

CyberSafe® for Windows

User's Manual



Table of Contents

General information about CyberSafe Top Secret	1
What's new in CyberSafe Top Secret 2.0	5
Notation Conventions used in this Manual	7
Who should read this Manual	8
License Agreement	8
Terms and definitions	8
Subject of the Agreement	8
Copyrights	8
Terms of Use	9
Duration of the Agreement	9
Responsibility	9
Guarantees of the Vendor (Supplier)	9
Licensing terms and conditions, notices and information of third parties	10
Assistance on how to use the Software	12
Additional information about the Software	13
Contact Information	13
CyberSafe Top Secret. Basics	2
Terminology and main functions of CyberSafe Top Secret	14
Terminology of CyberSafe Top Secret	14
Main functions of the Software	15
Symmetric and Asymmetric cryptography	16
More about cryptography	16
Getting started with CyberSafe Top Secret	16
Installation of CyberSafe Top Secret	3
Before installation	18
System Requirements	18
Installing and configuring CyberSafe Top Secret	18
Installing the Software	19
Creating a Certificate and configuring the software	20
Uninstalling CyberSafe Top Secret	21
Transferring CyberSafe Top Secret from one computer to another	22
CyberSafe Top Secret User Interface	4
Accessing CyberSafe Top Secret's main functions	24
The main window	24
Working with CyberSafe Top Secret Keys	5
Viewing keys	26
Creating a key pair	26
Using passwords	27
Keeping a Private Key private	27
Measures used to protect your Private Key	28
Creating backup copies of a Private Key	28
What to do if a Private Key is lost?	29
Distributing a Public Key	29
Publishing on a server	30
Attaching a Public Key to an e-mail	31
Exporting a Public Key to a file	31
Obtaining a Public Key from other users	31
Downloading Public Keys from a Key Server	31

Importing Keys and Certificates	32
Working with Key Servers	32

E-mail security 6

Encrypting e-mails with CyberSafe Top Secret	34
Exporting a Certificate to PFX format	34
Microsoft Outlook	35
Mozilla Thunderbird	41
The Bat!	45

Encrypting files with CyberSafe Top Secret 7

About file encryption	47
Encrypting files and folders	47
Public Key Infrastructure based encryption	48
Password based encryption	50
Creating encrypted .zip files	51
Additional encryption settings	53

Passwords and passphrases 8

What to use: password or passphrase?	55
Password strength indicator	56
Creating a strong password	56

1

General information about CyberSafe Top Secret

CyberSafe Top Secret is software that uses cryptography to protect your data from unauthorized access.

It has the ability to create certificates and encryption keys. Its toolkit can be used in such information fields as: file and folder encryption, E-mail protection, digital signature creation, as well as working as a Certification Center.

CyberSafe Top Secret has been tested and proven reliable for working on all Windows operating systems on PC.

The program encrypts information using the most common algorithms (AES, 3DES, ГОСТ, RSA, BlowFish) depending on the required degree of secrecy. Furthermore, CyberSafe Top Secret uses the libraries of three crypto providers (OpenSSL, OpenPGP, Crypto-Pro), making it an extremely flexible application.

For a more complete understanding of the program, you are encouraged to read the sections "*Terminology and main functions of CyberSafe Top Secret*" and "*Symmetric and Asymmetric cryptography*".

In this Section

What's new in CyberSafe Top Secret 2.0	5
Notation conventions used in this Manual.....	7
Who should read this Manual.....	8
License Agreement.....	8
Assistance on how to use the Software	12

What's new in CyberSafe Top Secret 2.0

CyberSafe Top Secret version 2.0 combines all the basic functions and quality of the previous version, and also has a number of improvements and additional options. At the same time, it has a completely redesigned user interface that makes working with CyberSafe simpler, more intuitive and more user friendly.

Version History

Version 2.0.0.21 (12.09.2013)

- Added the ability to select default encryption certificates.
- Corrected: made the status "Not available" status available for Revocation when the trust level is set at "Trusted by user custom policy."

Version 2.0.0.20 (11.09.2013)

- Corrected: Creation and installation of the CryptoPro Root Certificate.
- Installation of the CryptoPro Root Certificate without administrator rights.
- Corrected: An error when sending information about a certificate to a server with spaces in the certificate name.
- Added: Export CryptoPro Certificate.
- Added: Import CryptoPro Certificate.
- Changed: Certificate trust determination algorithm
- Corrected: Blank list of certificates for encryption after import and decryption.
- Corrected: Impossible to create CryptoPro Certificate after a valid certificate was rewritten.

Version 2.0.0.19 (23.08.2013)

- Corrected: Certificates work in Outlook and iPhone.
- Added: Creation and installation of the Root CryptoPro Certificate.

Version 2.0.0.18 (09.08.2013)

- Corrected: A certificate generation and storage bug.
- Changed: The structure of the database for Certificate serial number storage.
- Added: The ability to store and retrieve information about Certificates on the server by serial number.
- Added: Certificate verification in database by the serial number (Check Now).

Version 2.0.0.17 (06.08.2013)

- Changed: Publication confirmation code to 5-digit, code entry box appearance.
- Correct operation of Certificates in Outlook for digital signatures and encryption implemented.

Version 2.0.0.16 (05.08.2013)

- Detailed certificate creation progress information added.
- Prompt to overwrite a certificate during import added.
- Help-Home page added.
- Fixed a bug that caused exported foreign certificates to lack .pgp files.
- Fixed a bug that made "Next" button stay active after decryption.
- Fixed a bug that made decrypted files invisible in the folder during decryption.
- Unnecessary items in certificate setup removed.
- Added: Full stops to the end of the messages.
- Fixed a bug that gave an error message after aborting creation of a Certificate.

Version 2.0.0.15 (12.07.2013)

- Added: Emulation of the mouse and keyboard for the Crypto Pro biological sensor.

Version 2.0.0.14 (11.07.2013)

- Added: Crypto Pro digital signature verification.
- Added: Crypto Pro Certificate deletion.
- Certificate sorting bug fixed.

Version 2.0.0.13 (09.07.2013)

- Added: Checking the availability of a Certificate for encryption.
- Added: Crypto Pro digital signature creation added.
- Changed: Progress bar for adding files and encryption.

Version 2.0.0.12 (08.07.2013)

- Fixed a bug that would cause access issues after several encryptions/decryptions.
- Added: Progress bar for adding files to encrypt.
- Decryption progress bar made easier to understand.
- Added: Full stops to messages.
- Fixed a bug that caused issues with the "Delete" button in the file list.
- The first Certificate in the list for encryption became active.
- Fixed a bug that caused PGP keys to be lost after import during publication.

Version 2.0.0.11 (05.07.2013)

- Added: encryption and decryption of Crypto Pro files.

Version 2.0.0.10 (04.07.2013)

- Added a service to carry out commands with administrator rights.
- Added the ability to create a Crypto Pro Certificate.
- Added a change to the list of certificates for encryption, depending on provider.
- "More Options" button available for OPGP encryption only.

Version 2.0.0.9 (03.07.2013)

- Added: File integrity check.

- Added: Signature-based information extraction if the certificate is not found in the database on the server.

Version 2.0.0.8 (02.07.2013)

- Added: Trusted tag for OPGP certificate.
- Added: Checking on the server if a certificate is revoked.
- Bug fixed: error during file decryption if the necessary certificate is not there.
- Bug fixed: error in deleting certificate after decryption and signature check.

Version 2.0.0.7 (01.07.2013)

- Corrected: Right-Left scrolling when screen resized by default in certificate screen.
- Corrected: End of Access violation decryption.
- Corrected: Impossible to press More Options.
- Corrected: There should be a progress bar when unpacking files.
- Deleted: Horizontal scrolling in the certificate list.

Version 2.0.0.2 (14.06.2013)

- Added: File encryption.

Version 2.0.0.1 (07.06.2013)

- Prototype\Alpha

Notation conventions used in this Manual

Notes. Additional, but important details that draw your attention to important moments when using the Software. Reading them will help you use Cyber Safe Top Secret more efficiently.

Warnings. Indicate the possibility of data loss or a minor security breach. Warnings will tell you about situations where problems may arise if you do not take the necessary precautions. Give these points their due attention.

Alerts. Indicate the possibility of a significant loss of data or a serious security breach, as well as reports of significant problems that may arise if not taken timely measures to prevent them. Treat the warnings very seriously.

Who should read this Manual

This manual is addressed to anyone who intends to use the CyberSafe Top Secret to protect data on personal computers running the Windows operating systems.

Note. If you are not familiar with cryptography, refer to the "*Symmetric and Asymmetric cryptography*" and "*More information about cryptography*" sections.

License Agreement

This License Agreement is a general offer between "CyberSoft," OOO and the User, a physical or legal entity. This License Agreement in the case of the consent expressed in the form of silence within 7 days from the date of purchase, in accordance with Art. 433 Civil Code Russian Federation has the power of Contract.

Terms and definitions

- The Product is understood to be a system of computer programs for PC, including

media and documentation, which is subject to copyright and protected by law.

- Everywhere in the text the word "documentation" is understood to mean all printed materials and the media containing the documents in electronic form. The Documentation is an integral part of the Product.
- This Product (the software), including the media and printed materials, is distributed under a License Agreement.
- Subsequent installation of the Product is considered consent to the conditions of the License Agreement and its entry into force.
- In case of disagreement with any of the terms of the License Agreement, within seven days from the day of receipt of the product, the User must return the entire Product, including printed materials, and packaging with the media to the company that supplied this Product.

Subject of the Agreement

- Subject of this License Agreement is the commercial distribution to the User of rights of use and ownership of the Product.
- All conditions stated below apply both to the Product in whole and to all of its separate components.

Copyrights

- The Product and its components are the intellectual property of the developer and are protected by copyright law © 2013 CyberSoft (OOO).
- The right to use the Product is provided only to the end User as the owner, and no other third parties, without the written approval of "CyberSoft," OOO.

Terms of Use

- The User can store, install and use only a certain number of copies of the Product. The User has no right to store, install or use (in installed or installed form) more copies of the Product than granted to him and defined in the relevant documents on the right to use the Product.
- The user agrees not to distribute this Product. Distribution of Product is understood to mean granting access to third parties of faithfully reproduced components of the Product in any form by sale, rental, leasing, lending or other methods of alienation.
- The User has no right to carry out the following activities:
 - allow the use of Product by people not entitled to use it;
 - attempt to disassemble, decompile (convert compiled code into the source text) the programs and other components of the Product;
 - make any changes to the compiled code of the software except those, which are made by the means included in the Product and described in the documentation;
 - do any other actions with the Product infringing on Russian and international standards on copyright and use of software.

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

Duration of the Agreement

- This License Agreement shall enter into force from the moment of opening the package with CyberSafe Top Secret 2 media or installation of the Software from the Product and is valid for the lifetime of the Product.
- In case of violation of the License Agreement terms or inability to continue to fulfill its terms, all components of the Product (including printed materials, magnetic media, information files, archival copies) must be destroyed. The User shall confirm the fact of destruction of the Product in writing. In this case the License Agreement shall be considered lapsed.

Responsibility

- The User purchases the Product and is responsible for its use in accordance with the recommendations set out in the operating instructions.
- Illegal use, distribution, reproduction for third parties, and copying of the software are violations of the Law of the Russian Federation "*On legal protection of computer programs and databases*" and is punishable by law.
- In case of violation of this License agreement, the end User is deprived of the right to use the Product; the warranty service is cancelled.

Guarantees of the Vendor (Supplier)

- The vendor guarantees that the Product is in working order on the condition of observance of requirements of maintenance of operating, transportation, storage, correct use and usage in a "non-viral environment".
- In case of defects in the Software not related to violation of rules of use, transportation and storage the Product is subject to complaint within 10 days from the moment of discovery, and the vendor has to eliminate the defects upon receiving notice of the claim as soon as possible by its power and means up to the point of supplying copies of the product.
- The warranty period for the Product is 12 months.
- The starting date for calculation of the warranty period of the product is the date of delivery of the product, recorded in the form.
- The vendor (Supplier) accepts claims to the quality of delivery of the Product within thirty days from the day of delivery.
- The warranty is expired after the warranty period.

Licensing terms and conditions, notices and information to third parties

- The License Agreement makes reference to information in this file concerning the terms and conditions applicable to included in this product third party software code, as well as to certain comments and other information, that "CyberSoft," OOO has to provide to you under its license to certain software code. Relevant terms and conditions, comments and other information or links to them are given below.
- Notwithstanding the terms and conditions of any other agreements which may be made between you and "CyberSoft," OOO or any of its related or affiliated companies (collectively "CyberSoft"), the following third party software code are "Excluded components" and is subject to the following terms and conditions:
 - Excluded Components are provided "as is";
 - "CyberSoft" disclaims any and all express and implied warranties and conditions with respect to the excluded components, including, but not limited to them, the warranties of compliance or non-infringement of copyright rights, as well as the implied warranties about commercial use or fitness for a particular purpose;
 - "CyberSoft" will not bear any liability to you and will not pay you any losses on any claims related to the Excluded Components, as well as "CyberSoft" will not be liable for any direct, indirect, incidental and consequential damages or penalties related to the Excluded Components.
 - The Program includes software currently developed by The OpenSSL Project (<http://www.openssl.org/>). The OpenSSL toolkit falls under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

"CyberSoft" obtained the majority of the OpenSSL software under the terms and conditions of the following licenses:
 - *OpenSSL License*. Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 - All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
 - The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
 - Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
 - Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
 - This software is provided by the OpenSSL project "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. in no event shall the OpenSSL project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.
- *Original SSLeay License.* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
- If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an

acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

- This software is provided by Eric Young "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.
- The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license (including the GNU Public License).

Assistance on how to use the Software

To learn more about the product please read the following sections.

Additional information about the Software

For more information on Cyber Safe Top Secret visit the program website www.cybersafesoft.com. The website provides detailed video tutorials about how to use the software's basic functions.

On the forum you can ask questions, learn about troubleshooting techniques and the experience of other users.

Contact Information

For technical support, please send an email to support@cybersafesoft.com or use the contact form on the website: <http://cybersafesoft.com/contacts>. Please note that technical support by e-mail is possible only for users who use a paid version of the program.

Company address: Russian Federation, Moscow, Marxist str., 32
Tel.: 8 (800) 555-28-43

2

CyberSafe Top Secret. Basics

This section describes the terminology and basic functionality of CyberSafe Top Secret, as well as providing some important concepts from the field of cryptography.

