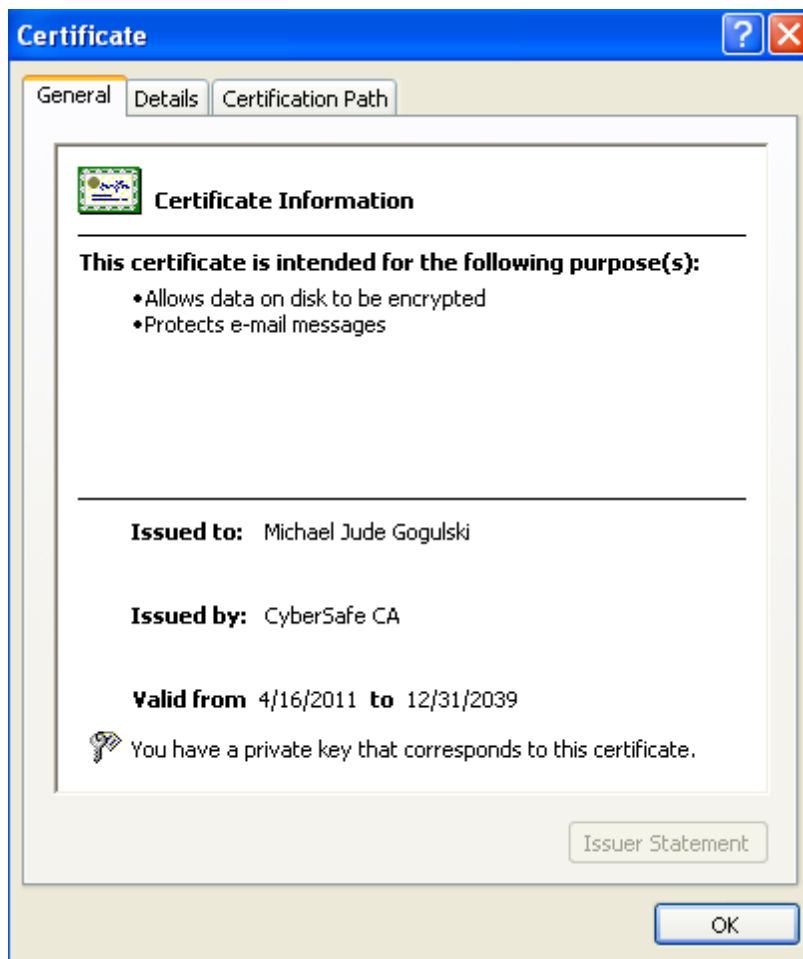
If it is impossible to decrypt the data, it is necessary to establish which key (certificate) was used for encryption, to find its fingerprint and to compare it with the fingerprint of the private keys (certificates) in certificate storage.

For example, Ivanov gave his .pid to Petrov. Petrov has encrypted a few files using the Crypto-PRO crypto provider and has transferred the files to Petrov. Petrov then receives the files but he cannot decrypt them. He should export his default .pid and open it using WinZIP or WinRAR, then open the file petrov@fsb.ru.gost.cer and see the key fingerprint in the properties of the ID.



It is always enough to compare just the first four characters. Now you need to::

1. Open your GOST certificate in certificate storage, which has the private key.



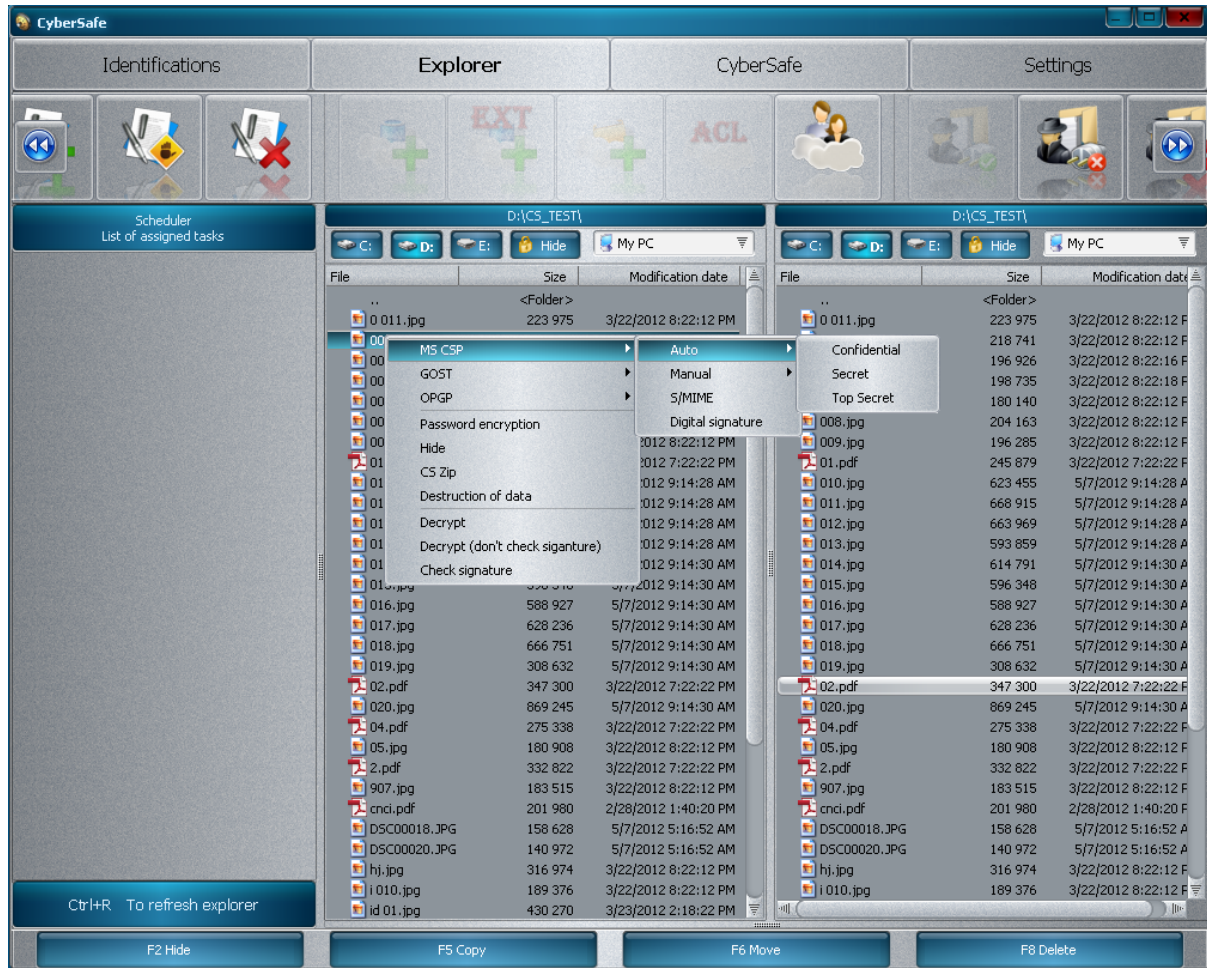
2. Look at the fingerprint of this key.
3. Compare the fingerprints with the properties of an .id in the CS (see the chapter "Properties").

Keep in mind that in CS, the serial number of a certificate is specified first and then the fingerprint indicated through the slash. If a discrepancy is found at any point in this sequence, you should correct the situation by issuing a new ID, preferably with another e-mail, or if you prefer to use the same e-mail, it is recommended that you remove all corresponding certificates of the crypto provider from certificate storage.

This confusion is possible if, before the installation of CS, there were certificates from this e-mail in certificate storage. Therefore, it is recommended if possible to import the .pfx file into CS's ID storage.

5 File Encryption

All file encryption is performed through the right-click menu of Windows explorer.



5.1 MS CSP

Automatic mode is designed to store files on a PC without them being transferred to the recipient. For convenience, there are three modes available to differentiate information in order of importance. Each subsequent mode provides a more stable algorithm and greater key length.

5.1.1 Auto - For official use

This type of encryption encrypts files and folders using EFS, and it masks them. The cipher is 3DES 192 bits. For more information about EFS, see http://en.wikipedia.org/wiki/Encrypting_File_System

5.1.2 Auto - Secret

Auto - This type of encryption encrypts files and folders using PKI (for more information about PKI,

see the chapter “Basic concepts of asymmetrical cryptography”) and it masks them. The cipher is AES 256 bits. The certificate to encrypt is taken from the .id by default and it corresponds to the properties of the ID designation in PK.

5.1.3 Auto - Top Secret

Auto - This type of encryption encrypts the files and folders with a password, which is taken from the value of a private key (PK) by default for MS CSP, and it masks them. The cipher is BlowFish 448 bits. □The encrypted data disappears from the explorer and any file manager, and becomes available in the CS explorer (see CS explorer).

5.1.4 Manual - EFS

This This type of encryption encrypts files and folders using EFS. The cipher is 3DES 192 bits. For more information about EFS, see at http://en.wikipedia.org/wiki/Encrypting_File_System. EFS is designed to store files on a PC without their transfer. It is very convenient due to the fact that files are available for any purpose without having to be decrypted first.



Attention! EFS has several disadvantages that makes this type of encryption vulnerable. CS eliminates these disadvantages.

The special Software to decrypt EFS ElcomSoft ESF Recovery, which according the developers "restores" (simply cracks) EFS in 99% of cases is unable to decrypt EFS on a PC that uses the CS.

5.1.5 Manual – PKI

This ty This type of encryption encrypts files and folders using PKI (for more information about PKI, see “Basic concepts of asymmetrical cryptography”). The cipher is AES 256 bits. The certificate to encrypt is taken from the public ID, which is imported into CS. Thus, this type of encryption is intended to transfer files to others. You can select multiple recipients for the files.



Attention! If the file is encrypted by Ivanov for Petrov by a certificate from Petrov without adding a senders certificate (Ivanov), the file can not be decrypted by Ivanov.

5.1.6 Manual - BlowFish

This type of encryption encrypts files and folders with a password, which is taken from the value of the private key (PK) by default for MS CSP, and it masks them. The cipher is BlowFish 448 bits. It does not work for transferring that file to a recipient, because the password is a private key of the encryptor. This mode is useful for copying data to a removable carrier or transferring data over open communication channels on the PC where you installed CS with the same private key as on the PC on which the encryption was done. In other words, Ivanov encrypts the files at home to copy them to a flash drive and to decrypt them at work, where there is a private key, like at home.

5.2 GOST

5.2.1 Secret

This type of encryption encrypts files and folders using PKI (for more information about PKI, see “Basic concepts of asymmetrical cryptography”) and it masks them. The cipher is GOST 256 bits. The certificate to encrypt is taken from the certificate storage of the .id file by default, and it corresponds to the properties of the ID designation done by GE.

5.2.2 Manual - PKI

This type of encryption encrypts files and folders using PKI (for more information about PKI, see “Basic concepts of asymmetrical cryptography”). The cipher is GOST 256 bits. The certificate to encrypt is taken from the public ID, which is imported into CS. So, this type of encryption is intended for transferring files to others. You can select multiple destinations for the files.

5.2.3 Digital signature

Digital signature (DS) is the attribute of an electronic document that allows us to establish that there is no distortion of information in an electronic document since the creation of the DS, and to compare the holder's signature to his certificate. The value of a DS is obtained by a cryptographic transformation of information using the private key. □ The files are signed with help of a key, which corresponds to a .id file by default GS designation.

5.3 OPGP.

All operations with standard Open PGP are identical to the functions described above.

5.4 Data masking

The method used in CS to hide files is one of the best and it is based on using a driver called a "hook" by specialists. Its function is to intercept requests made by the OS to the structure of the disc and to give values with a filter. When the machine boots in safe mode, the files are hidden, when trying to view a PC through remote administration tools (TeamViewer, Radmin)

the hidden files are also not visible. If you uninstall CS and manually remove libraries the files will still remain hidden. □CS does not use the dubious practices of other programs for hiding files, which set some signs for the hidden files in the operating system, and call them MyHiddenFolder, or creating icons various places in the PC with a smart title like lamHidingFiles and so on. This method is self defeating- anyone looking for hidden files would see right away that there are files hidden on this computer.