In this Section

Terminology and main functions of CyberSafe Top Secret.....	14
Symmetric and Asymmetric cryptography	16
Using CyberSafe Top Secret for the first time.....	16

Terminology and main functions of CyberSafe Top Secret

To use the CyberSafe as efficiently as possible, you should become familiar with its basic features, and technical terms, which are discussed in this section.

Terminology of CyberSafe Top Secret

Before you first start working with CyberSafe Top Secret, you should be familiar with the following terms:

- **Encryption.** The process of encoding of information to help protect it from unauthorized access. Gaining access to encrypted information without a special decryption key is impossible, so even if an attacker manages to get it, they will not be able to use it.
- **Decryption.** The process of receiving of encrypted messages and decoding them, whereby the protected data goes back to its original state and becomes available for use.
- **Digital Signature.** Data you send to other users can be digitally signed by private key. Once the recipient gets the files he checks the digital signature on them using the public key and this test proves that the data received is from you and not from anyone else.
- **Verifying Digital Signature.** The process that allows you to determine whether the private digital signature key of a particular user was used to create it or not.
- **Key pair.** The combination of a private and public key. When creating a Certificate in CyberSafe you are actually creating a key pair. In addition to the Private and Public keys, it includes your name and email address, which is very convenient. A key pair is your identification in the digital world the same way as your passport or driver's license identifies you in the physical world.
- **Public Key.** Public-shared key that you send to other users in order to enable them to send you messages encrypted by it (messages that can only be decrypted using the private key) and to verify your digital signature. Public keys are intended for wide distribution. Public and private keys are mathematically dependent on one another, however, obtaining the private key from the public key is impossible.
- **Private Key.** Your personal secret key, which should be kept confidential. Only it will allow you to decrypt data encrypted using the Public Key. Also only the Private Key allows you to create digital signatures, which can be verified using the Public Key.

Warning. Do not entrust your private key or password to anyone! Keep private key completely confidential.

- **Keyserver.** The place Public Keys are stored. Some companies use Keyserver to store their employees' Public Keys, so they can find each others' Public Keys and exchange encrypted messages.
- **Smart cards and tokens.** Portable devices on which you can create or to which you can copy your key pair. Creating a key pair on a smart card or token you increase the level of security because to encrypt or decrypt files or to create or verify a digital signature you will have to have this portable device. Therefore, if an unauthorized user tries to access your computer your encrypted data will be completely safe because your key pair is not stored on your hard drive but on a smart card or token, which is on your person.
A copy of a key pair on a smart card or token is a good way to use it without interacting with the operating system, create a backup copy, and distribute your public key.

Main functions of the Software

CyberSafe Top Secret is a software that uses cryptography to protect your data from unauthorized access.

CyberSafe's functions allow it to accomplish a great many tasks in the field of information security. A list of main functions of the program is given below.

- **File and Folder Encryption.** A function that provides the ability to encrypt any file, folder or multiple files to be stored on a personal computer or to send to other users. Encryption can be Public Key Infrastructure-based (PKI) or password-based. You can decrypt files using CyberSafe Top Secret only.
- **Creating Encrypted Zip-Archives.** A feature that allows you to combine any number of files and folders into single encrypted archive for easy transfer or backup. The zip-archive is password-protected; it can be decrypted on any computer.
- **Working as a Certification Authority.** CyberSafe Top Secret includes the specialized application CyberSafe Certificate Authority, designed for creating, storing and working with certificates, as well as working as a Certification Authority.
- **Email encryption.** A function to protect e-mails that are exchanged via clients such as Outlook, The Bat!, Thunderbird and others. With this feature all your e-mail correspondence will be protected from outsiders.
- **Digital Signature.** A function for creating digital signatures on files and folders using a Private Key, as well as ensuring the verification of signatures using Public Keys.

Symmetric and Asymmetric cryptography

Symmetric cryptography got its name due to the fact that the same secret key is used in the process of encryption and decryption of information. It is also called traditional cryptography. This type of cryptography is great for protection of files, which are not expected to be transferred to other users. However, if you intend to send encrypted data to someone else, especially to people with whom you are unfamiliar, this kind of data protection is not very good. In practice, sending secret keys, especially on unsecured communication channels and updating them in a safe and reliable way is very problematic.

Asymmetric cryptography. In the process of encryption and decryption of information different keys are used – Private Keys and Public Keys. Therefore, this kind of encryption is also called PKI-Based encryption (Public Key Infrastructure). The Private Key is your personal secret key that is used to decrypt messages and create digital signatures. This key should be kept secret from others with the utmost confidentiality. The second key is open or public. In accordance with its name, you can share it with other users. Actually, you have to share it.

Asymmetric cryptography works as follows. Suppose you want to exchange encrypted messages with a friend from another city. Each of you must have CyberSafe Top Secret on your computers. First of all, you both must create your key pairs consisting of public and private keys. Your Private Key you keep secret,

and the Public Key is published on the Keyserver. So does your friend. After that you download your friend's Public Key from the Keyserver, and he downloads yours (other possibilities exist for the exchange of Public Keys; read more about this in section "*Working with keys*"). Now your friend can send you a message encrypted with your public key. Data encrypted with a Public Key can only be decrypted using a Private Key. Even your friend will not be able to decrypt the message, he encrypted. Public and private keys are mathematically linked, however obtaining a private key from a public one is impossible.

More about cryptography

For more information about cryptography, visit the CyberSafe homepage from the main menu of the program.

Using CyberSafe Top Secret for the first time

When you first use CyberSafe Top Secret we recommend you follow these steps:

1 Install CyberSafe Top Secret on your computer

If you are a corporate user, your system administrator may offer you special instructions for installing or configuring the Software. But anyway, installation is the first step.

2 Follow the recommendations of the program

To help you get started with CyberSafe after installation, the program will prompt you through several stages:

- Create a Certificate and a Key pair;
- Publish your Certificate and Public Key on the Keyserver.

If the setup wizard has been configured by the system administrator, the software can suggest other tasks.

3 Exchange Public Keys with other users

After the Certificate is created, you can exchange encrypted messages with other users (having previously exchanged Public Keys). The exchange of Public Keys is the first and important step. To send the user an encrypted message, you need a copy of his Public Key, and to allow the user to send an encrypted message to you, he has to have your Public Key. If you didn't publish your public key on the CyberSafe Server, do it now. If you don't have the Public Key of the user to whom you want to send an encrypted message, the CyberSafe Server is the first place to search for it.

4 Check any Public Keys you download from untrusted servers

If you download a Public Key from an untrusted server try to make sure that it has not been changed and that this key really belongs to the right person. To do this, compare the unique fingerprint of your copy of the Public Key of the user with unique fingerprint of a genuine Public Key (a good way is to call the owner of the key on the phone and ask for information about the unique fingerprint, so you can compare). Public Keys stored on trusted servers, such as the CyberSafe Server have already been checked.

5 Start protecting your files and e-mail

After the Key pair has been generated and you have exchanged Public Keys with other users, you can begin to use encryption, decryption, digital signing and verification with e-mails and files.

3

Installation of the CyberSafe Top Secret

This section describes how to install CyberSafe Top Secret on a local computer, and the first steps of how to use the program after installation.

In this Section

Before installation.	18
Installing and configuring CyberSafe Top Secret.	18
Uninstalling CyberSafe Top Secret.	21
Moving CyberSafe Top Secret from one computer to another.	22

Before installation

This section describes the minimum system requirements needed to successfully install CyberSafe Top Secret on a local computer running Windows.

System Requirements

Before starting the installation, make sure that your operating system meets the following minimum requirements:

- Microsoft Windows 2000 (SP 4), Windows Server 2003 (SP 1, 2), Windows XP Professional 32-bit (SP 2, 3), Windows XP Professional 64-bit (SP 2), Windows XP Home Edition (SP 2, 3), Windows Vista (all 32- and 64-bit versions, including SP 1, 2), Windows 7 (all 32- and 64-bit versions), Windows 8 (all 32- and 64-bit versions).

Note. The Software will be fully compatible with the above operating systems only if they have all the latest Microsoft updates.

- 512 MB RAM
- 88 MB free hard drive space

Installing and configuring CyberSafe Top Secret

This section contains information about how to properly install and configure CyberSafe Top Secret.

Installing the Software

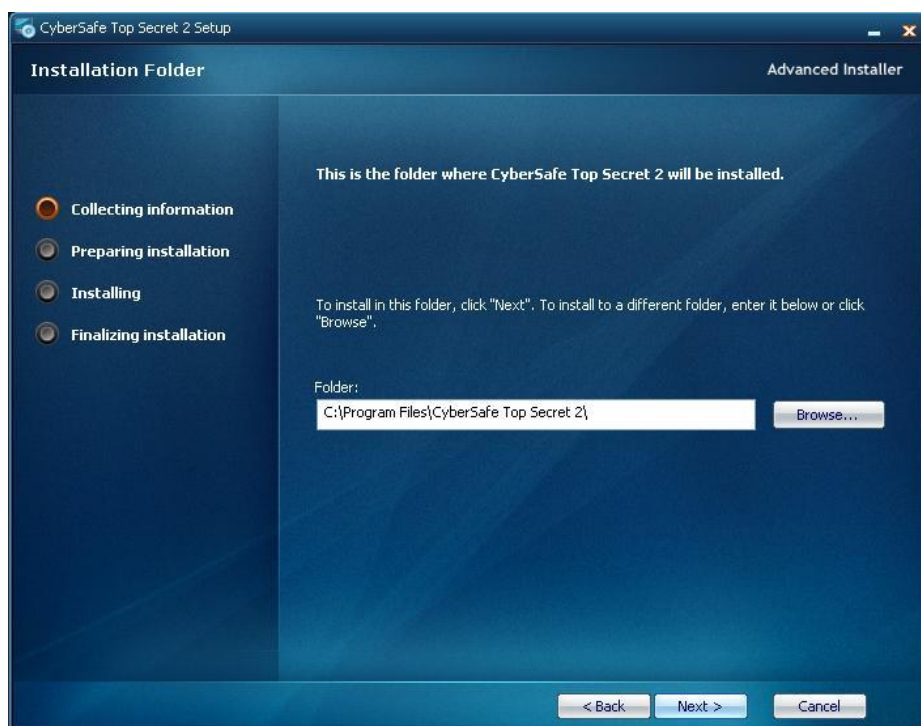
Note. To install CyberSafe Top Secret you must have administrator rights. Before starting the installation, we recommend you close all other applications and programs.

► **To install CyberSafe Top Secret, follow these steps:**

- 1** Find the installation setup file on your computer - a file with *.exe extension.
- 2** Double click on this setup file.
- 3** Follow the instructions on the screen:

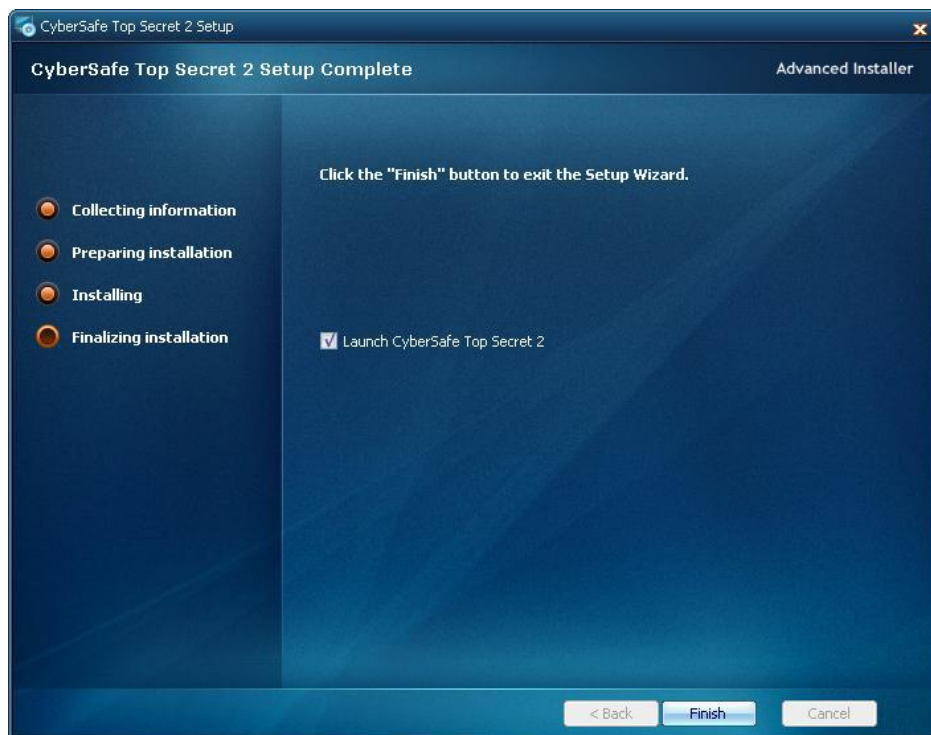
In the CyberSafe Setup Wizard, click **Next**.

The default path for files with the installed program will be as follows: **C:\Program Files\CyberSafe Top Secret 2**. If you want to choose a different installation directory, use the **Browse** button. Then click **Next**:



After you are finished preparing for installation, click **Install**. If you decide to change some of the settings, return to the previous settings, using the **Back** button.

If the installation was successful, on its completion, you will see the following window in which you should click **Finish**. If you want to launch the program immediately after installation, check the appropriate checkbox:



- 4 If you are prompted to restart your computer, do so. Installation of CyberSafe Top Secret 2 is finished.

Creating a Certificate and configuring the Software

Once installation is completed CyberSafe Top Secret and, if necessary, your computer is rebooted, the program will start automatically.



The 'Create Certificate' dialog box contains the following fields and options:

- E-mail *: test@cybersafesoft.com
- Password *: [masked] with a 'Show password' checkbox and a 'Password is strong' indicator.
- Name *: Test Certificate
- Organization Unit: Q&A Dpt.
- Organization: CyberSoft LLC.
- Country: Russia
- Validity, days: 365
- Key size, byte: Radio buttons for 1024, 2048, 3072, 4096, and 8192.
- ☒ Publish after creation
- A photo of a man.
- Buttons: Next > and Cancel.
- A 'Clear' link is located next to the Country field.

It is recommended to fill in the optional fields - this information will be present on your certificate, including your photo. Specify the size of the encryption key in the range from 1024 to 4096 bits and its term of validity. A checkmark in the checkbox *Publish after creation* will lead to automatic publication of your certificate on the CyberSafe Server - leave it enabled and click the **Next** button.