However, it should be understood that in contrast to cryptography, where there is a guarantee that your files cannot be decrypted, hiding files does not provide such a guarantee. It all depends on the degree of the training of the specialist who is exploring the user's PC. Whatever tricks the hiding software uses, hidden files can still be found. Therefore, CS offers automatic modes in which the hidden files additionally are encrypted.

Once again: The best way to protect information is to hide the fact that anything is being protected.

Masked files are visible in CS explorer for users working in the folder. Files do not remain in their location on the drive for convenience and safety. Later, the user can sort them into the hidden folders in CS explorer. This principle applies to multimedia managers (WMP, iTunes), when the files are added to the library, and then the user sorts them by album and so on.

Masked folders remain in place and can be accessed through CS explorer.

5.5 Decrypting

This command applies to any encrypted file of any software, not only to CS. The structure of the file is defined by algorithm and crypto provider, and CS attempts to decrypt the file using a set of private keys for all a user's .id's, not just the default .id.

5.6 Verifying a signature

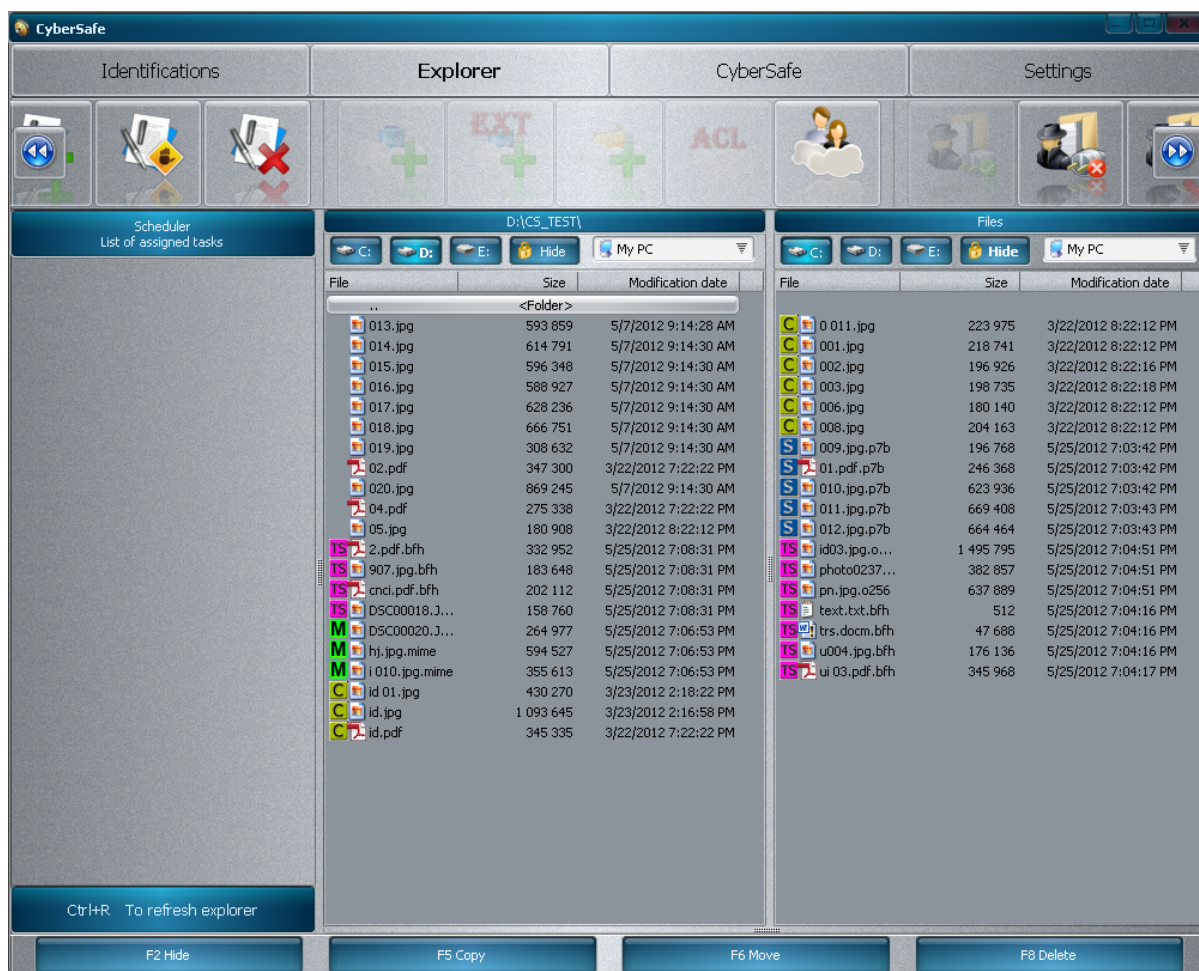
When verifying a signature, there is an analysis of the crypto provider and signed certificate, then there is a search for this certificate in the public ID, and if it is found it is displayed on the form.

If the signature certificate has a value of the e-mail ivanov@kgb.ru with a fingerprint of "FS 56", and in the public ID there is already a certificate with the e-mail ivanov@kgb.ru with the fingerprint of "GH B7" and the crypto provider matches, then the error will be displayed as "Possible ID fake." The word may mean that such a situation is possible if the user has updated his certificate. In order to clarify you must contact the user and to ask him to dictate the first characters of the fingerprint of his certificate for a signature (SH, GS or PS). A "Replace ID" button will appear on the form.

If you try to edit the signed file a validation error will appear: "File has been changed"!

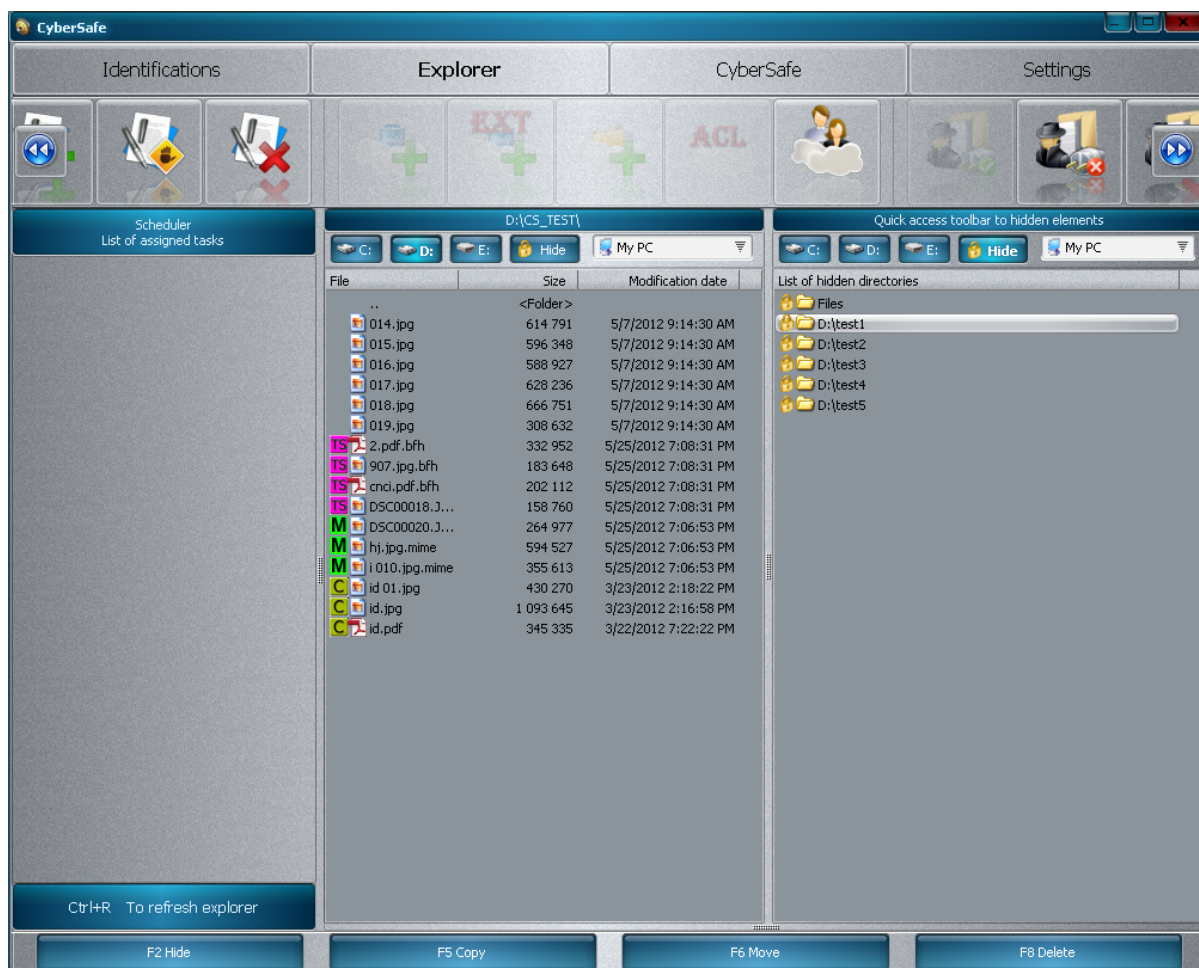
If the signature is faked there are two possibilities: an attempt to fake a file without forgery of signature, and the falsification of signature on the file. These two situations are excluded by checking of CS.

6 CS explorer



6.1 Work with hidden objects

Pressing the “Hide” button grants the user access to the hidden objects on a PC. Hidden directories are marked by a padlock icon.

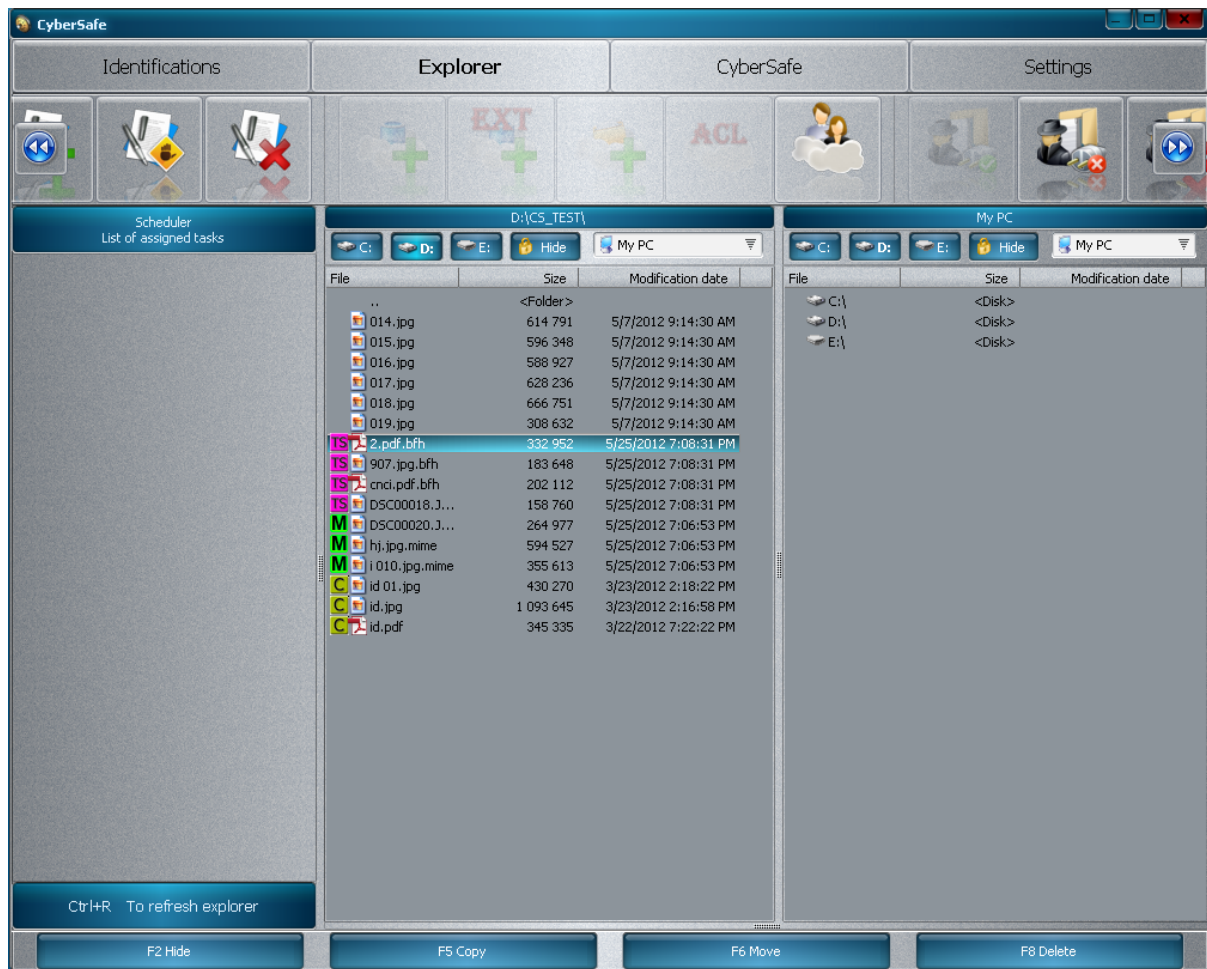


First, hidden files are moved into the users directory "Files" of the working folder. From there, they may be moved to the appropriate folders. If the hidden files are moved to a visible folder, they will then become visible.

Users can make visible any hidden object by pressing the "Show" buttons or F2 on the keyboard, and by pressing the same buttons visible objects can be hidden.

Moving visible files to a hidden folder makes them hidden.

6.1.1 Tag and running of files

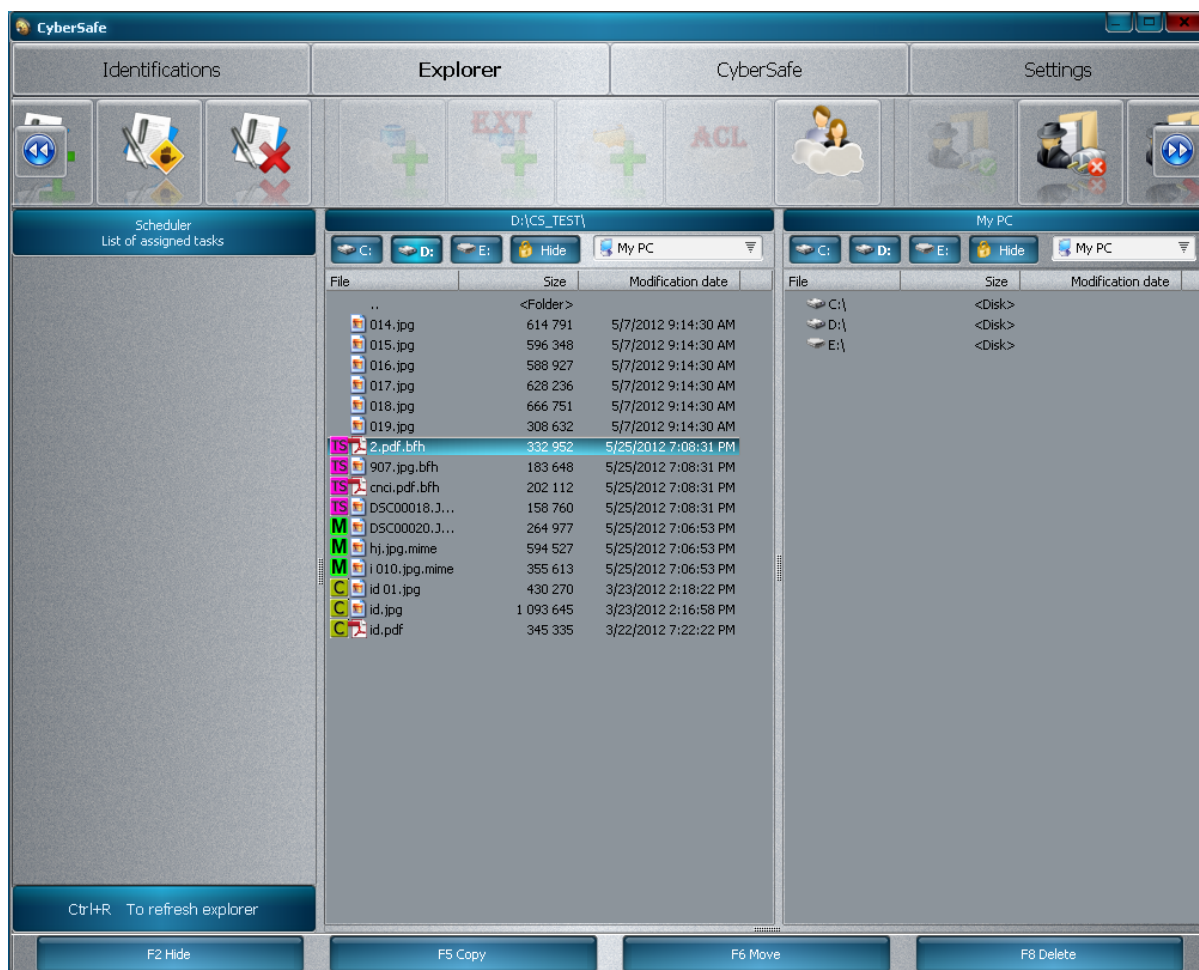


C – Confidential corresponds to FOU (for official use).

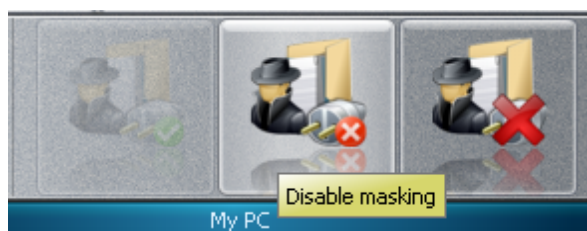
S – Secret.

TS – Top Secret.

Double click a file to run it. The file is decrypted and opened by the application, which corresponds to this type of file. The file is launched online and it is tracked until it is closed by the application, whereupon it is encrypted again. If there is an attempt to exit CS before the closure of all encrypted files, a warning will be displayed stating that the task was not completed with all the files. It is recommended to save and to close the file in the application before exiting CS.



6.1.2 Disable masking



When masking is disabled all hidden folders become visible. After closing CS, masking turns on again. This feature disables the filtration of drives, but it does not mark a folder visible. It is not recommended to use this mode, unless it is absolutely necessary.

To turn on masking again the user can click on the icon “**Enable masking**”.

6.1.3 Unmask all

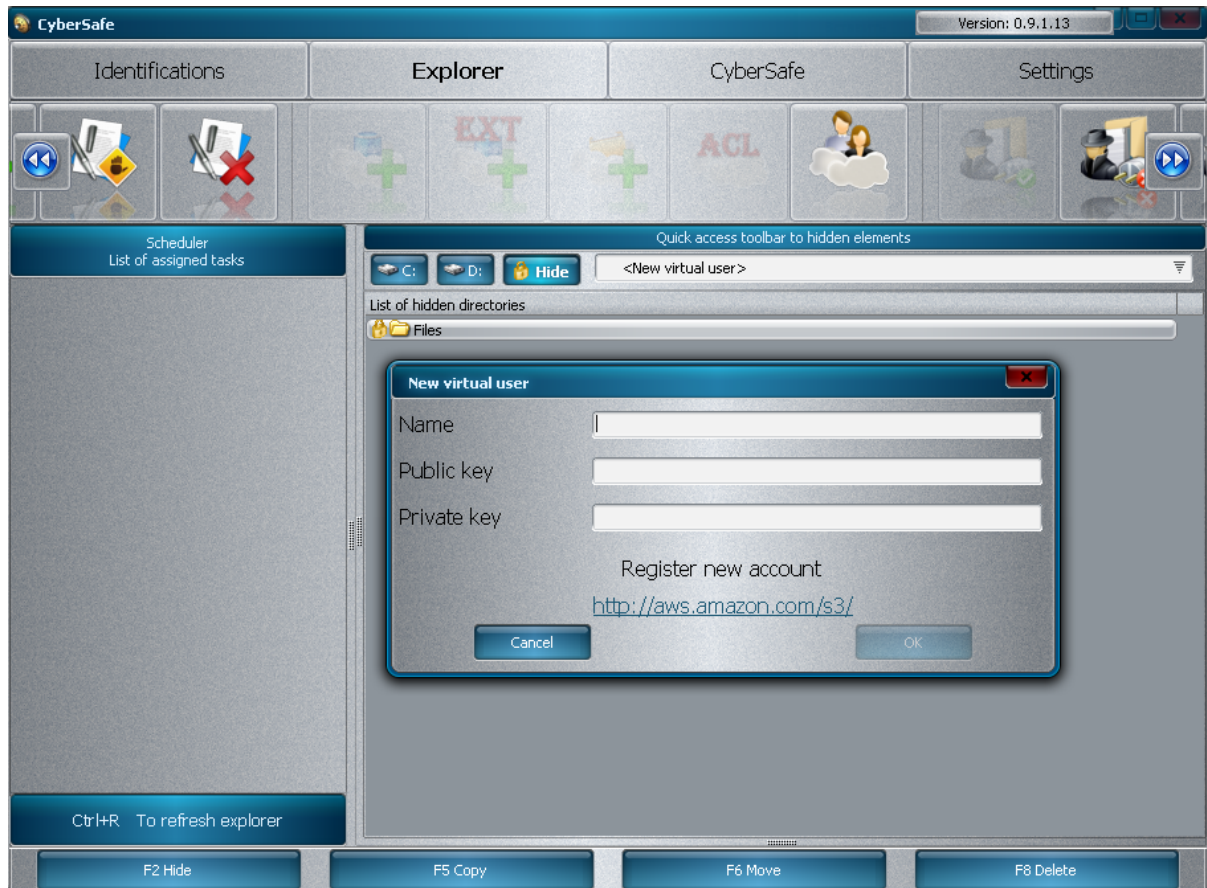
This mode marks all previously hidden folders as visible. After turning off CS the folders will be visible. It is recommended to use this mode only when uninstalling CS.

6.2 Amazon S3.

CS allows users to back up data on Amazon S3. To start working with Amazon S3 the user must register and receive keys to enter.

To do this:


1. Select "New Amazon S3 account" from the drop-down list.




2. Click the "Register new account" link. After registration, the user should receive the keys for entry.

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

 **Access Keys**

 X.509 Certificates

 Key Pairs

Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.

Your Access Keys

Created	Access Key ID	Secret Access Key	Status
October 18, 2010	AKIAJMQ3TNJA5QCJ3JBA	Show	Active (Make Inactive)

[Create a new Access Key](#)

[View Your Deleted Access Keys](#)

For your protection, you should never share your secret access keys with anyone. In addition, industry best practice recommends frequent key rotation.