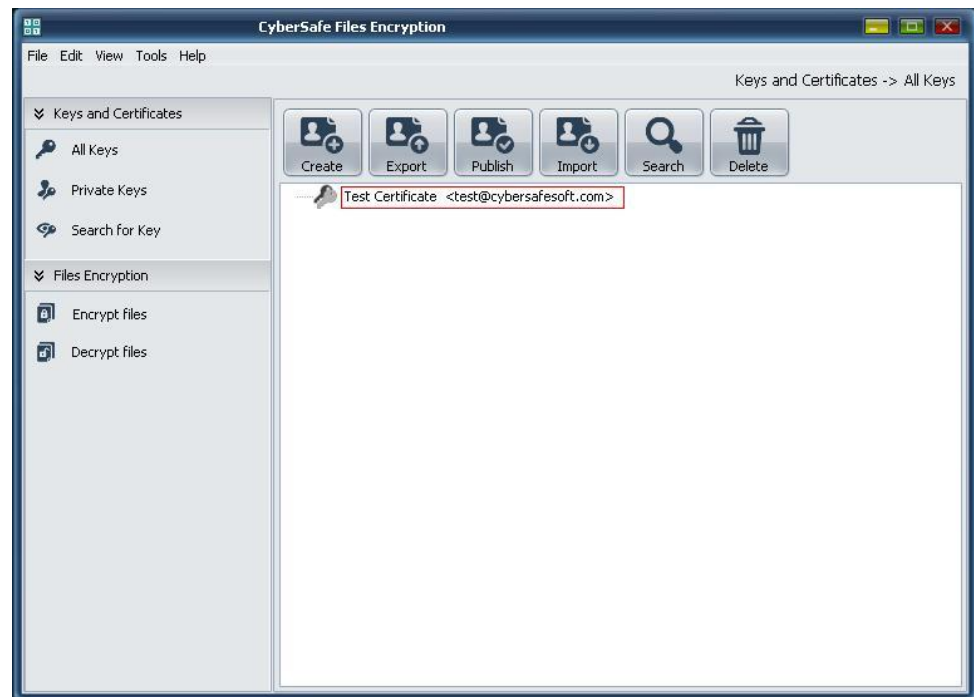
After that, your certificate keys will be generated, and a code will be sent to the email address you entered. You have to type the code into the appropriate field and then your Certificate will be published on the Server.



The 'The confirmation code' dialog box contains the following elements:

- Title: The confirmation code
- Text: Please check your email and copy \paste the confirmation code for the certificate publishing
- Text input field: 7DC1E
- Buttons: OK and Cancel.

After successful confirmation, Certificate creation is completed. The result can be seen in the Main window:



Creation of the Certificate is finished.

Uninstalling CyberSafe Top Secret

You can delete the Software from your local computer using the standard Windows function "Add or Remove Programs".

► **To uninstall CyberSafe Top Secret using the standard Windows function do the following:**

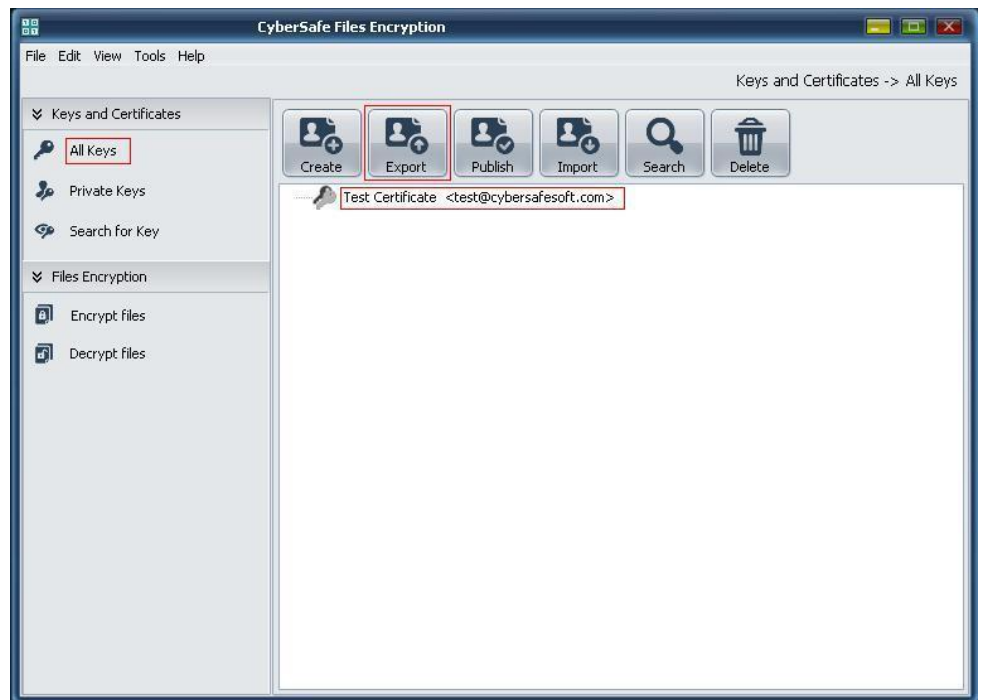
- 1 Go to **Start > Control Panel > Add or Remove Programs**.
- 2 In the list of installed programs find CyberSafe Top Secret and click **Remove**. In the system dialog box requesting confirmation to delete the program, click **Yes**.

Moving CyberSafe Top Secret from one computer to another

Moving CyberSafe Top Secret from one computer to another is not a complicated process. The main task is to correctly move a Key File, which you will have to export from the database of the program that is installed on the one PC and import to a said database on another PC.

► **To move CyberSafe Top Secret to another computer do following:**

- 1 Select **All Keys**, in the *Work Area* select your Certificate and in the *Options Menu* press **Export** button.
- 2 In the dialog box enter your password for this Certificate.



- 3 You should export the Key File with *.id extension, so in the pop-up window you must tick "ID file export":



- 4 Specify the folder to which you are exporting the selected files and click **Accept**. The selected files will be exported. Key file name the same as your e-mail and has the *.id extension. Copy this file to the new computer and, if necessary, remove CyberSafe Top Secret from the previous PC.

Note. After uninstalling CyberSafe Top Secret from your local computer, certificates and Key files you've created will not be deleted.

- 5 Install CyberSafe Top Secret on the new computer according to the instructions described above.
- 6 Select **All Keys** and in the *Options Menu* press the **Import** button. In Windows Explorer, locate the key file, specifying the location where you copied it, highlight it, and click Open. In the next window type your password. Next, the program will import the specified key file and create your Certificate. Moving CyberSafe Top Secret to another computer is finished.

4

CyberSafe Top Secret User Interface

This Section describes CyberSafe Top Secret's User Interface.

In this Section

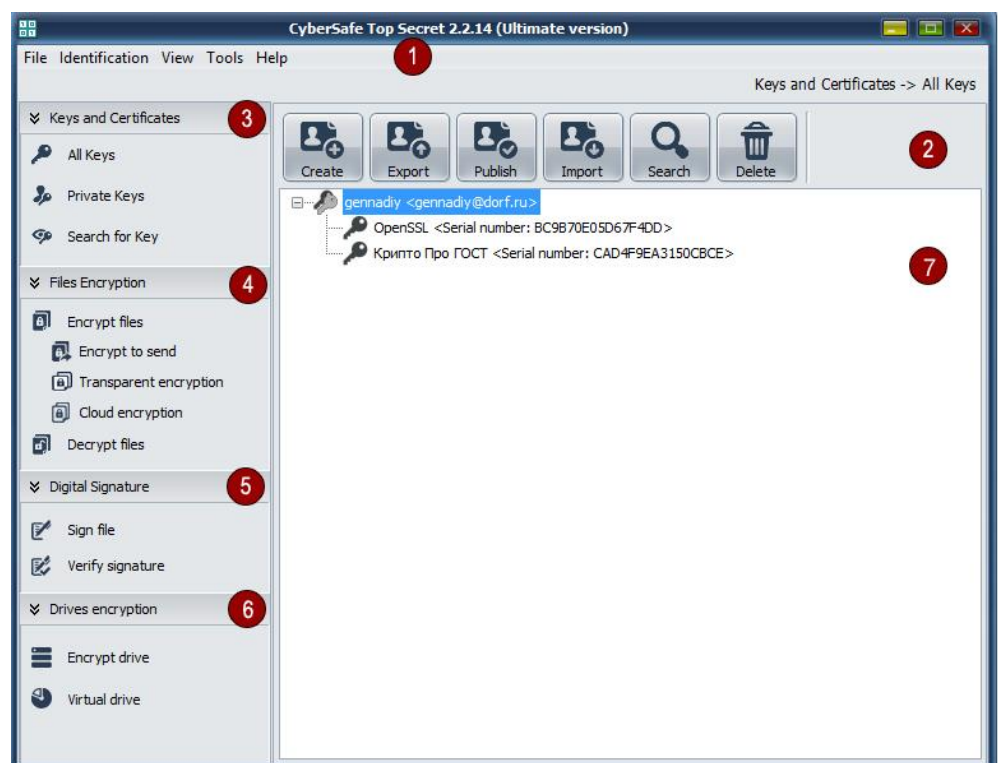
Access to the CyberSafe Top Secret's main functions..... 20

Access to the CyberSafe Top Secret's main functions

Access to the main functions of the program is possible through its Main Screen that you can open either double clicking on the program shortcut (*.exe file), or by clicking **Start > All programs > CyberSafe Top Secret 2**.

The Main Screen


The interface of the Main Screen contains all of its general functions.



Cyber Safe Top Secret Main Screen includes:

-
- | | |
|----------|---|
| 1 | Main Menu. Provides access to the basic functions of the program. Menu items contain further drop down tabs corresponding to the selected category. |
| <hr/> | |
| 2 | Options Menu. Contains the options Create, Export, Import, Publish, Search and Delete and others. All or some of them can be applied to files, folders, drives, and certificates. |
| <hr/> | |
| 3 | Keys and Certificates. The tabs "All keys", "My private key", and "Search for keys" are available. In search results you will receive information based on the name or email address of users. |
-

-
- | | |
|----------|--|
| 4 | Files Encryption. You can encrypt files and send them to the recipients or encrypt data on your local PC using Transparent Data Encryption feature. Also Cloud encryption feature is available. |
|----------|--|
-
- | | |
|----------|---|
| 5 | Digital Signature. Allows you to create your own digital signature as well as verify other users digital signatures. |
|----------|---|
-
- | | |
|----------|--|
| 6 | Drives Encryption. Allows you to encrypt hard drives and partitions of any size and to create encrypted virtual drives. |
|----------|--|
-
- | | |
|----------|---|
| 7 | CyberSafe Top Secret Work Area. Displays information and actions that can be undertaken in accordance with the selected menu item. |
|----------|---|
-

Boxes in the vertical menu numbered 3 and 4 are initially displayed in expanded form, but they can be minimized to help you work more efficiently. To minimize/maximize a box use the icon .

Items in the *Options Menu*, as well as the content of the *Working Area* change depending on which of the items in the boxes were selected.

For example, if the **Encrypt Files** function is selected, the *Work Area* will be ready to accept files and folders for encryption (you simply can drag and drop them there) and in the *Options Menu* items *Add Folder* and *Add File* will be active.

At the same time, if the item **All Keys** is selected in the *Work Area* a list with all available keys will be available and in the *Options Menu* items *Create*, *Import* and *Search* will be active.

5

Working with CyberSafe Top Secret Keys

By working with keys CyberSafe Top Secret means the creation and storage of Key pairs and Certificates, as well as importing and exporting Private Keys and Public Keys.

This section describes the types of keys, the process of creating the Key pair and Certificate, distributing your Public Key, and getting Public Keys from other users.



In this Section

Viewing Keys.....	26
Creating of a Key pair.....	26
Protecting your Private Key.....	27
Distributing a Public Key.....	29
Obtaining a Public Keys from other users..	31
Importing Keys and Certificates.....	32
Working with Key Servers.....	32

Viewing Keys

To view keys on your key ring open CyberSafe Top Secret and in the box **Keys and Certificates** select:

- **All Keys.** All keys on your key ring will be displayed.
- **Private Keys.** All your Private Keys will be displayed.
- **Search for Key.** Search for a key by the user's e-mail address.

Your Private keys have an icon  and contain your Public and Private Keys. Other users' keys are displayed on the key ring when the item **All keys** is selected have an icon  and contain only the Public Keys of those users.

Creating a Key pair

Perhaps you have already created a Key pair in the CyberSafe Top Secret independently after the first start of the program, or working with its previous versions, but if not, you need to do it now, because when using CyberSafe Top Secret virtually every everything you can do involves a Key pair.

Creating a Key pair in CyberSafe Top Secret takes place during Certificate creation. Generated keys are stored in the program's database and, if necessary, can be exported as individual files.

Warning. Do not keep creating new keys and certificates. Certificates used in CyberSafe Top Secret work like an electronic passport or driver's license; by them in large numbers, you will eventually confuse yourself and those users with whom you exchange encrypted messages. It is best to have one Certificate and one Key pair.

► To create a Key pair:

- 1 Make sure the item Keys and Certificates is selected.
- 2 In the Options menu select **Create**. Go through the procedure for creating a Certificate that is described in detail in the section "*Creating a Certificate and configuring the Software*".
Specify the **Key size** in a range from 1024 to 4096 bits. The larger the

key, the more secure it is, but the longer it will take to generate.

Specify the Validity of the **Key** in days. By default validity is 365 days. On the expiration of a validity period you will need to create a new Key pair.

- 3 Make sure that after you create a Certificate, it and the generated keys are displayed on the key ring in the *Work Area*. If you do not see the new Certificate in the list, ensure that the item *All keys* or *Private Keys* is selected in the box *Keys and Certificates*.

Warning. At this stage it is recommended to make a backup copy of your Private key and save it in a safe place. Your Private key is very important - if you used it for encryption of valuable data and then loose the Key it can be devastating. Read more about it in clause "*Protection of the Private key*".

Using Passwords

Encrypting a file and then being unable to decrypt it is a painful experience that will make you understand how important it is to choose a password that you can always remember.

Most applications require the creation of password from three to eight characters in length. It is a bad idea to use a word that can be found in the dictionary as your password. This is not recommended, since this password is vulnerable to attacks using password guessing from a database compiled from dictionaries. The approach here is that a program for breaking passwords goes through all words available in the dictionary and their combinations until it can determine your password. These programs can find arrays with passwords, even if they use terms that have been more or less changed from their original form in the dictionary.

To protect against this type of attack it is recommended to create a password which includes a combination of uppercase and lowercase letters, numbers, punctuation marks and spaces. This will ensure a strong password, but complicate its memorization.

Desire to resist such attacks leads you to create a strong password that is easy to forget. This can lead to loss of information, because you cannot use the password for decryption of your own protected files.

If the password was chosen impromptu likely will lead to it being completely forgotten. Try to use phrases that have already taken root in your long term memory. This should not be something that you recently repeated to someone, and it shouldn't be a famous quote, because your goal is to create a password that is difficult for attackers to guess.

Of course, if you will be so unreasonable as to write your password, and attach it to a monitor or put it into a drawer, then it will not matter how difficult a combination you chose.

For more information on this issue, see clause "*Working with passwords*".

Protection of Private Key

"CyberSoft" strongly recommends that you perform the following steps immediately after you create your own certificate and key pair.

Warning. Not using the following guidelines may lead to a loss of valuable data in the future.

- Create a backup of your Private Key in another safe place as long as your primary copy has not damaged or lost yet. For more information on this issue see the paragraph "*Creating backup copies of Keys*"
- Look at the selected password again to make sure you do not forget it. If you are unsure about this, change your password RIGHT NOW to one you will not forget.

Your Private Key is very important because if the data was encrypted using the

sender's Public Key, decryption is possible only with the recipient's Private Key. This is also true for your password. If you lose your password or Private Key you will not be able to decrypt data encrypted using the sender's Public Key as well as data encrypted for your personal use.

Once data is encrypted, nobody, not even the "CyberSoft" Company will be able to decrypt it without your Private Key and password. This means that if you encrypt important information for personal use and then either forget your password or lose your Private Key, the encrypted data will be completely inaccessible and unusable.

Measures used to protect your Private Key

In addition to creating backup copies of your keys, you must also be very careful with respect to where to store your Private Key. Despite the fact that your private key is protected by a password, known only to you, there is a possibility that someone will find out your password and then will be able to use your Private Key to decrypt your emails or forge your digital signature.

In order to prevent attackers who might intercept your password and use your Private Key you should store it only your personal computer. If your computer is connected to a network, make sure that your files are not included in a general backup where other users can access your Private Key.

Given the fact that when you connect to the network your computer becomes more vulnerable, if you work with valuable information, your Private Key can be stored on a floppy disk that can be used as an old-fashioned key whenever the need arises to read or sign the secret information.

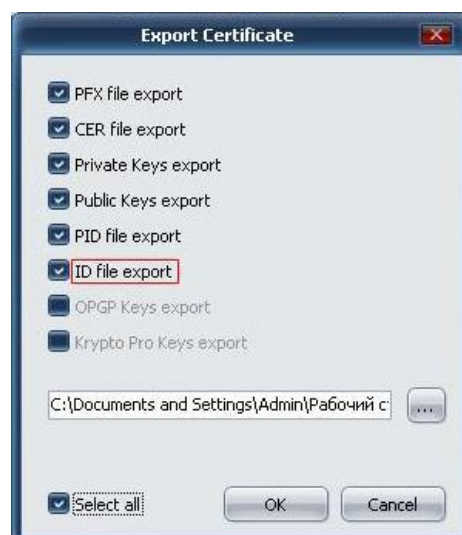
Note. Changing the password on your Private Key does not automatically change the password on any copies of the key (for example, created during backup). If you suspect your Private Key and Certificate could be compromised, "CyberSoft" recommends that you remove all previous copies of the key and then create the Certificate again.

Creating backup copies of a Private Key

Your Private and Public Keys are stored in the database of the program in an *.id file. To create backup copies of them to store in another location on your hard drive or on a USB stick the Key should be exported from the database.

► To create backup copies of your keys:

- 1** In the box *Keys and Certificates* select **Private Keys**.
- 2** In the *Work Area* in the list of your Private Keys highlight the key you want and press **Export**. In the dialog box enter the password for this key (Certificate).
- 3** In the dialog box tick **ID file export** and specify a location on your computer or removable media where your keys will be exported, then click **OK**:



- 4 The exported file containing your Private and Public keys has the *.id extension. If the directory to export is different from the place where you want to store your backup copy of the keys, locate the exported file with this extension and copy it to a safe place. This can be a CD or DVD, or another PC or USB-flash drive that you keep in a safe place. Please note that **you must not share this file with other users, as it contains your Private Key.**

What if a Private Key is lost?

If your Private Key is lost and you don't have a backup copy, you'll never be able to decrypt information encrypted by this key for your personal use as well as information encrypted with the appropriate Public Key by other users. This information is useless and cannot be recovered.

Distribution of Public Key

Once your Key pair is created, you need to distribute copies of your Public key to those users with whom you intend to exchange encrypted messages. You make your Public Key available to those who will send you encrypted information and verify your digital signature and you need the Public keys of the users you plan to send encrypted messages.

You can distribute the Public Key in several ways:

- Publish your key on the server (see paragraph "*Publishing on the server*"). By and large, this method is the basic and it may be sufficiently.
- Add the Public Key in e-mail message (see paragraph "*Adding a Public Key in e-mail message*").
- Export the Private Key to a file (see paragraph "*Exporting Private Key to a file*").

Publishing on the server

The best way to make your Public Key available to others it is put it on a public server, which is a large database of keys. Thus, users will be able to send you encrypted messages without having to specifically request a copy of your Public Key. Also, you don't need to store large amounts of Public Keys that you rarely use.

There are many key servers around the world including CyberSafe's Server on which you can make your public key available to all.

Before you start working with some of the key servers and place a copy of your Public Key there, please note the following points:

- Is this the key you intend to use? Other users will try to contact you and encrypt information using this Public Key. Therefore, we strongly recommend that you publish only Public Keys that are really intended for other users on keyservers.
- Will you remember the password for this key? Or, if you do not intend to use it, perhaps it would be better not to publish the key on the server?
- Some key servers, unlike CyberSafe's Server, adhere to a policy that if a Public Key is published on the server it must remain there in future because of which you may have difficulty with removing a Public Key. On some servers, there are functions for automatic key distribution to other servers, so even if you can remove your key from the server, it can still appear on it later.

As a rule, users publish their Public Keys on the CyberSafe Server during the creation of a Certificate and Key pair. If you have already done it, you don't need to publish your Public Key again. In most cases, there is no need to additionally publish your Public Key to other key servers.

Take into account the fact that other servers cannot authenticate published Public Keys, so if you download a Public Key from this server you may be required to spend more effort to contact the owner of this Public Key and compare the unique electronic fingerprint of this key.

► To publish the Public Key on the server manually

- 1** Open CyberSafe Top Secret.
- 2** Make sure in the box Keys and Certificates the item **My Private keys** is selected.
- 3** In the *Work Area* select the key you want to publish and in the *Options Menu* press the **Publish** button.
- 4** A confirmation code will be sent to your email. Copy and paste it in the dialog box and click **Accept**. After this your Public Key will be published on the server.

Once your Public Key is published on the server it becomes available for users who want to send you encrypted data or to verify your digital signature. Even if you do not specify your Public Key to the users directly, they can obtain a copy by using the search function and your email address.

Many users include the web address of their Public Key at the end of their e-mail messages. In most cases, the recipient of this e-mail just clicks on the address to obtain a copy of the Public Key on the server. Some even place a unique fingerprint of the Public Key on their business cards for easier verification.

Adding a Public Key into e-mail message

Another good way to distribute your public key to other users is to add it to an e-mail.

When sending your Public Key, don't forget to sign the email with its digital signature. Thus, the recipient can verify your signature and make sure that no one has tampered with the information at this stage. Of course, if your key has not been checked by any trusted guarantor, the recipient can be sure that it is your digital signature only by its unique fingerprint checking with you personally.

Exporting a Public Key to a file

Another way to share a Public Key with others is exporting it in a ***.pid** file, after which you should make this file available to the person you want to exchange encrypted information with.

Obtaining Public Keys from other users

Besides the fact that you need to distribute your Public Key, you also need to obtain Public Keys from other users to send encrypted messages to them and verify their digital signatures.

You can do it in several ways:

- Find the public key manually on the server;
- Add a Public Key attached to an email to your key ring;
- Get a Public Key from an exported file.

Public keys are just blocks of text, so they can easily be added to your key ring by importing them from a file or by copying them from an email.

Downloading Public Keys from a Key Server

If the person you want to send an encrypted message is an experienced user of CyberSafe Top Secret, they probably already put their Public Key on the CyberSafe Server or on another server. This is convenient because it always has the most recent version of the key. In addition, it eliminates the need to store lots of public keys on your key ring.

There are numerous public key servers, such the CyberSafe Server, where you can find the other users' keys. If the user hasn't specified the web address where their Public Key is stored, you can access any keyserver and search for the key using their name or email address. This may or many not work however, because not all public key servers regularly update information about keys stored on other servers.

► To obtain Public Key from a keyserver

- 1 Open CyberSafe Top Secret and in the **Keys and Certificates** box select the option **Search for Key**.
- 2 In the dialog box type the user's e-mail address and click **Accept**.
- 3 If user's key is already on the CyberSafe server it will automatically be added to your key ring.
- 4 To check whether the key has been added to your key ring select **All Keys**. The key should be displayed in the list of the keys.

Importing Keys and Certificates

In CyberSafe Top Secret you can import certificates that were created previously. For this you will need a ***.id** file containing your Public and Private Keys. Once imported, you can use a Certificate to encrypt files and to create digital signatures.

You can also import other users' Public Keys to your key ring if a ***.pid** file is available to you. This file contains the user's Public Key (for example, he copied this file onto your computer or uploaded it to somewhere you can download it from). After you import the Public Key, it will be added to your key ring and you will be able to encrypt files for this user.

► To import a Certificate

Note. Before you import a Certificate that contains a Private Key, make sure you know the password for this Certificate.

- 1 Open CyberSafe Top Secret and select the **Keys and Certificates** box.
- 2 In the *Options Menu* select the **Import** button.
- 3 In the system window specify the path to a ***.id** or ***.pid** file and click **Open**.
- 4 The Certificate will be imported and the key will be displayed on your key ring. To check whether the key was imported select **All Keys** and find it in the list of the keys.

Working with Key Servers

You can use the CyberSafe Server or any other public server available on the Internet to store keys.

- **The CyberSafe Server.** CyberSafe provides a free public key server for our user's convenience, providing quick and easy access to the Public Keys and Certificates of other users of the program. It uses new technology that verifies the key associated with a given email address. So the server does not store unused keys or multiple keys assigned to the same email address. Also, the server has none problems associated with older generation servers.
By using the CyberSafe Server you greatly increase your chance to find a particular user's public key.
- **Other key servers.** In most cases, other key servers are also open publicly-accessible servers that store users' Public Keys. Nevertheless, you may have access (for example, through a company in which you work, or for any other reason) to private servers.

6

Email protection

This section explains how to use CyberSafe Top Secret to protect your e-mails when using e-mail clients.

In this Section

E-mail encryption using CyberSafe Top Secret	34
Working with Microsoft Outlook	35
Working with Mozilla Thunderbird	41
Working with The Bat!	45

E-mail encryption using CyberSafe Top Secret

To protect email correspondence we use encryption. CyberSafe Top Secret provides you the ability to protect your e-mails when using any email client (Thunderbird, Microsoft Outlook, The Bat! and others).

Before you begin exchanging encrypted messages with other users, you need to exchange Certificates containing Public Keys with them. This can be done by sending each other digitally signed messages and then adding the user Certificate to your list of contacts.

Once you and other user have certificates with each other, sending encrypted emails will be no different than sending normal emails. It will also encrypt any file attached to messages.

Exporting Certificates to X.509 and PKCS#12 format

To work with mail clients you need a PKCS#12 Certificate (a file with the *.PFX extension) and X.509 Certificate (a file with the *.CER extension). Some mail clients require the Certificate to be placed in Windows storage, others import them into their own storage.

► To export a Certificate in a *.PFX file

- 1 Open CyberSafe Top Secret and in the *Keys and Certificates* box select **All Keys**. All keys on your key ring will be displayed.
- 2 Highlight the necessary Certificate from the list and in the *Options Menu* click **Export**.
- 3 In the dialog box enter your password for this Certificate.
- 4 In the next dialog box tick **PFX file export** and **CER file export**. Specify a location on your computer where the Certificate will be exported to. Click **OK**:



- 6 The Certificates are exported to the specified place with a *. pfx and *. cer extensions.

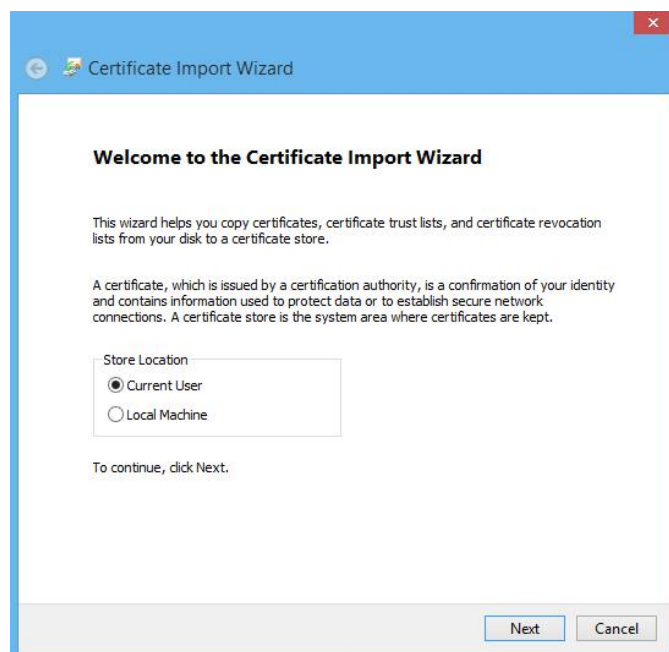
Consider that together with these two certificates *CyberSafe Root Certificate* was exported which we will use to configure encryption in some mail clients.

Working with Microsoft Outlook

Using a .PFX Certificate, you can configure encryption and digital signatures in Microsoft Outlook.