[Learn more about Access Keys](#)

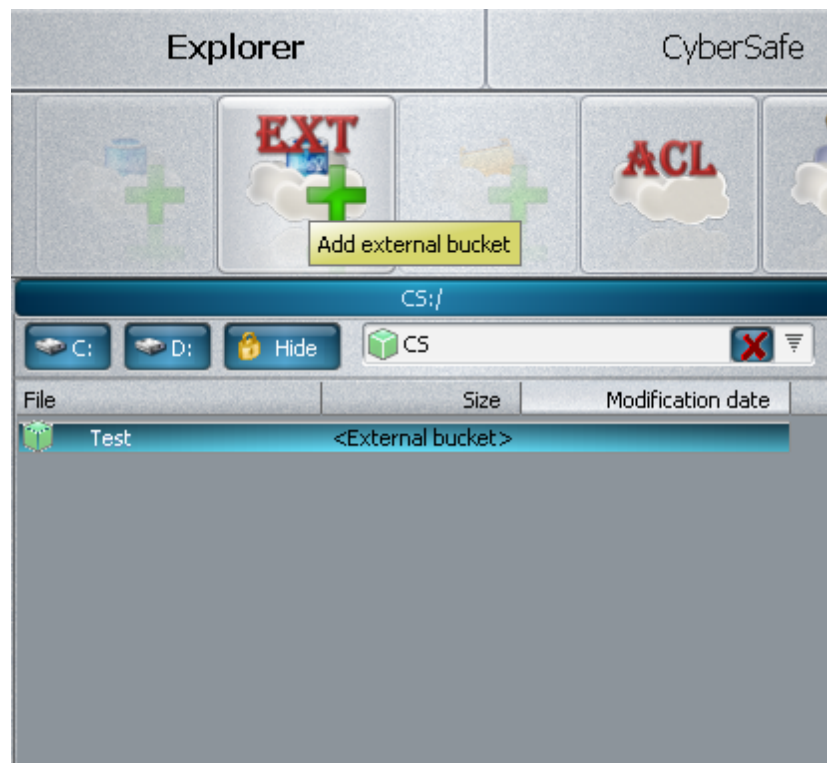
3. These keys must be entered in the fields of Public (Access) and Private (Secret) keys.

If the data is correct the account will be created in CS, and the user can start working with Amazon S3.

6.2.1 Create a bucket

In Amazon S3 data is stored in containers called “buckets.” Each bucket name must be unique within Amazon S3. That is, a bucket called “test123” the only bucket with that name in Amazon S3. Therefore, if the user creates a bucket and gets an error, then he must specify a unique name. This is to ensure that everyone can access any bucket with public access. Also, a user cannot use capital letters, or any foreign script in the name of a bucket. This restriction does not apply to folders and files.

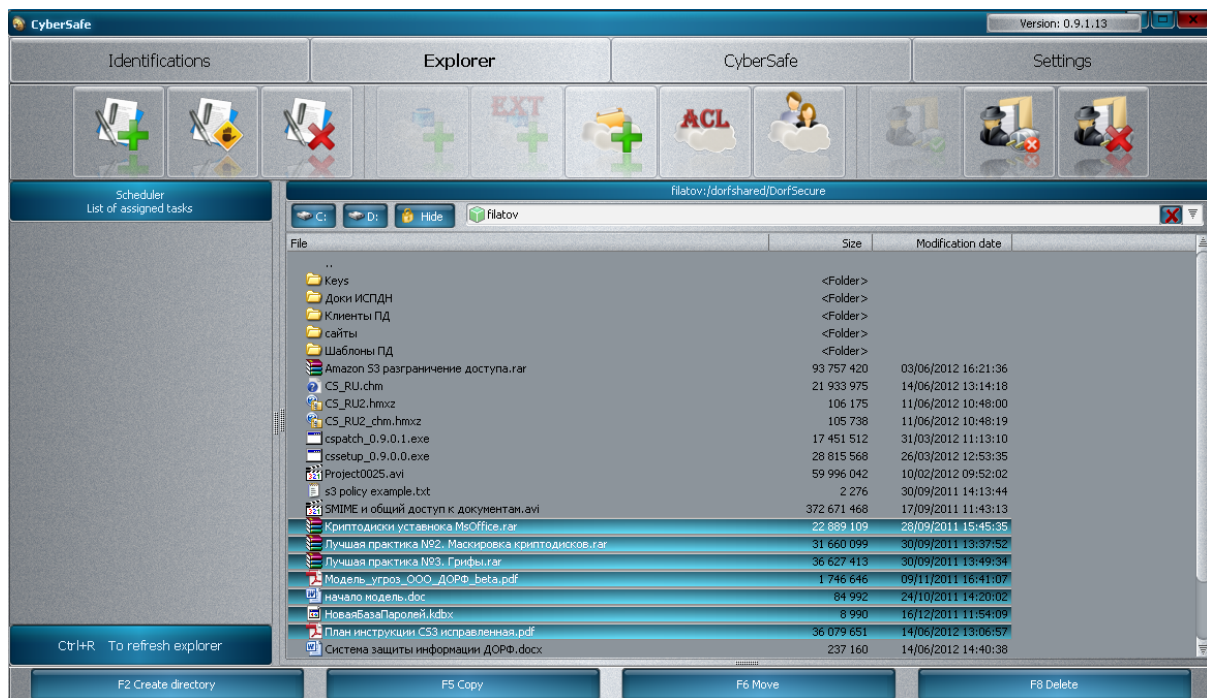
Adding an external bucket:



6.2.2 Create a folder

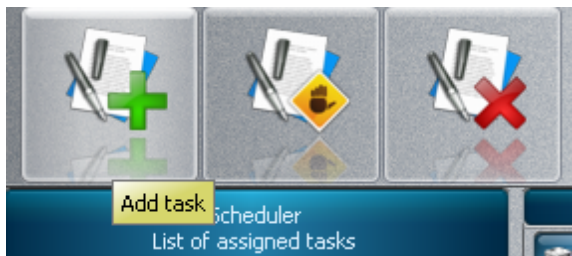
After creating a bucket the user creates the folders structure. There are no restrictions on names of folders.

Further, there is no difference in copying, and moving files and folders from working with a PC:



The user can copy multiple files simultaneously. The user only has to copy the files and folders and the files will all be copied automatically, with no need to copy each one manually.

6.3 Scheduler



When the user clicks "Add task" a form to create a new task in the scheduler opens:

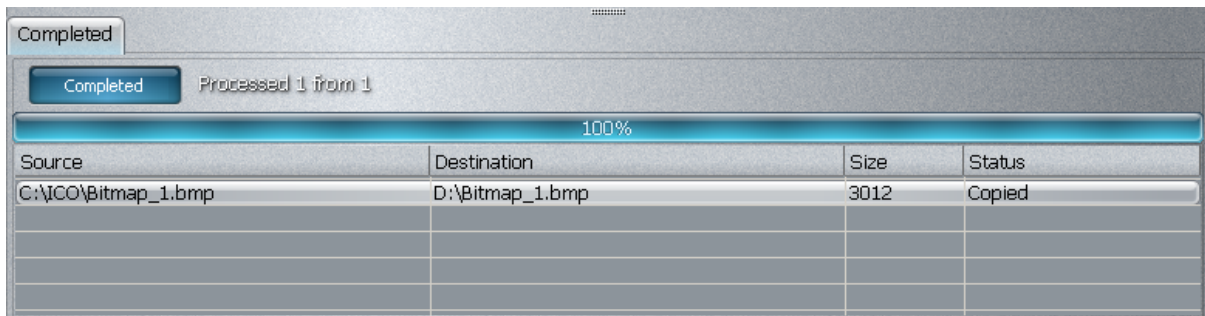
The image shows the 'Scheduler new task' dialog box in Windows. It is divided into several sections: 'Visible name' (set to 'New task'), 'Source' (Location: 'My PC', Element(s): empty), 'Destination' (Location: 'My PC', Directory: empty), 'Actions' (Operation: 'Copy' selected, Additional parameters: 'Do not encrypt', 'Archive' checkbox unchecked, 'Add date/time to archive name' checkbox unchecked), and 'Schedule' (Periodicity: 'Once every week per' selected, Days: 'Sundays', Time: '19:47'). At the bottom are 'Cancel' and 'OK' buttons.

The scheduler provides a convenient tool for backing up to Amazon S3. The user selects the Source, the Destination for backing up, and the frequency of backup. The user can also set additional copy options such as file compression and encryption.

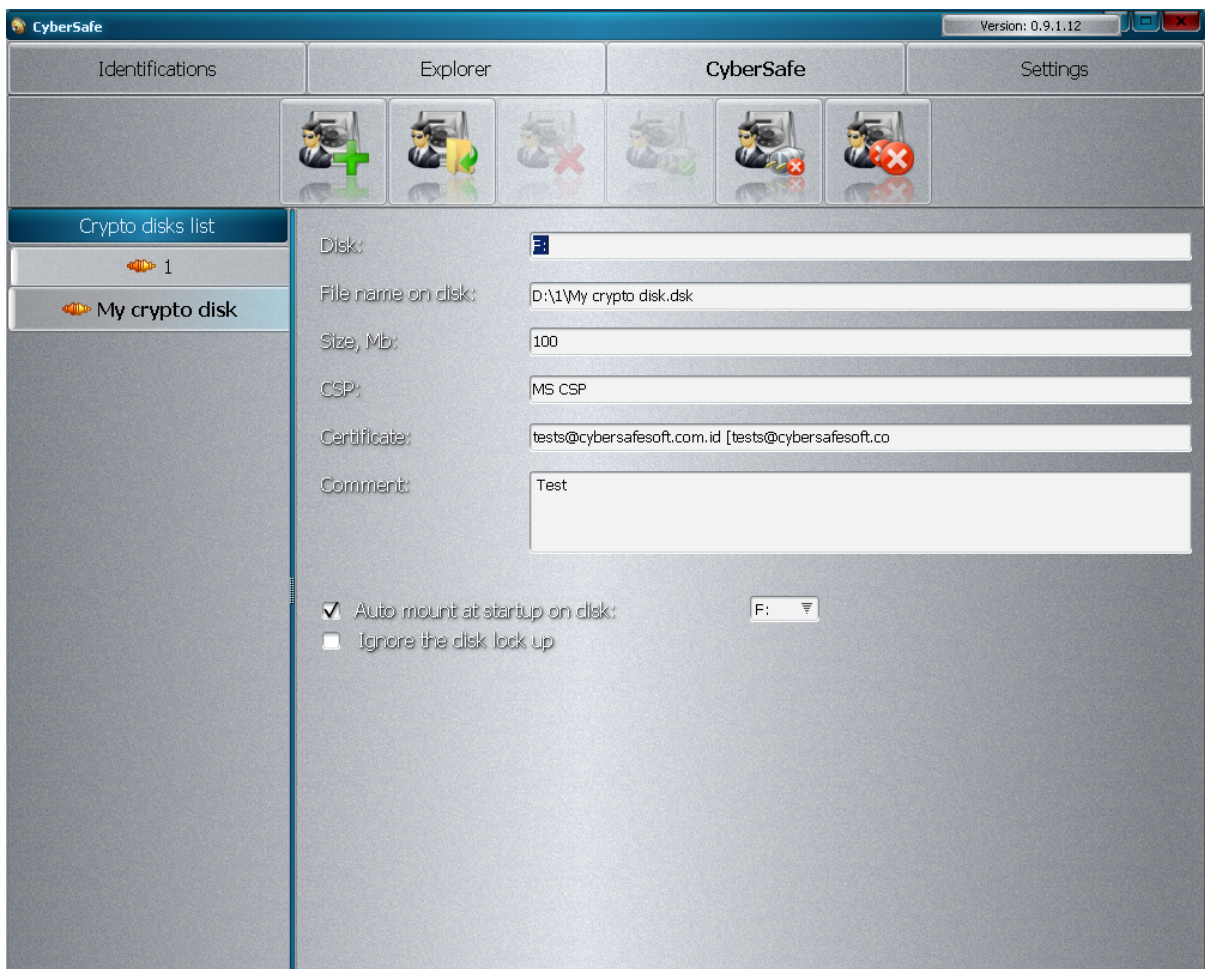


The pause button on the task means that the task is waiting for its time to start. To start the task immediately the user must click on the pause button. The icon of button will change to play and the task will begin.