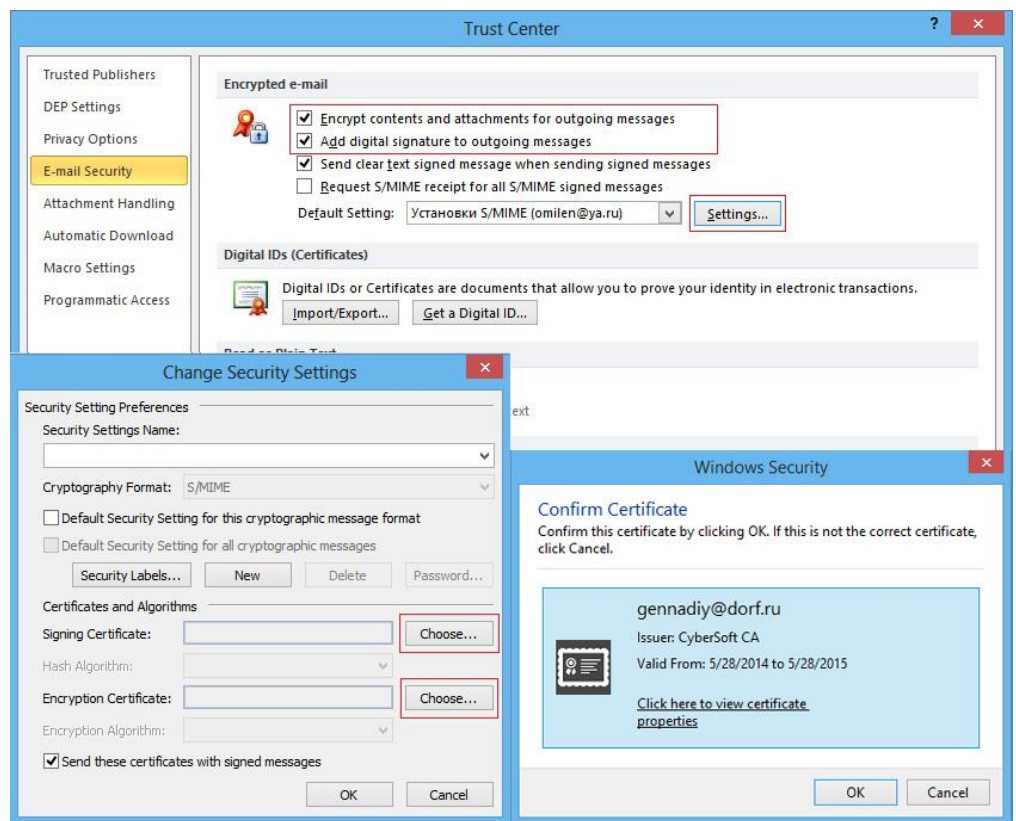
► To configure encryption

- 1 Install PKSC#7 Certificate to the Windows Storage. To do this double clicking the .pfx file and follow Certificate Import Wizard instructions. This certificate contains your Private Key, so you will have to enter your password.



- 2 Open Microsoft Outlook and select the appropriate Certificate (you don't have to import the Certificate in this case because when CyberSafe Top Secret is running all certificates are already in Windows storage).

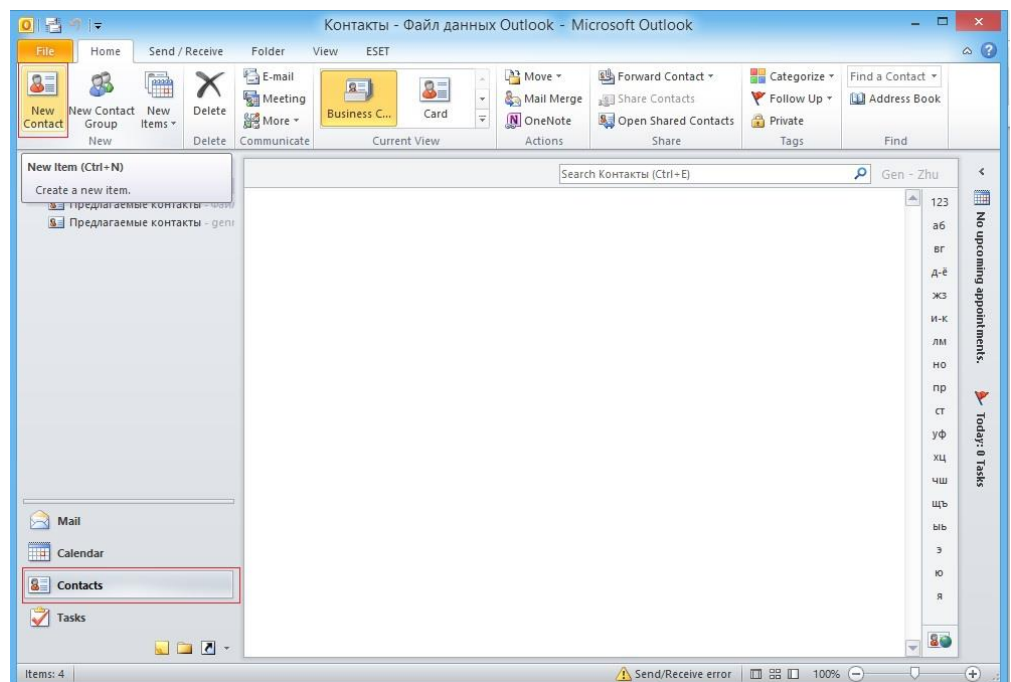
To do this, go to: **File > Options > Trust Center > Trust Center Settings > Email Security > Settings > Choose ...**



box *Encrypted e-mail* tick **Encrypt contents and attachments for outgoing messages** and **Add digital signature to outgoing messages**.

3 Next, you need to test the encryption on yourself.

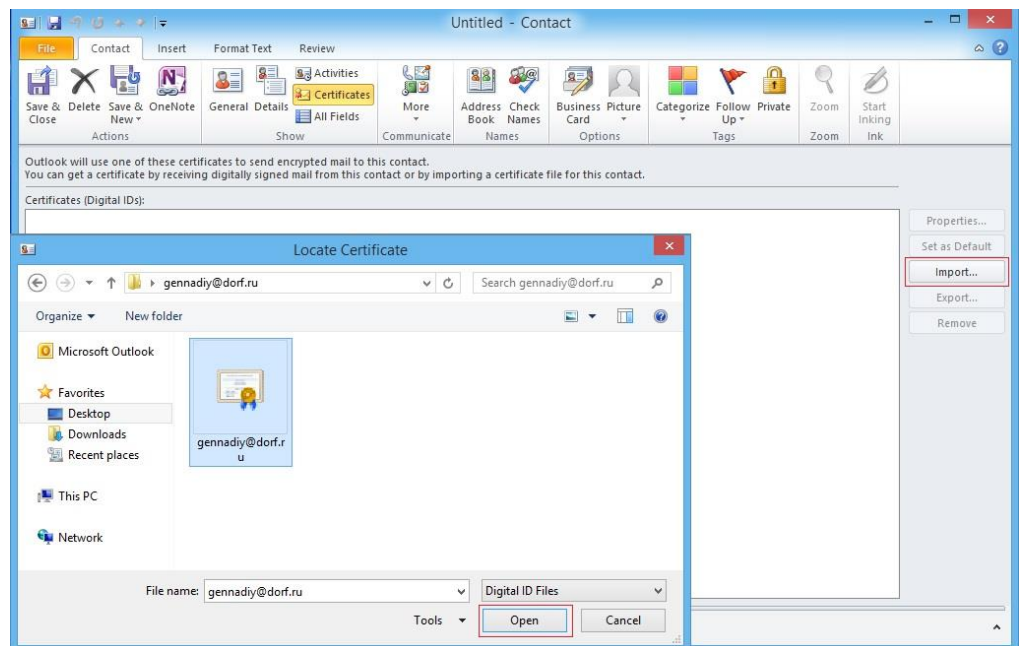
- Create a new contact. Go to: **Home > Contacts > New contact**.



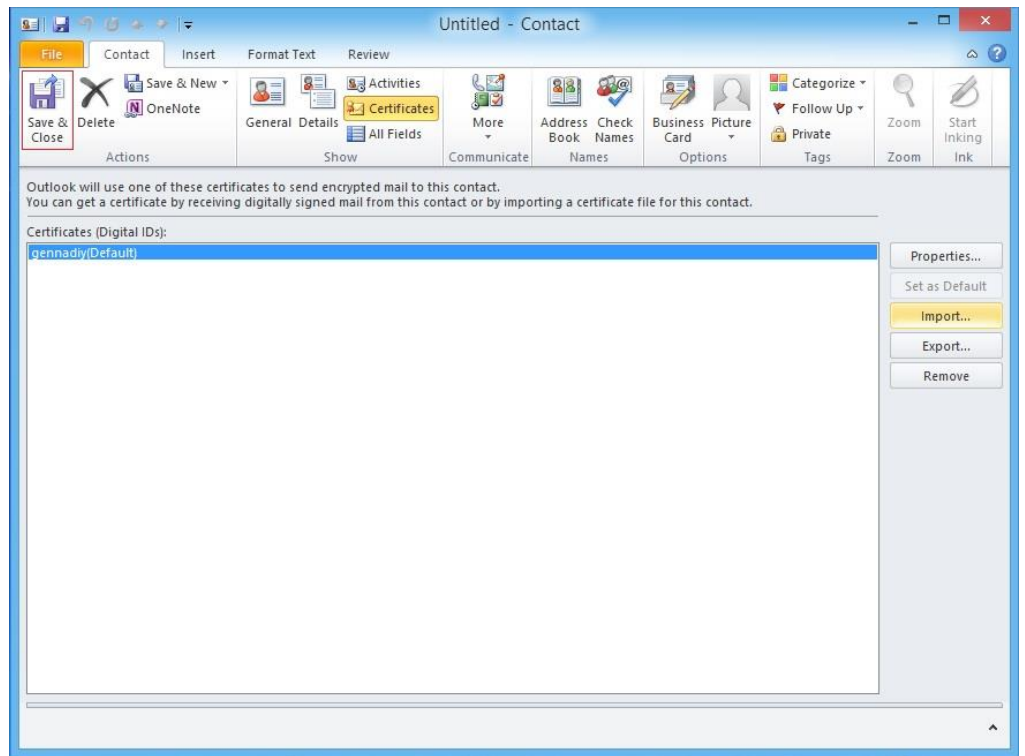
- The window for creating a new contact will be opened. Fill in the required fields.



- Next, you need to import the certificate for this contact (in this case yours). To do this on the **Contact** tab choose **Certificates** and press **Import**. In the system window **Locate Certificate** specify a path to a ***.cer** file and press **Open**. (You can export this file from CyberSafe Top Secret the same way as a *.pfx file (see the paragraph "Exporting Certificates in .PFX format").

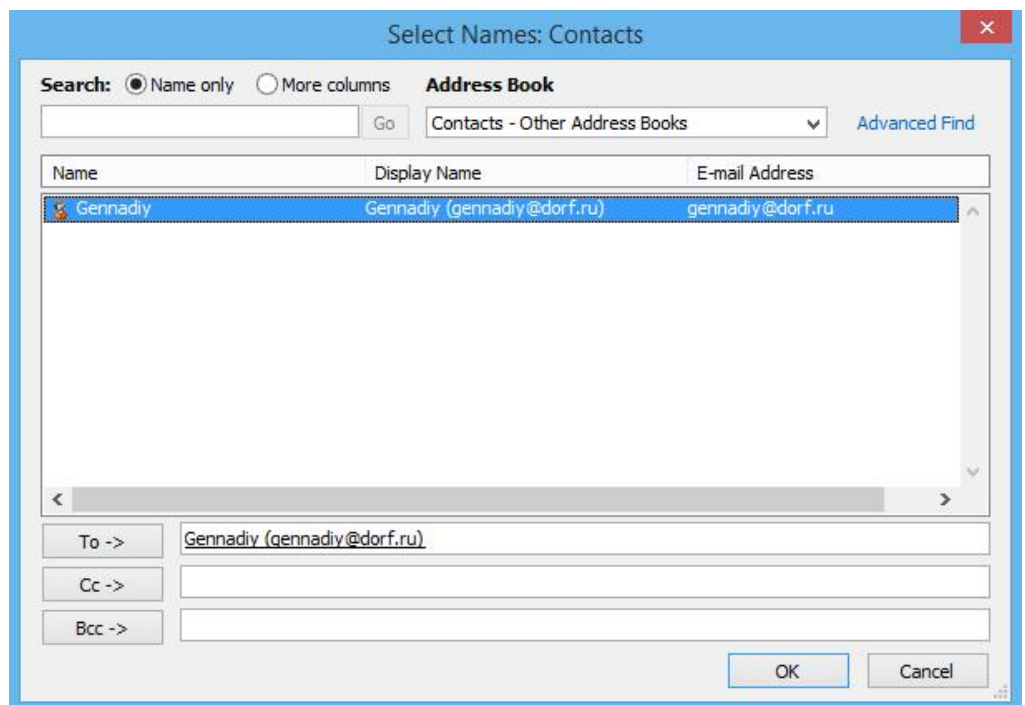


- In the dialog box that asks you whether you want to add the certificate click **Yes**. In the window *Certificates (Digital ID's)*, a new certificate will be displayed. Click **Save & Close**.

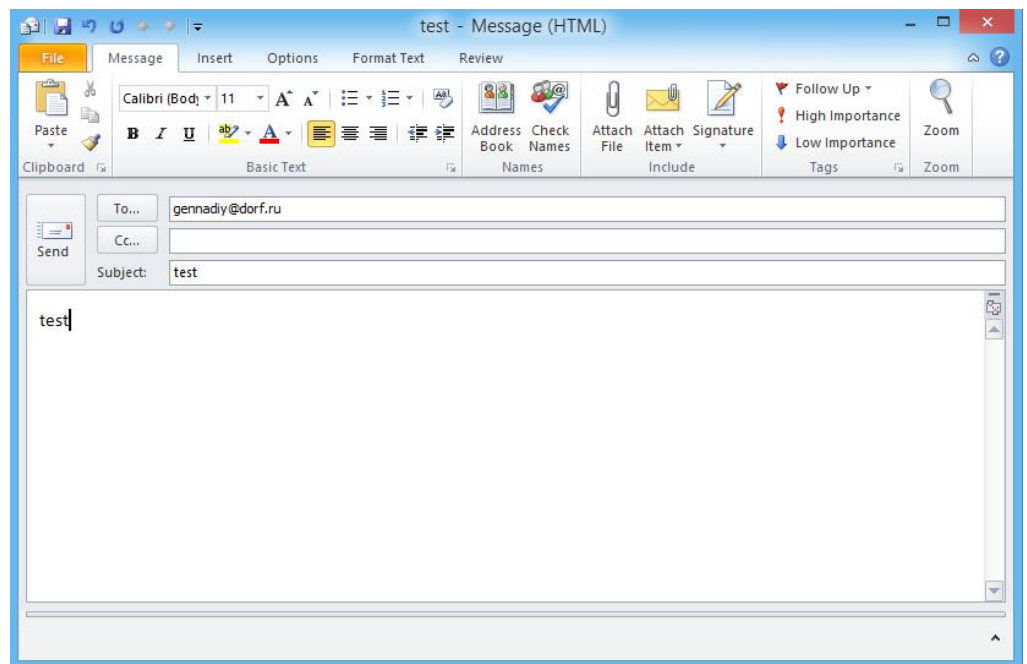


The Certificate has been added to the contacts.

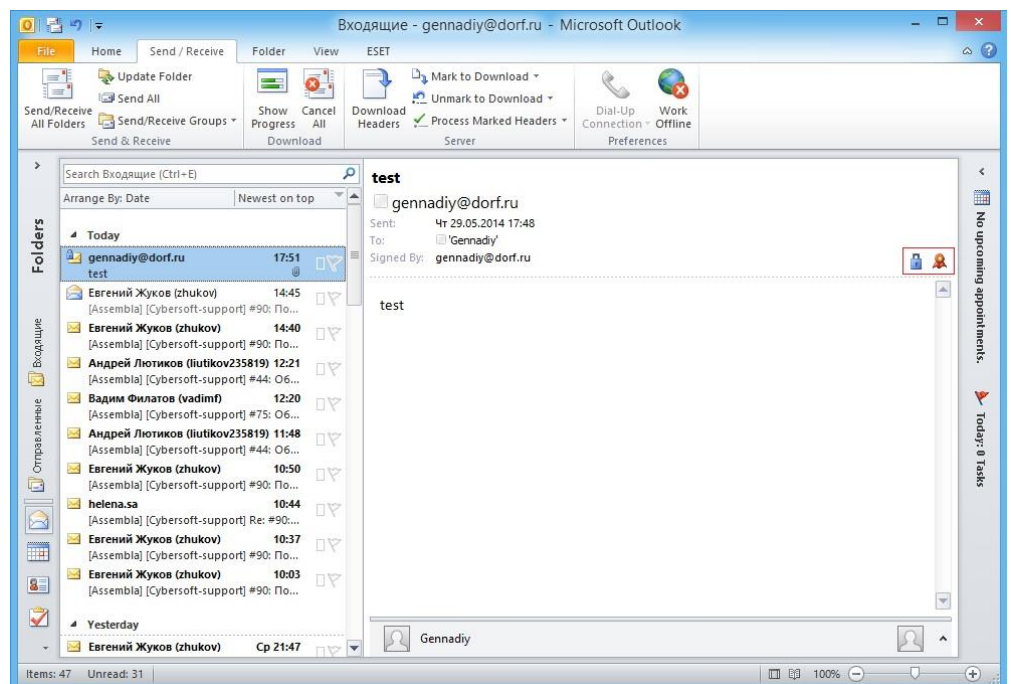
- Send an encrypted message to yourself. To do this go to: **Mail > New E-mail**. In the **To** field select the contact you created by highlighting it from the Address Book list and click **OK**:



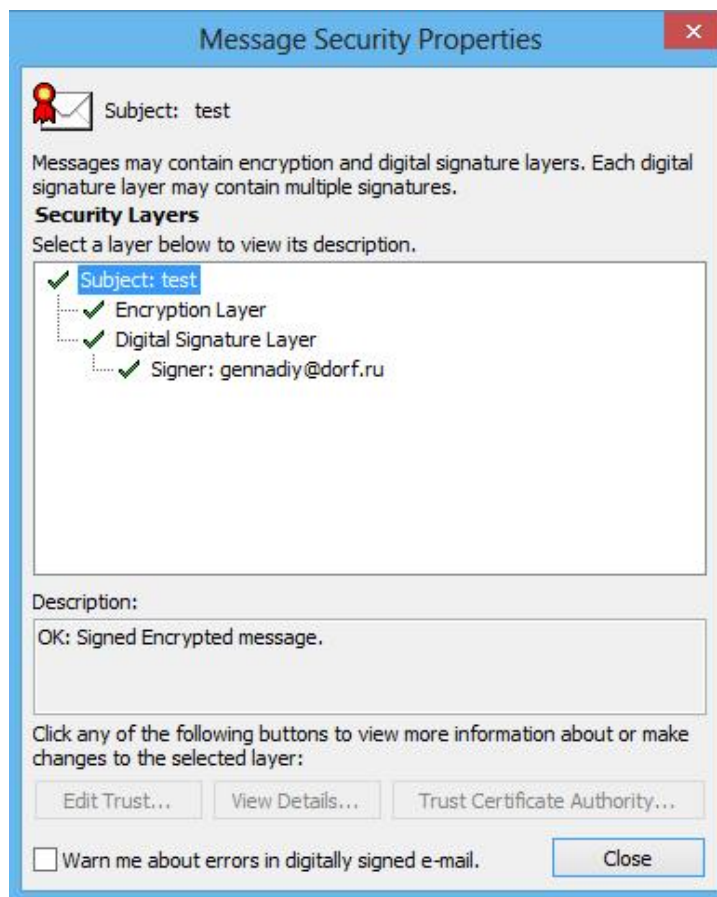
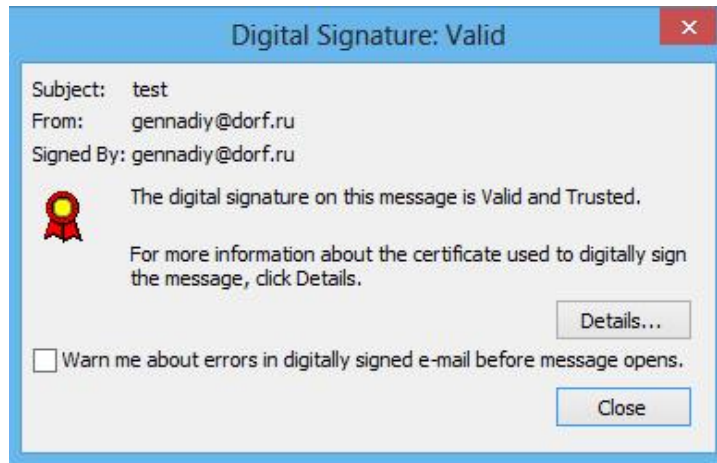
- Fill in the *Subject*: field, enter the message and press **Send**:



- Go to **Home > Inbox**. In the list of incoming messages a message you sent will appear. It is encrypted, as evidenced by the blue icon with a padlock in the upper left corner. Click on it with the mouse to automatically decrypt and open it in a nearby window.
If you do not see the email you sent in your inbox, go to the **Send/Receive**, and then click **Update Folder**.



- To view Message Security Properties or information about the digital signature click the appropriate icons in the field of general information about the message:



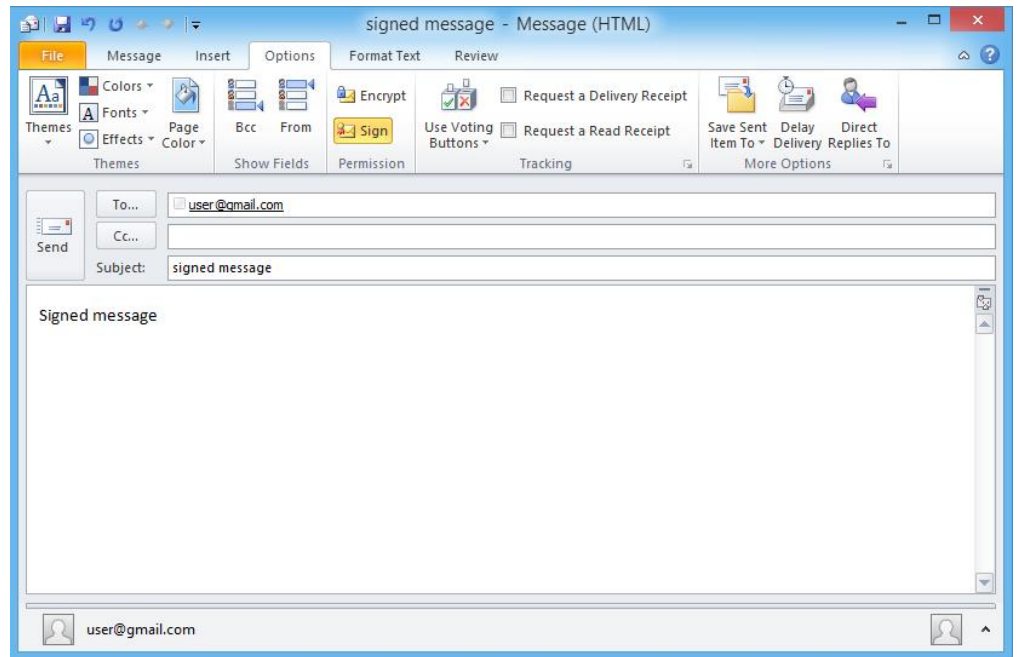
- If the user's Certificate is valid and the digital signature is authentic, you will see a green checkmark in the message safety properties window.

Encryption is configured.

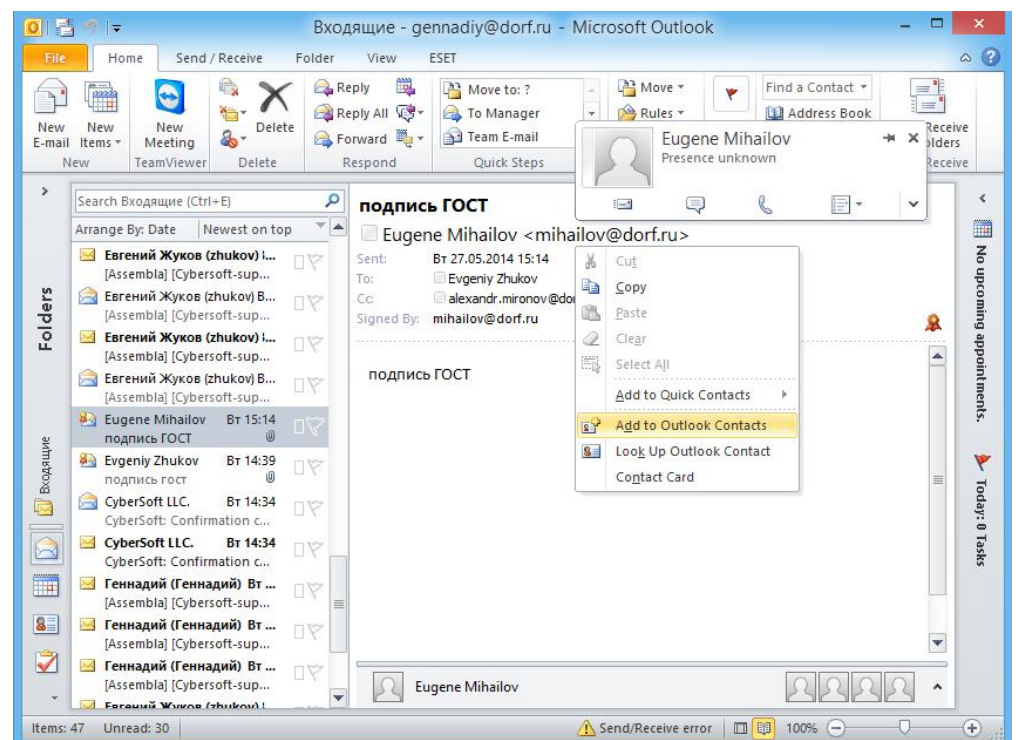
- 4 Similarly, send your Certificate (a *.pid file) in a digitally signed message to other users and get their signed Certificates. When users are added to the Address Book you can send their encrypted messages.

Please, note that if the user to whom you send an encrypted message hasn't received your Public Key yet, they will not be able to decrypt it. So first you have to send them an unencrypted e-mail containing your Public Key and signed with your digital signature.

To disable encryption go to the **Options** tab and disable **Encrypt**, leaving **Sign** enabled:



To add a recipient to your *Address Book* you need to right click on the sender's name and select **Add to Outlook Contacts**:



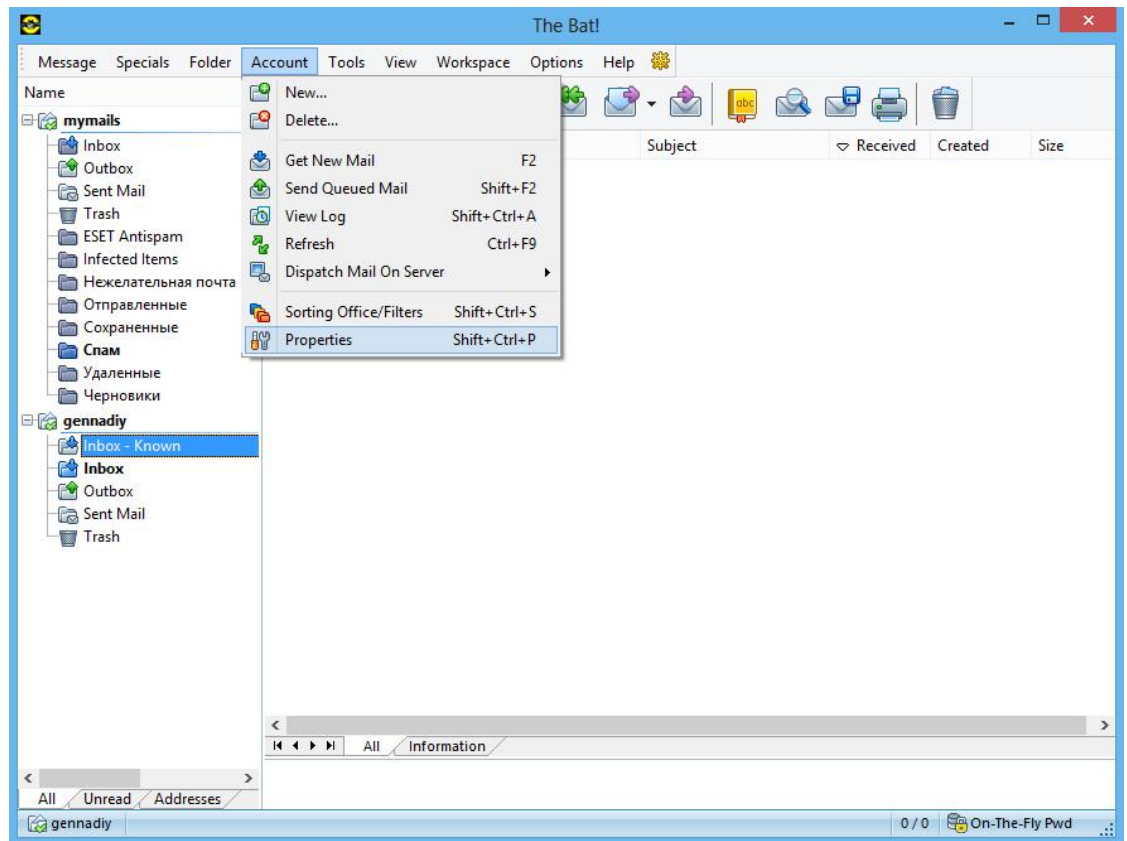
Microsoft Outlook checks the certificate in the following scenario. If the publisher of the certificate is listed as trusted the certificate is considered trusted. In this case CyberSafe Certificate Authority was automatically added to the trusted list during the first run of the program.