After the task is finished a message box will appear, stating that the operation has ended:



7 Crypto disks



Encryption on the fly is encryption of user files performed in real time. It is usually transparent and typically is carried out by the creation of virtual, encrypted logical discs.

Transparency means that the secure encryption software should be integrated into the system in an organized fashion and provide the user and other software the opportunity to continue working without changes, in addition some or all of the files will become inaccessible, if the storage medium falls into the wrong hands.

The workflow of CS consists of:

1. The creation of a new encrypted volume: the choice of storage location, the choice of crypto provider and access ID.
2. Connection of encrypted volumes (mounting): All volumes are added to the encryption library on the left side of the interface. Connecting a volume makes it accessible as a new logical drive, which can then operate as all other disks. The transparent function of CS guarantees the normal functioning of the disk, while protecting the information stored on it.
3. The detachment of the encrypted volume (dismounting): This is performed at the user's request after the user is finished working with the volume or automatically during shut down or when the user restarts computer.

Steps 2 and 3 are repeated every time. CS does not allow eliminating or reducing some of these steps, because this would inevitably reduce the level of protection. While the volume is not connected, the data in the encrypted volume is not available for reading or modification. Even if the storage device falls into the wrong hands, without the personal ID, which is encrypted, the volume cannot be connected all that will be found is a set of meaningless bytes.

The great disadvantage of this system is that files larger than 10-20-50 GB on the disk will leave some signs that they are crypto containers. Therefore, the main principle of protection - to hide the fact of protection - is radically disrupted. In practice, nobody will hack into such disks, because it is easier to get a password or the key file from the user. There are many methods for this.

In CS such files are masked, which significantly complicates the procedure for obtaining access to the data.

Also, a huge drawback is that when mounting the disk all the data is decrypted, not only that which is used. For example, if a user needs one MS Word file to work with, and the crypto disk contains 10,000 files. The user mounts the disk with all 10,000 files, and 9,999 will not be needed. This is not about speed, but as you can see from the chapter "Methods of data theft," it is extremely dangerous to keep all data decrypted for a whole working day. To do so would be absolute nonsense.

Another drawback is the ability to connect to any logical drive on the network. Even if it is not installed with total access to a disk, there are many ways to connect to any drive, if the user uses their computer in a networked environment.

When the user works on a terminal server (MS RDP), all disks are visible to all users.

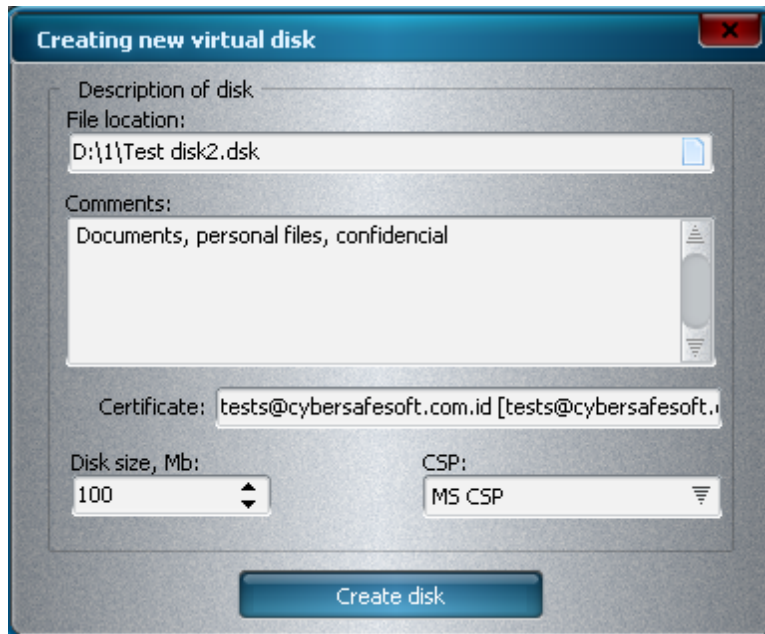
In our opinion, a good use for crypto disks is placing a database for common use on them. For example, there is a certain PC in a network on which the crypto disk and database will be installed, and to which multiple users will connect. The disk is mounted, and it is public and there is a password set to use the resource.

In other cases, we would not recommend using the crypto disks. In CS it is much more convenient to set FOU, Secret, and other tags on the files and folders. The data is always available in CS explorer, where it is hidden from the eyes of outsiders, and at any given moment only the files that the user is working with are decrypted, and the files are not visible

when using a remote connection (Radmin, VNC, TeamViewer), nor are they visible when user tries to access the disk through the network and so on. If after all that, an intruder gets access to the files and finds them, they are ALWAYS encrypted, except for the 2-3 files that are being used currently, but they are still locked from copying.

We use crypto disks in CS only because many users are accustomed to working with them.

8 Generating



In this form, the user must:

1. Select a storage location for the crypto disk.

A good choice would be a previously hidden folder on the disk. After this the certificate, which will be used for encryption of the session key is ascertained.

2. The size of disc and crypto provider is then chosen.

The disk is encrypted by the generated session key, which is 256 bits long for AES and GOST algorithms. A session key is encrypted with a public key of certificate with a length from 1024 to 4098 bits. A system like this is guaranteed to work against any intruder in 2011: from the amateurs to special services. The advantage of this system compared with a password system in all other software types is that the length of a session key has a maximum of 256 bits or 32 characters. Just imagine having to remember a password up to 32 characters. Usually, the users set weak passwords of 6-8 characters, which can be broken. Another advantage is that these keys do not need to be memorized.

Creating a disc requires a few words. There are 2 methods of creating crypto containers. The first is to create a file, and then connect it as a logical disk and format it. This procedure takes a few seconds. For example, PGP functions in this manner. The second method involves the

creation of a file and the encryption of it, and only then it formats and connects it. This procedure takes 10 times longer than the first, however, it is considered more reliable (TrueCrypt). CS has based its work on the second method. The table below shows some comparative characteristics of working with crypto disks.

Table No 1. Speed of the crypto disks.

Name of software	Time of creating a disk 1GB (sec.)	Data transfer time on disk 766 MB of data (sec.)
<i>TrueCrypt</i>	20	29
<i>CS</i>	30	35
<i>BestCrypt</i>	50	29
<i>PGP</i>	10	56
<i>InfoWatch CryptoStorage</i>	10	126

Measurements were taken on a PC with Vista OS, 4MB RAM, 4- processor Extreme X9650, with a 766 MB. mkv file.

Thus, it is clear that those programs, which use crypto disk encryption technology at the beginning work much faster with data. Therefore, it is better to wait the extra 2-3 minutes while creating a disc, to get better data protection and speed later.

8.1 Mounting

Once it is created, the disk will appear in the library of drives. Click on the "mount" button and then select the proper letter and the disk will be connected as a logical disk and will be accessible for any activities in the Windows operating system. After connection, the link icon appears on the left of the disc. □ The remaining functions of crypto disk (unmount, open the file of crypto disk, unmount all, delete) in our opinion do not require special explanations.

8.2 Auto-mount



When the user runs CS the selected disk will be connected to the letter which the user selected and checked in the box "Automate at startup ...". It's very convenient to have a constant need for a permanent letter: Database, unlicensed software and so on.

9 E-mail encryption

Outlook Express - Outlook 2010, The Bat!, Eudora - all e-mail clients support S / MIME. To encrypt an e-mail you need a file with the private and public key and a certificate in PKSC # 7 format. Some of them require these files to be installed in certificate storage, others import them into their certificate storage, therefore, they need a .pfx (p.12) file.

With CS a user can export an ID in any form, including .pfx (see the chapter "ID Export").

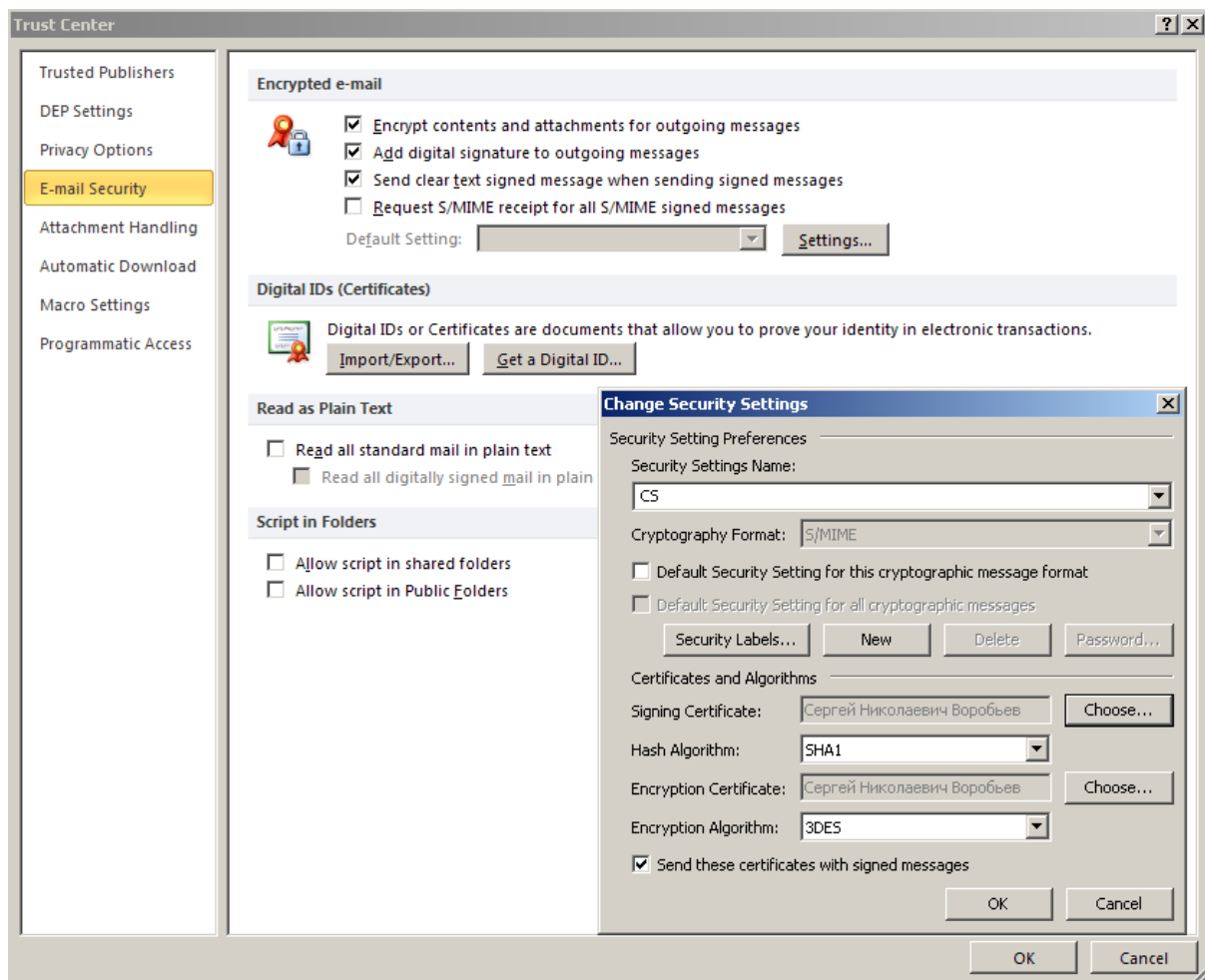
9.1 Outlook.

In case of Outlook the export is not required because keys are already installed in the active state of CS in certificate storage and are ready to use.

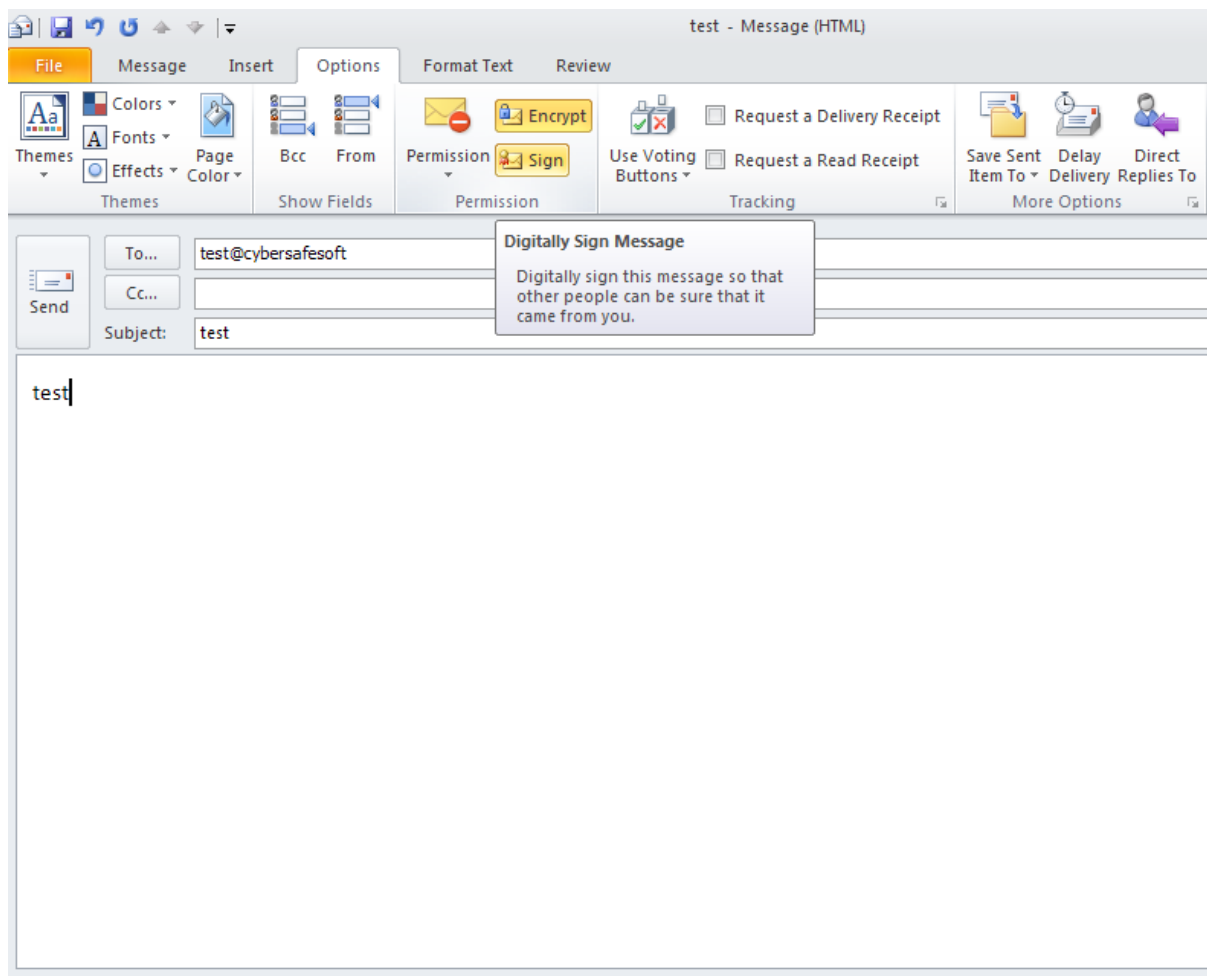
To do this:

1. First you need to install the certificate in Outlook.

File-Options-Trust Center-Email Security-Settings-Choose...



2. Then to check “Encrypt all outgoing”, “Sign all outgoing”.



Now you need to check the encryption on yourself.

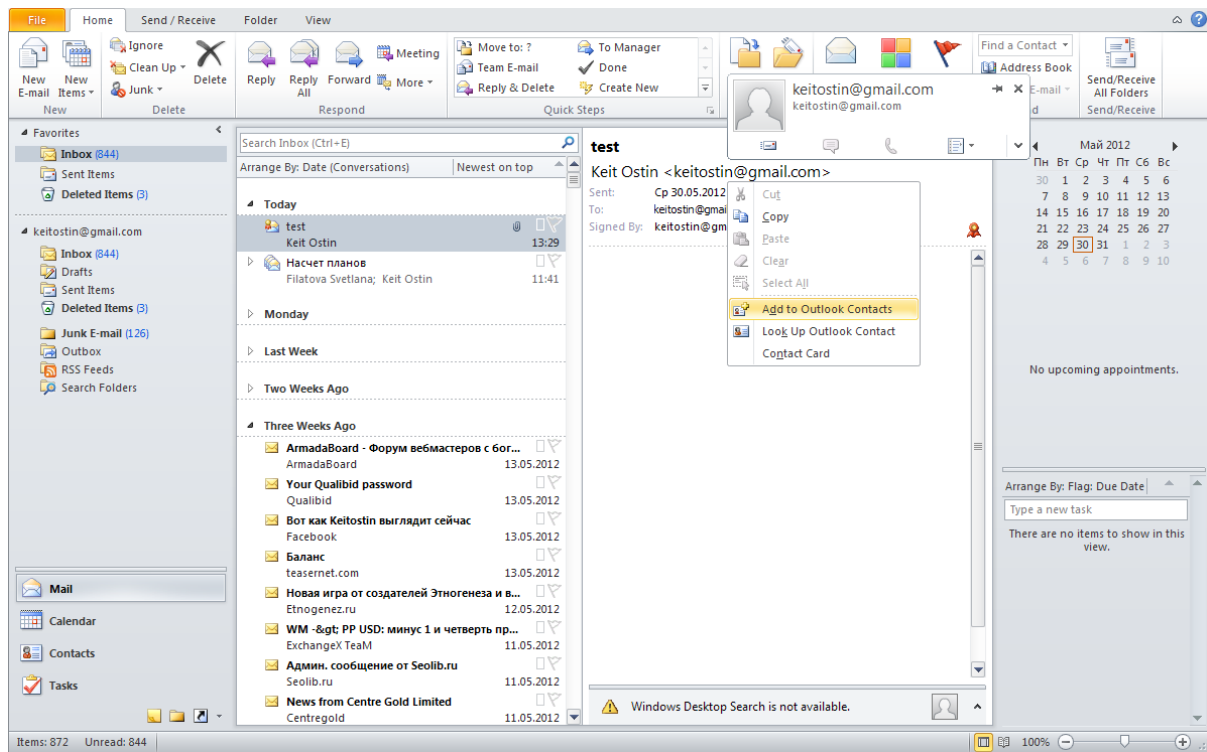
1. Write a letter to yourself.
2. Then go to the Options tab and verify that Signature is checked, click "Encryption" to disable.
3. Send.

If you do not disable the encryption key you will see a message stating that there is no recipient's certificate and encryption is impossible.

Next:

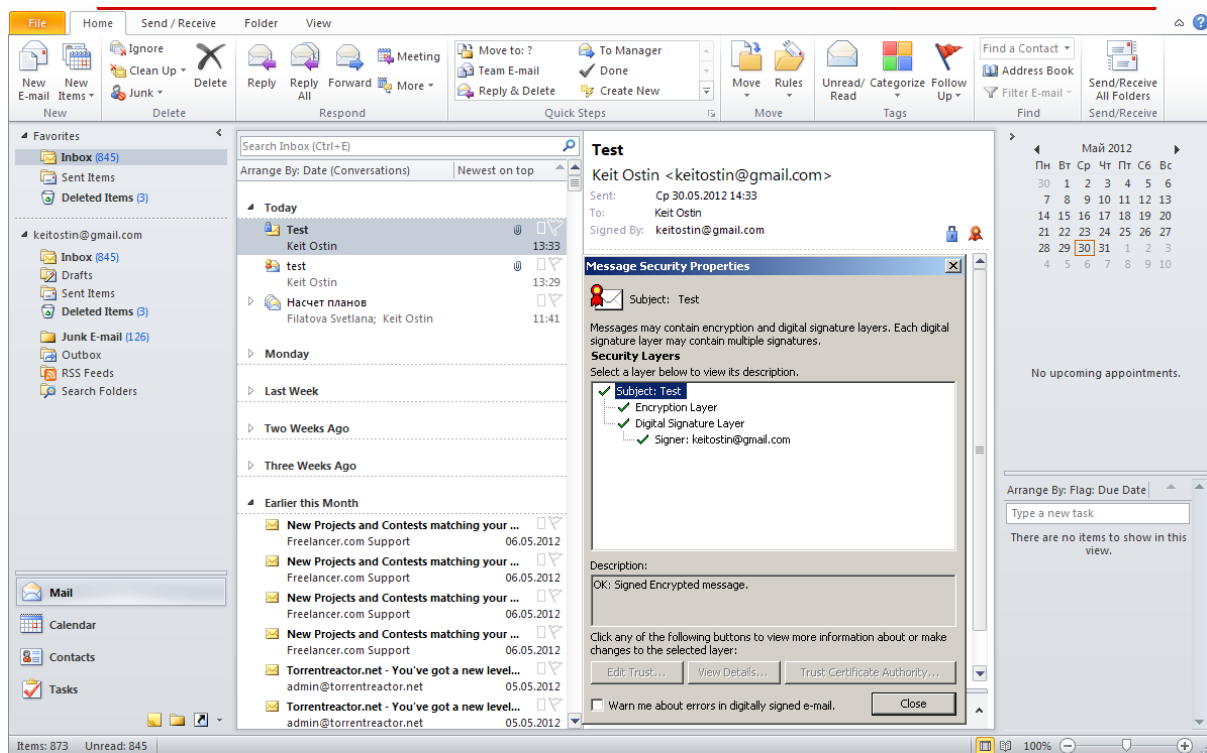
1. The e-mail with signature is received.
2. Open the sender field (From:).
3. Right click, and add to contacts.
4. Select the "Certificates" tab in the contacts and make sure that certificate appears in the contact.

5. Then click "Save and exit".



Now the user creates a new e-mail, picks himself from the list of contacts, and leaves on the "Encrypt" button and clicks "Send."

Now we receive an encrypted e-mail and we can see that the letter came with a blue padlock icon. To read and decrypt it, double click. To test the algorithm and the recipient's e-mail, we can click on the padlock and then on "Levels of encryption."



We should also send the certificate with a signature to those, who want to encrypt for us and we should get the certificate with a signature from them as well. We add contacts and can encrypt.

If the certificate is valid, and a signature belongs to an owner of an e-mail, the user will see the green check marks when checking the signature.

Outlook checks the certificate as follows: if the issuer of the certificate is trusted, the certificate is also trusted. In this case on first start of CS, CyberSafe CA is automatically added to the trusted list. Also we need to know if the sender's certificate contains the phrase e-mail ivanov@gmail.com and there can be no more certificates issued by CyberSafe CA for the e-mail of ivanov@gmail.com. Thus, if the user himself does not add some pirate CyberSafe CA certificate to the root centers, then all the letters he receives with a green check mark next to the signature can be trusted.