Note. CyberSafe Top Secret allows you to create only a single certificate per e-mail address. This means that if the user has not personally added any invalid certificates, all messages with green tick opposite the item *Digital Signature Layer* that he receives are trustable.

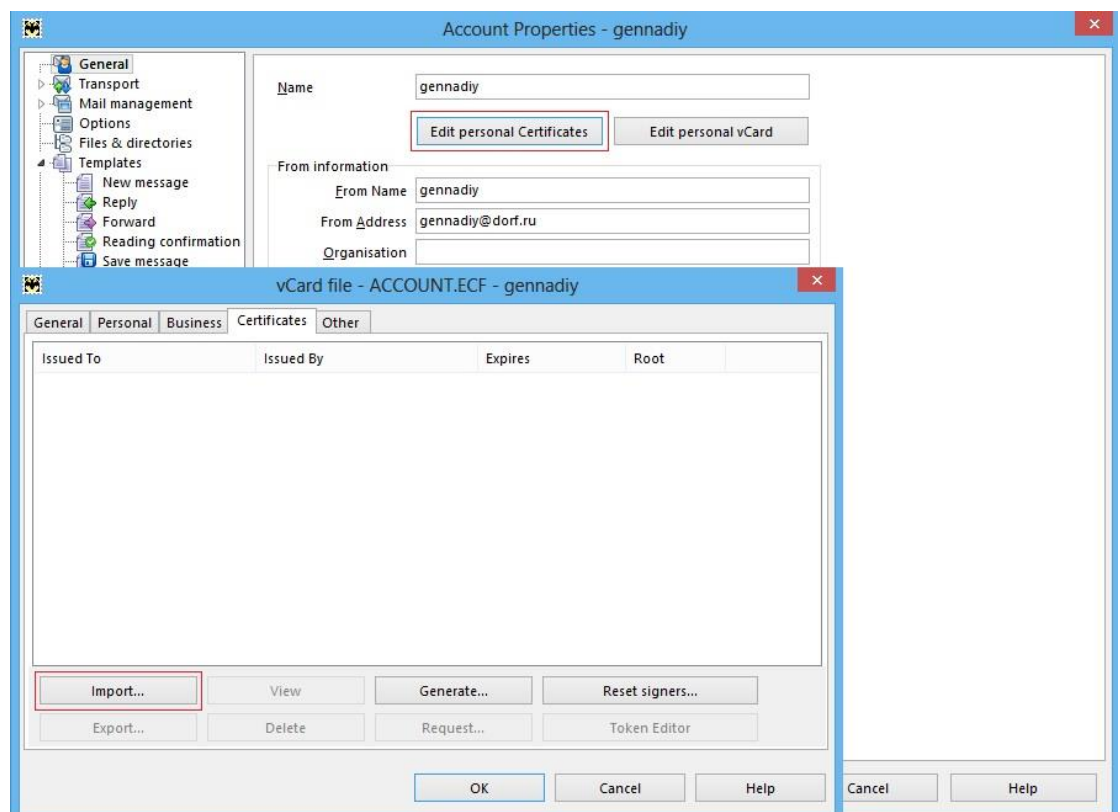
Working with The Bat!

► To configure encryption

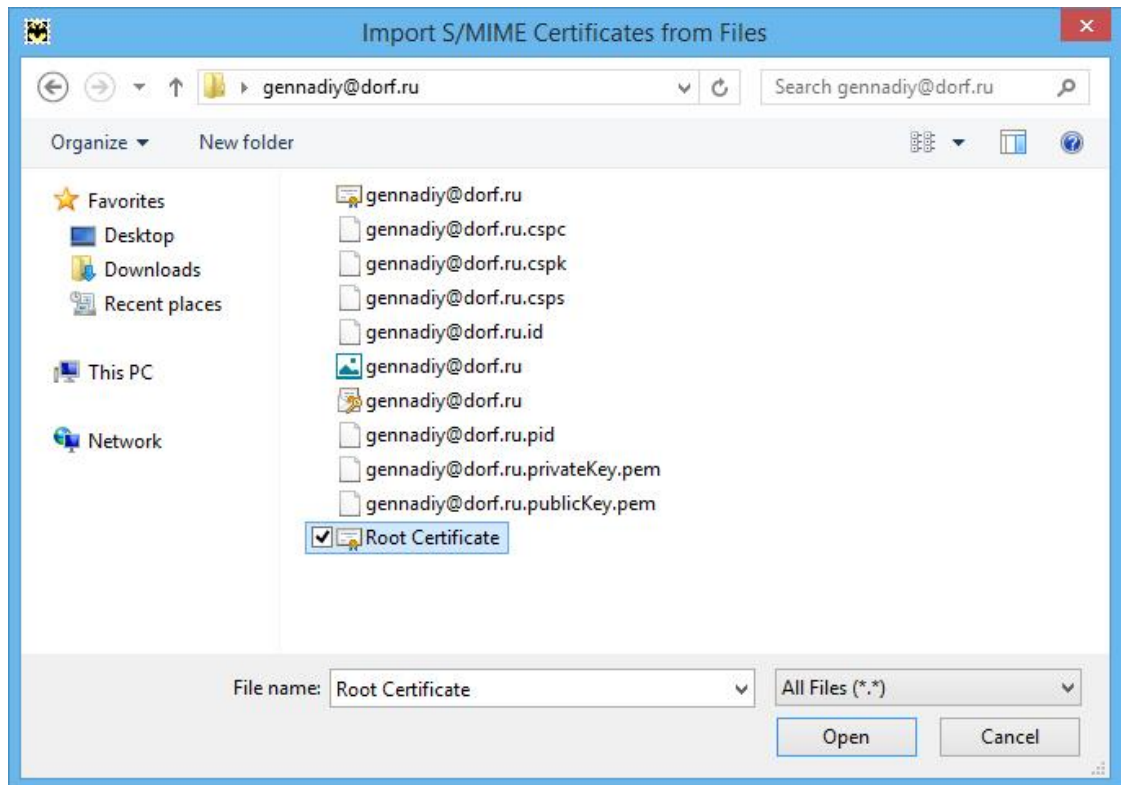
1 Open The Bat! and go to **Account > Properties:**



2 In the *Account Properties* window select **General > Certificates > Edit Personal Certificates > Import:**



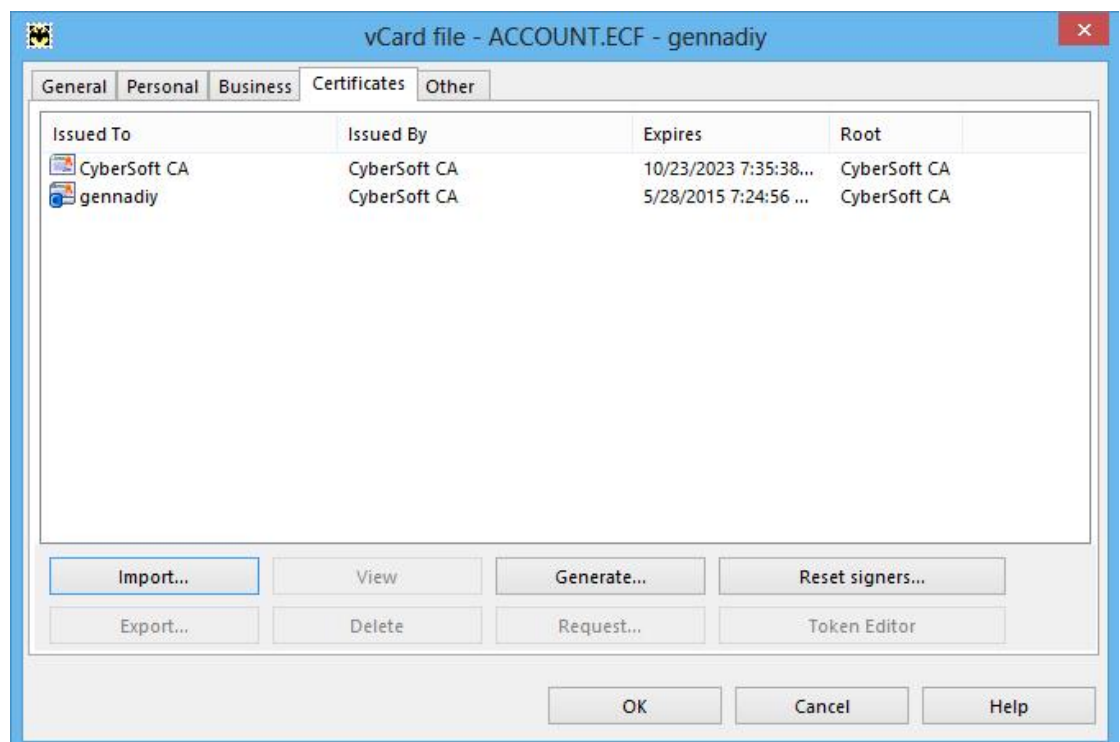
- 3 In the next system window specify the path to the *Root Certificate* (about exporting this file see paragraph “*Export the Certificate to X.509 and PKSC#12 format*”).



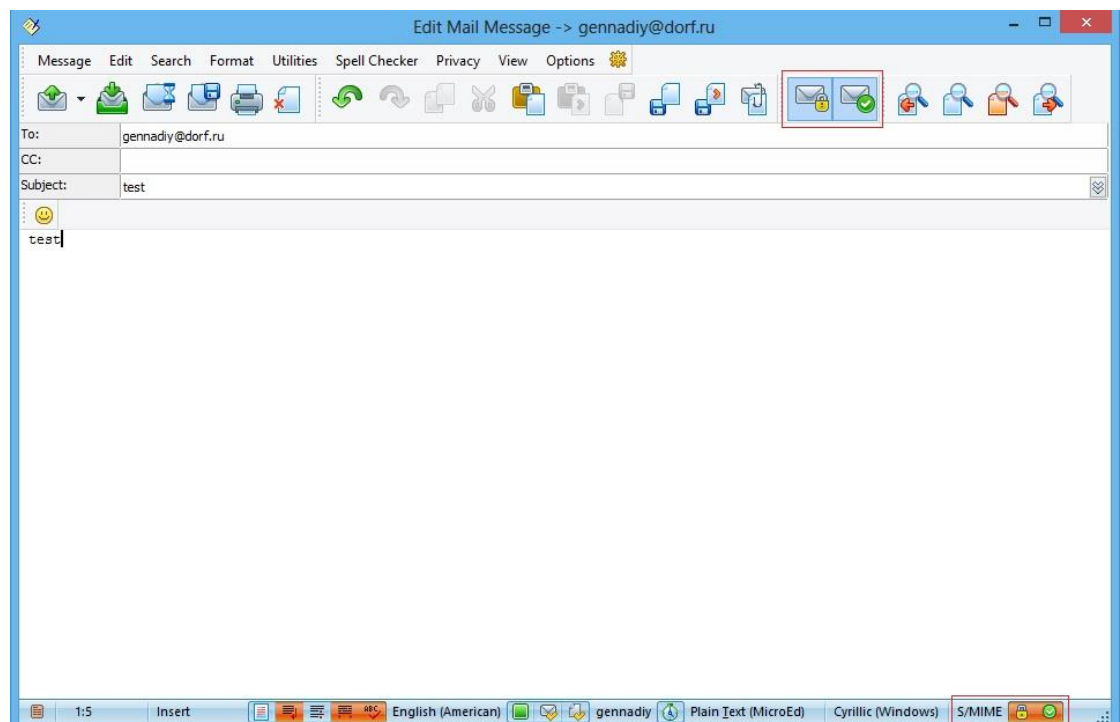
Click **Open**.

In the same way import your PKSC#12 Certificate (the file with the *.PFX extension). You will have to enter your password to this Certificate.