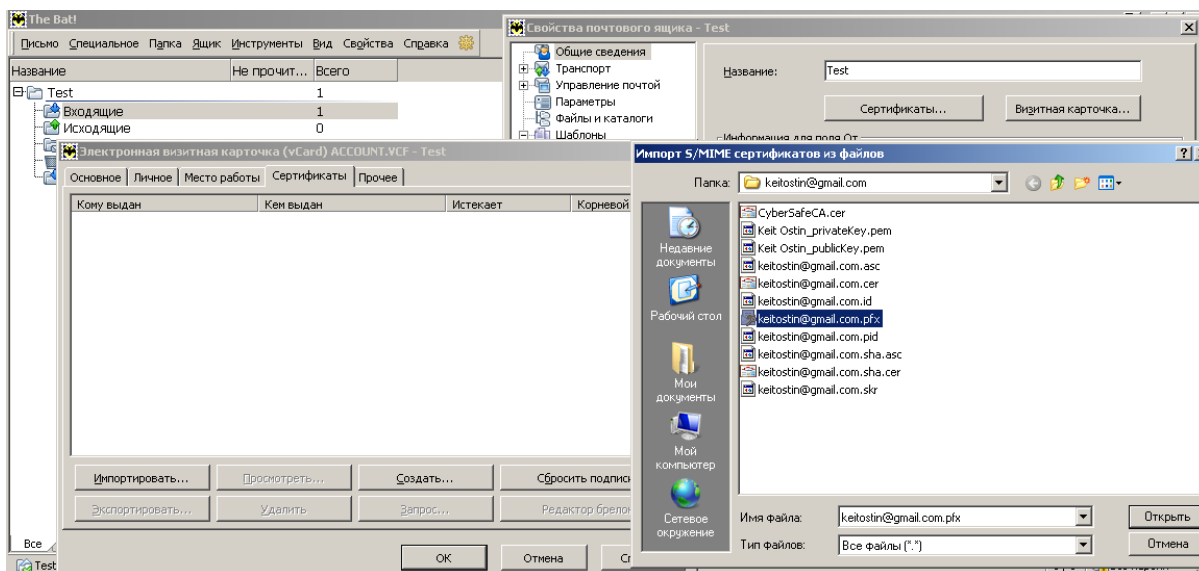
When checking the files, there is even more rigorous inspection of certificates.



Attention! Some programs and services (Thunderbird, Outlook Web Access, Windows Mobile ActiveSync) require online verification of the certificate for its withdrawal (Revocation). We believe this is absolutely useless for safe functioning. The certificates of CS will be void, as they did not pass this test. CS offers very flexible work with the certificates and it allows them to be created on a user's PC without any unnecessary inquiries. In addition, CS does not allow 2 identical certificates to be created with the same e-mail address. Therefore, we do not set the center of certification on a public server. If you still need to use such programs or services, you can receive a free certificate from COMODO for example: <http://www.instantssl.com/ssl-certificate->

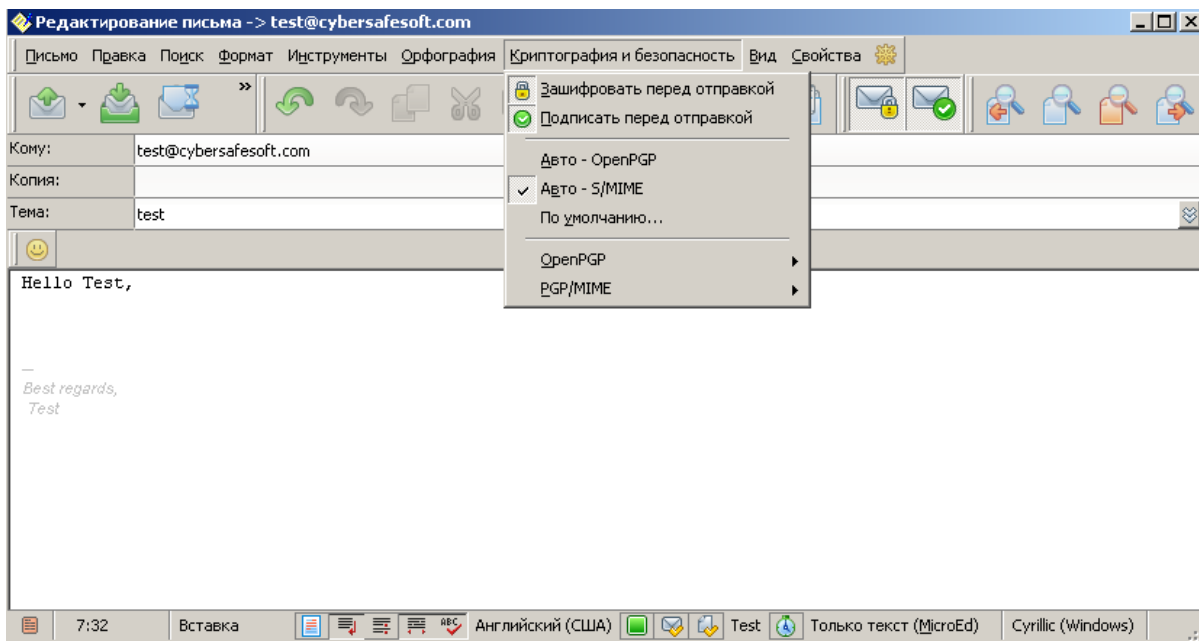
products/free-email- certificate.html then you can import it into CS. However, be aware that such a certificate cannot be used for EFS encryption.

9.2 The Bat!



Tools - Properties of the mailbox - General - Certificates - Import - (enter password). After installing, the certificates will not be trusted. Double click on the Personal certificate - Path of certification - Choose CyberSafeCA - Add to trusted.

Create a new mail and check it for encryption and signature. Enter the password to .pfx. Click OK.



Then, send the certificate with a signature to those, who want to encrypt for us and we obtain from them their certificate with a signature. We add to contacts and can then encrypt.

10 Encryption of Skype

Skype is the best and most popular client for business people. However, few people think about how Skype functions. Skype is in fact the most secret and little known client that is available today. Its operating principle is clear, but its functioning methods, as well as the information that Skype sends to the network remain unknown.

A few people know that if a user has sufficient PC resources (channel width, and a static IP) that user, without knowing or choosing to becomes a super node in the peer network. Traffic from other Skype clients flows through this network. There is no message server as in ICQ, the flow of traffic passes through randomly selected sites using Skype.

Skype bypasses all firewalls, and sends a large flow of information to the network. The traffic is encrypted, and therefore it is impossible to establish what information is being sent.

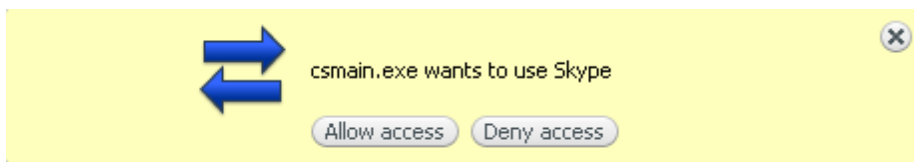
In connection with such sophisticated encryption and the company's unwillingness to disclose its code, a question has arisen about the real purpose behind Skype. In addition, many experts agree that behind the scenes, Skype works closely with U.S. government agencies, because such a large number of phone calls and correspondences cannot simply be left uncontrolled by the NSA. Therefore, the safety of correspondence and calls over Skype is a very big issue.

But the widespread use of Skype in the business community, as well as the complete lack of protection solutions regarding correspondence over Skype on Windows inspired us to create a type of forced encryption of Skype chats before they get to the network.



How To:

1. You should right click on the icon of CS in the notification area to display the shortcut menu.
2. Then to select "Encryption of Skype."



The only way to work with Skype is through its API. Therefore, when you connect CS to Skype, an inquiry will appear, press "Allow access."

3. Now click on the contact with whom you want to encrypt in the Skype contact list.
4. After that right click on the CS tray icon and choose "Assign certificate."

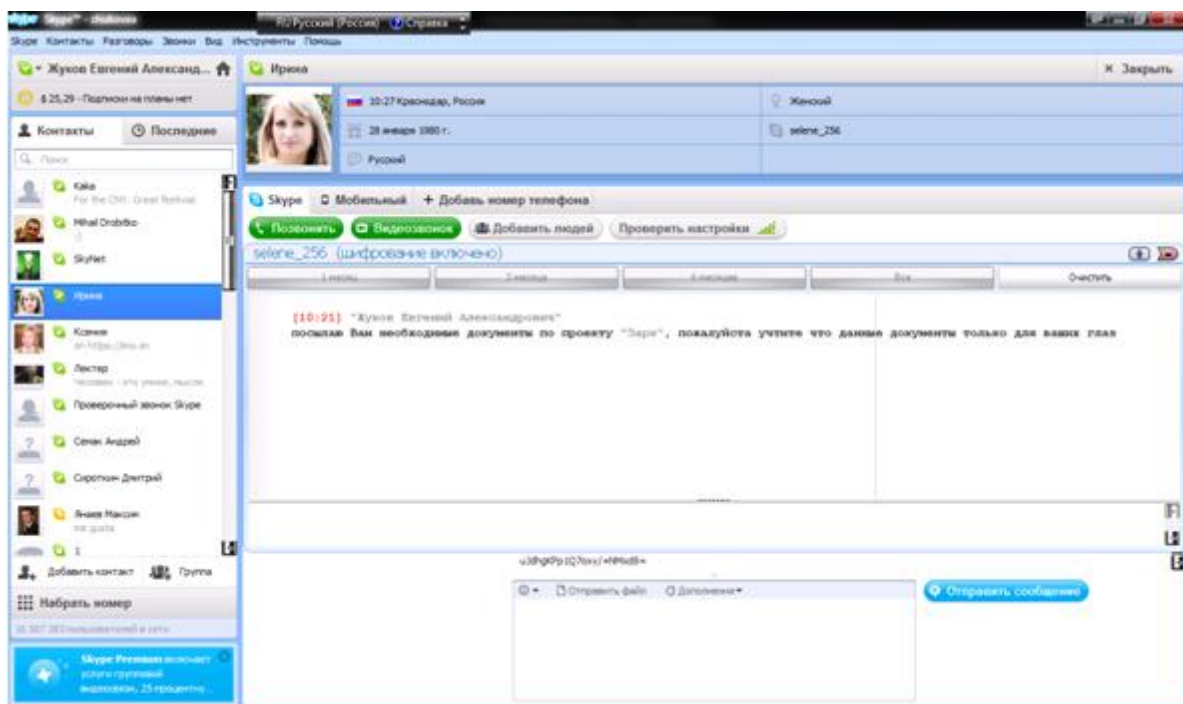


Attention! The certificate of the contact and not of the user is what is assigned.

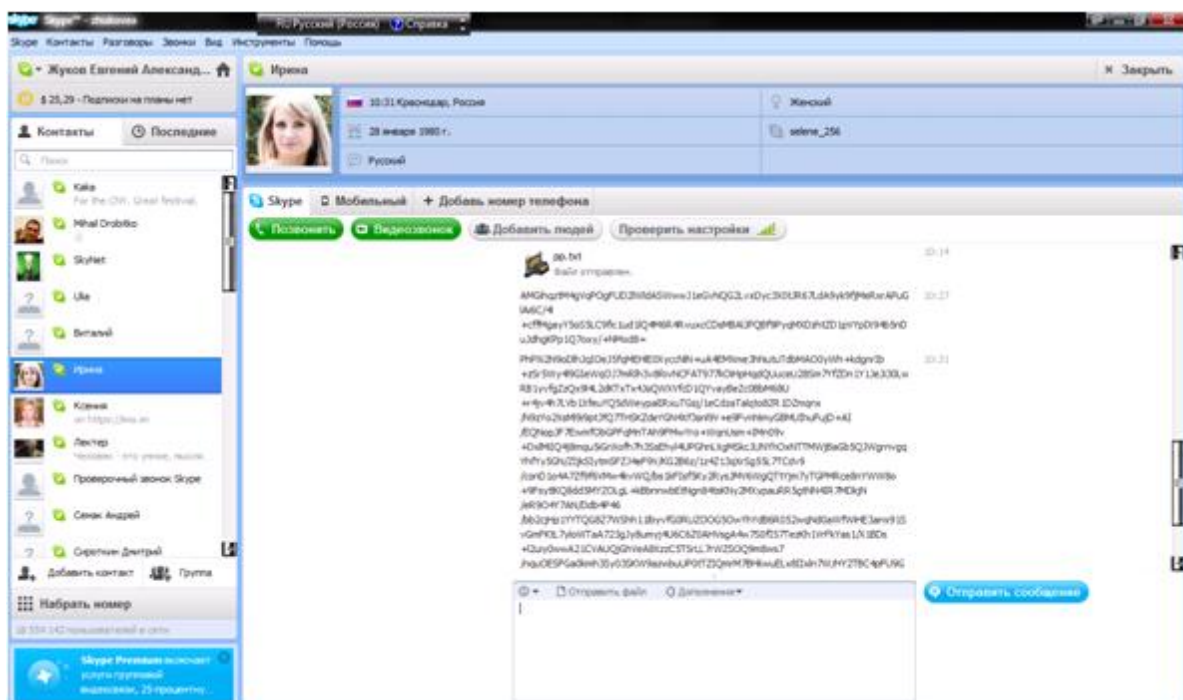


Before the certificate is assigned, "Encrypt" is not available. After clicking "Assign certificate," a list of certificates for this contact will appear. In order to share the certificates with a contact one should pass to the other his .pid file and import it, see the chapters "Export" and "Import".

After the certificate is assigned, "Encrypt" becomes available. After you click encrypt, a special window will appear, which will automatically fill the reading area in which the process of encryption and decryption of the messages will start.



As you can see, a window for text input in Skype is available for sending not encrypting messages, files, and smiles. Also, the user sees when a contact sends a message normally.



When you select another contact with which encryption is not enabled the window of encryption disappears. When you return to the contact with whom communication is encrypted, the encryption window will appear again.

An .id (.pfx in the certificate storage) by the default is used for decryption. Therefore, the transmitted .pid must correspond to it, otherwise the message can not be read.

11 Methods of information theft

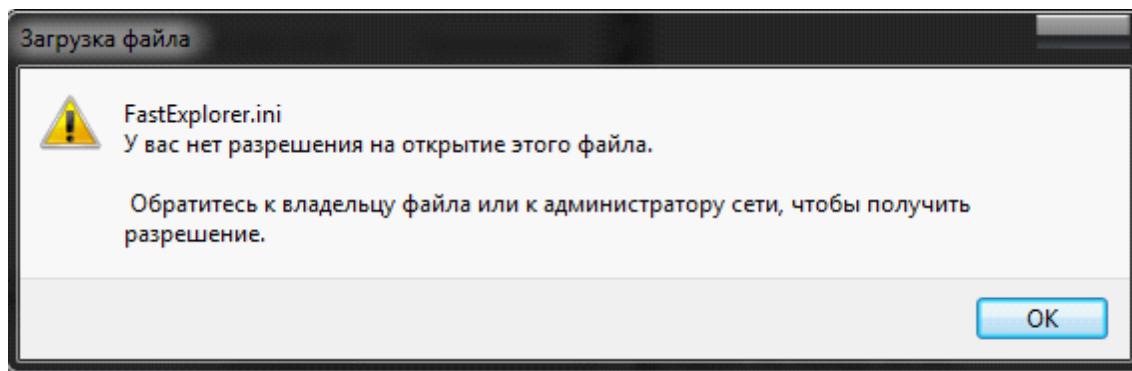
It should be understood that any serious theft is preceded by thoroughly studying the target. The type of target must be determined: male, female, level of PC knowledge, which programs are used for chat, e-mail, which programs are used for the protection of information, etc. The more studying done by the thief, the longer it will take him to prepare for the theft. When the target is a company, not only the methods of protection, and network topology are studied, but every employee, because the human factor is weakest link in any protection.

11.1 Trojan

Trojan programs send information from the infected computer to their owners. Usually this is done through port 80, which is always open.

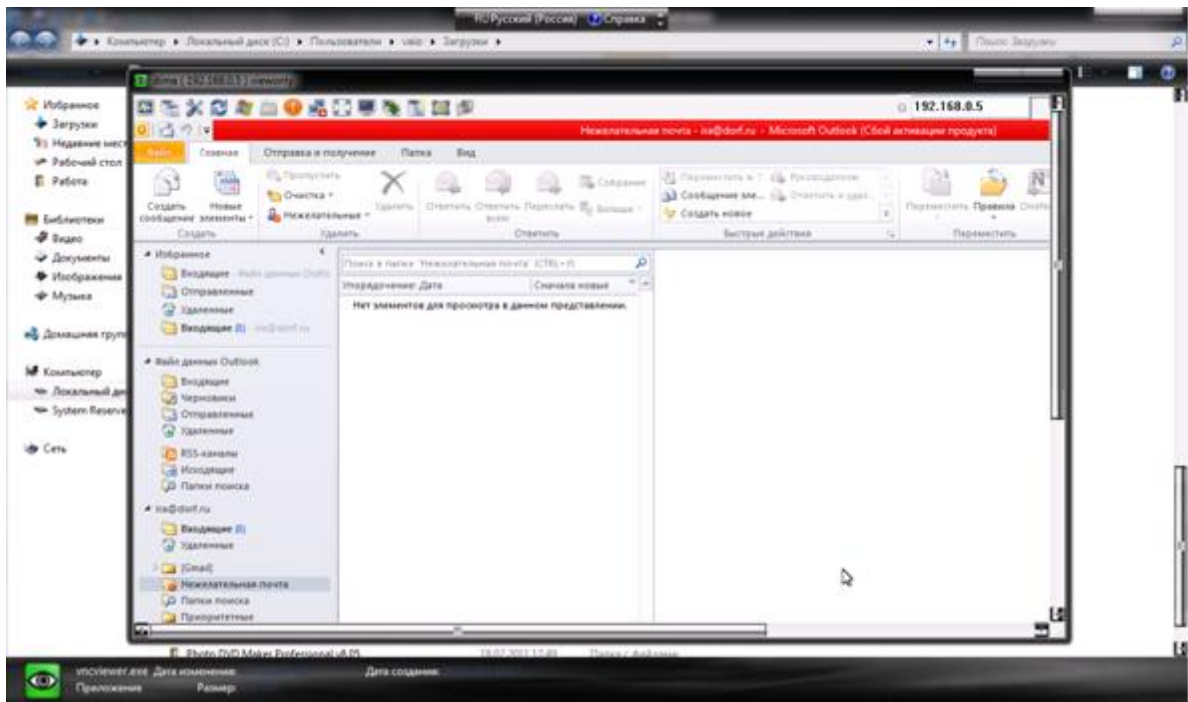
Methods of security already performed by firewalls are not considered by us. Therefore, regarding CS we can say that the counteraction is to encrypt the important information. Say example, the target is a document on a personal laptop. The most convenient way would be to set a tag for a folder with important documents as Secret. CS encrypts a folder and hides it. At the same time they remain all encrypted. If the Trojan program tries to send a file through the hidden channel then this file will remain encrypted.

Attention! You cannot use FOU (EFS) to protect from Trojan programs, if CS is active. The active state of CS is the state in which all keys are installed in certificate storage. EFS automatically decrypts and sends the file. In a lockup state, when CS is not running, any attempt to move such a file (an attempt to transfer it outside the PC) will fail.

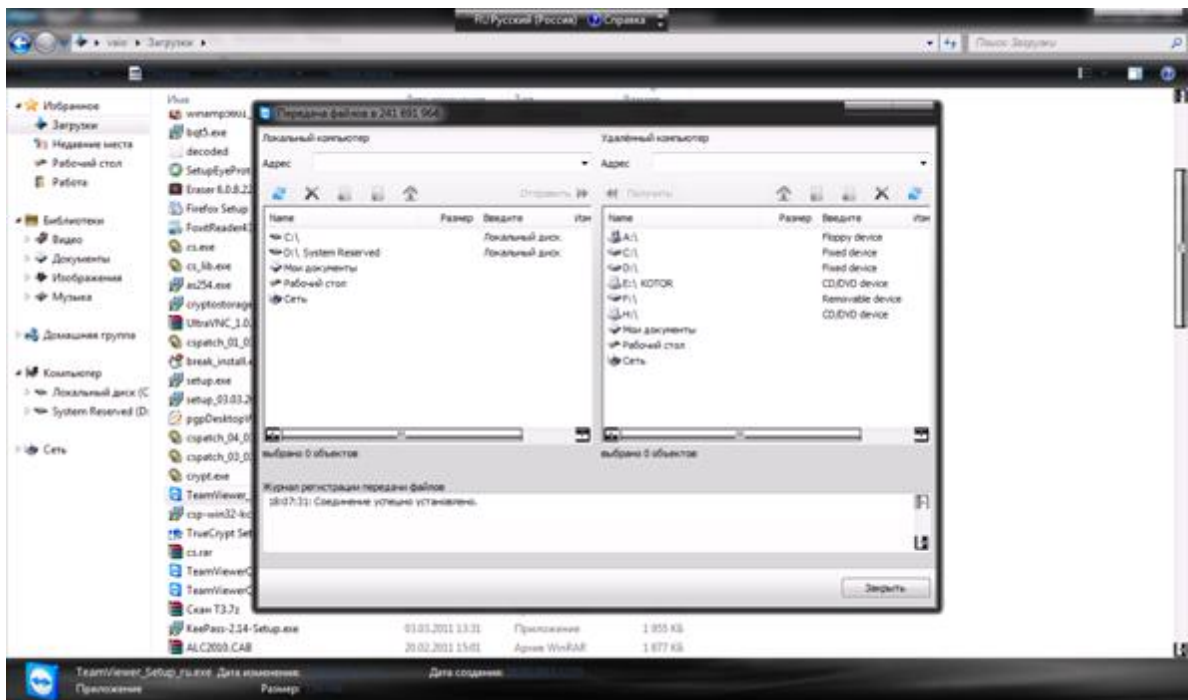


11.2 Remote Desktop

Trojan programs may be based on a modified TeamViewer, Radmin, UltraVNC, and so on. They are very suitable, therefore, they are the most common methods of stealing information.



Here is the connection to the target through UVNC. The viewing of the information is certainly very important, but it is still very important to copy the information from the victim's computer.



This is done through "File Transfer", for example, TeamViewer. Now the intruder can see if a crypto disk is currently mounted in the victim's PC, all information can be copied, and not just information that is being used by the target. In the case of the labels FOU, Secret, and so on,

this is impossible. The hidden folders are not visible through TeamViewer. Even if the invader sees the CS explorer, then without him taking control for a long time, which cannot happen secretly, it will not help him at all. All files are always encrypted.

The interception of control is clearly visible to the user. However, TeamViewer can disable remote display. Therefore, if the screen suddenly turns black without apparent reason, you should immediately reboot it or shut down the PC, while also rebooting and turning off the Internet. Put the firewall in Custom mode, when on every access of any application in the network there is a question set. Also, make sure there are no suspicious files added in the list of trusted applications and so on.

11.3 Seizure of PC by law enforcement authorities

This is a very common situation in business.

If you do not have the signs of CS being installed on your PC (including this guide), it is very unlikely that someone will suspect that you are hiding information. Even if they suspect, they need to know exactly how CS works in order to find the information, otherwise it would take too much time for the various attempts that would be required. Even if the information is found, it is encrypted. Here everything depends on user, who should not give the keys to start CS or if the keys are stored remotely on a token, the user should not give anyone the token itself.

It is not possible to decrypt the information of EFS, nor even AES, GOST or BlowFish. In order to test CS, the user can encrypt a few files with EFS in manual mode or FOU, then download a demo version of ElcomSoft EFS Recovery, but CS should be in lockup mode or switched off (because it will set the keys) and then try to decrypt the encrypted EFS data on the disk. Once again, ElcomSoft gives a 99% guarantee that they can decrypt EFS files.