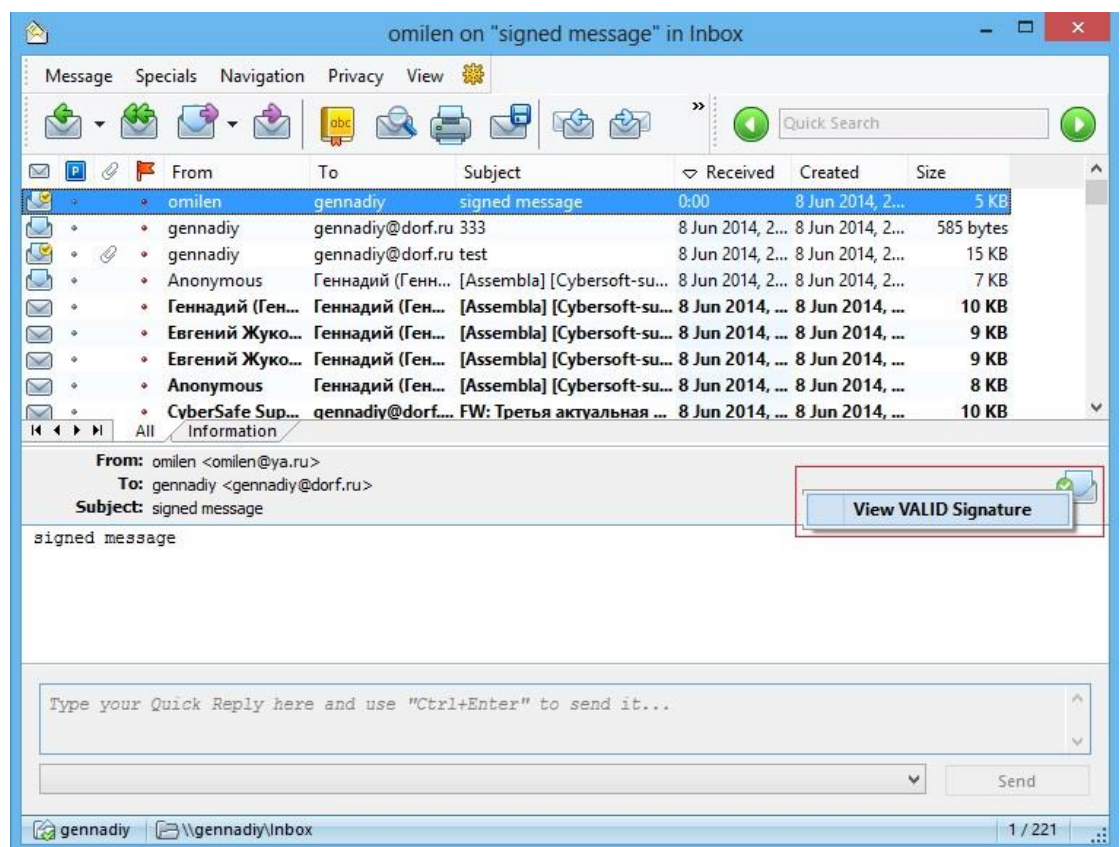
- 4 The Certificates will be imported and displayed in the list of certificates:

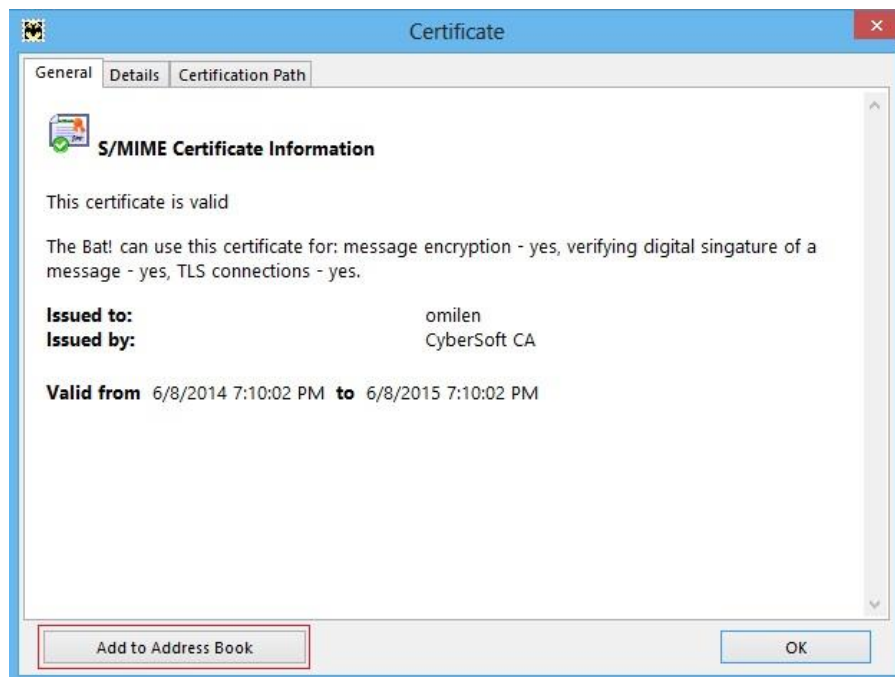


- 5 Create a new message. To do this go to **Message > New**. Fill in *To* and *Subject* fields, type the message. To encrypt and sign the message, select the appropriate buttons with the padlock and green tick on the envelopes. Send your letter.

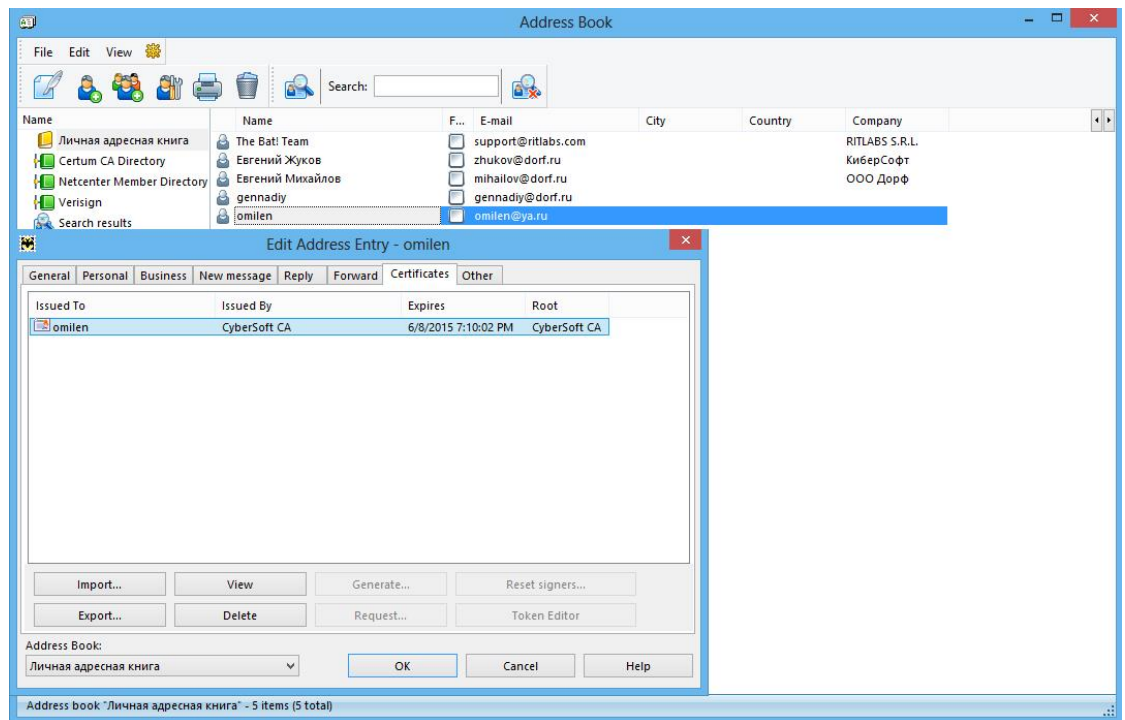


- 6 Please, note that if you haven't got recipient's Public Key yet, you will not be able to encrypt your message. So first you have to get his Public Key (file with the *.cer extension) from his signed message. To do this select **View Valid Signature > View > Add to Address Book**:



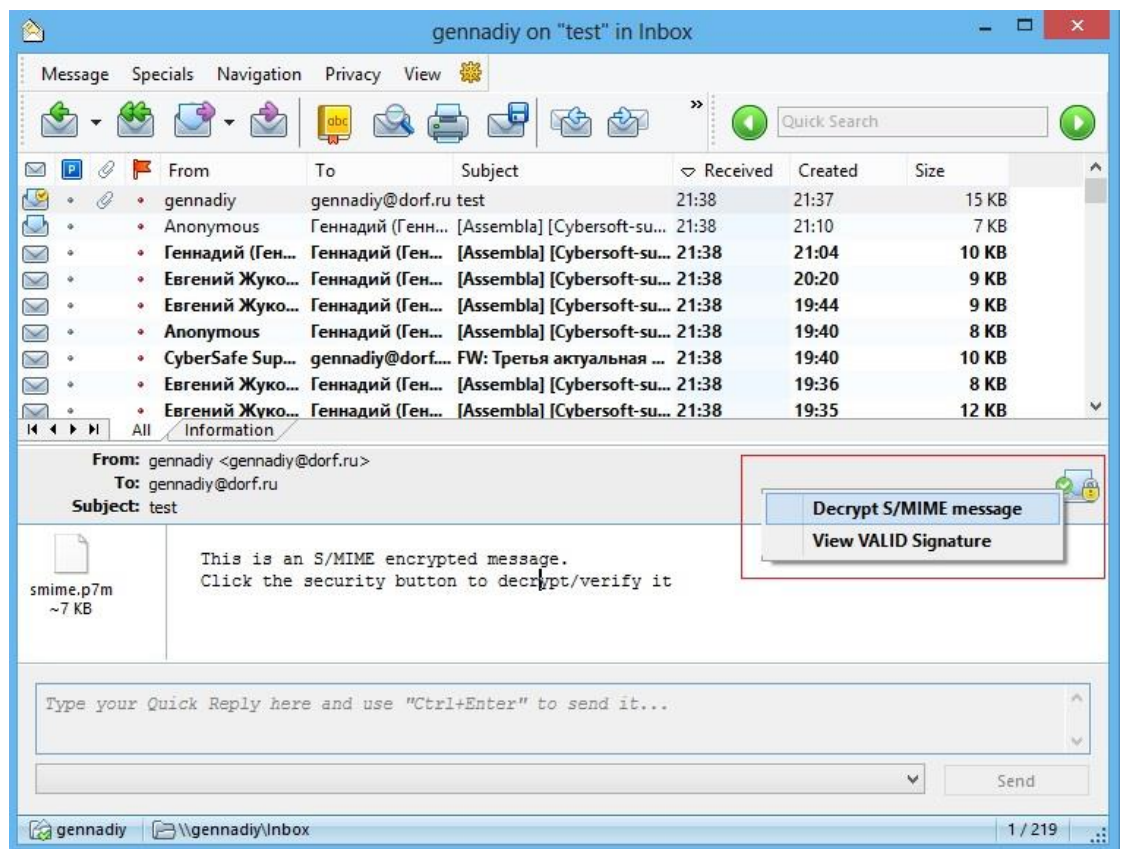


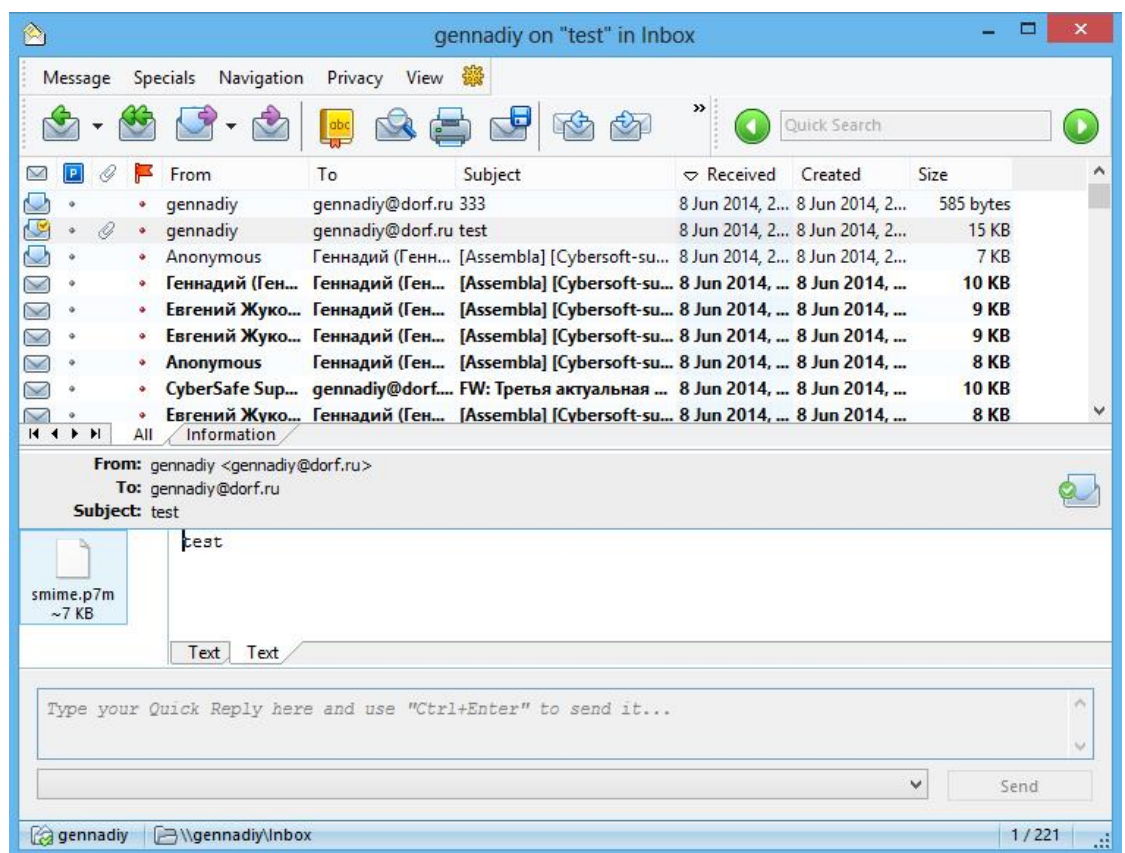
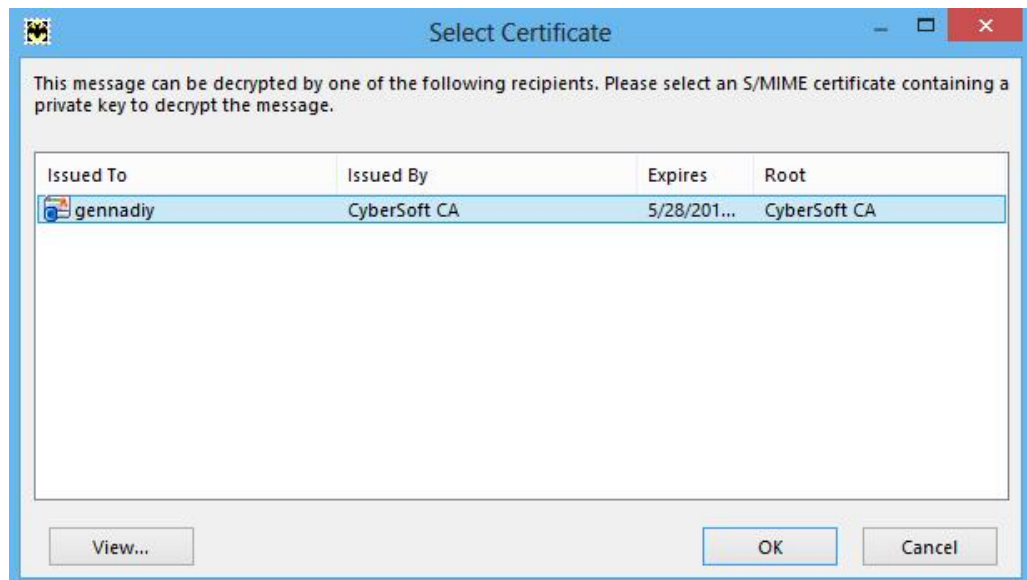
User's contact will be added to your *Address Book* and his Certificate with Public Key will be attached to this contact:



As soon as recipient receive your Public Key you will be able to exchange encrypted messages.

- 7 To decrypt an encrypted message select **Decrypt S/MIME message**, in the next window select your Certificate and enter your password for your Private Key. The message will be decrypted:



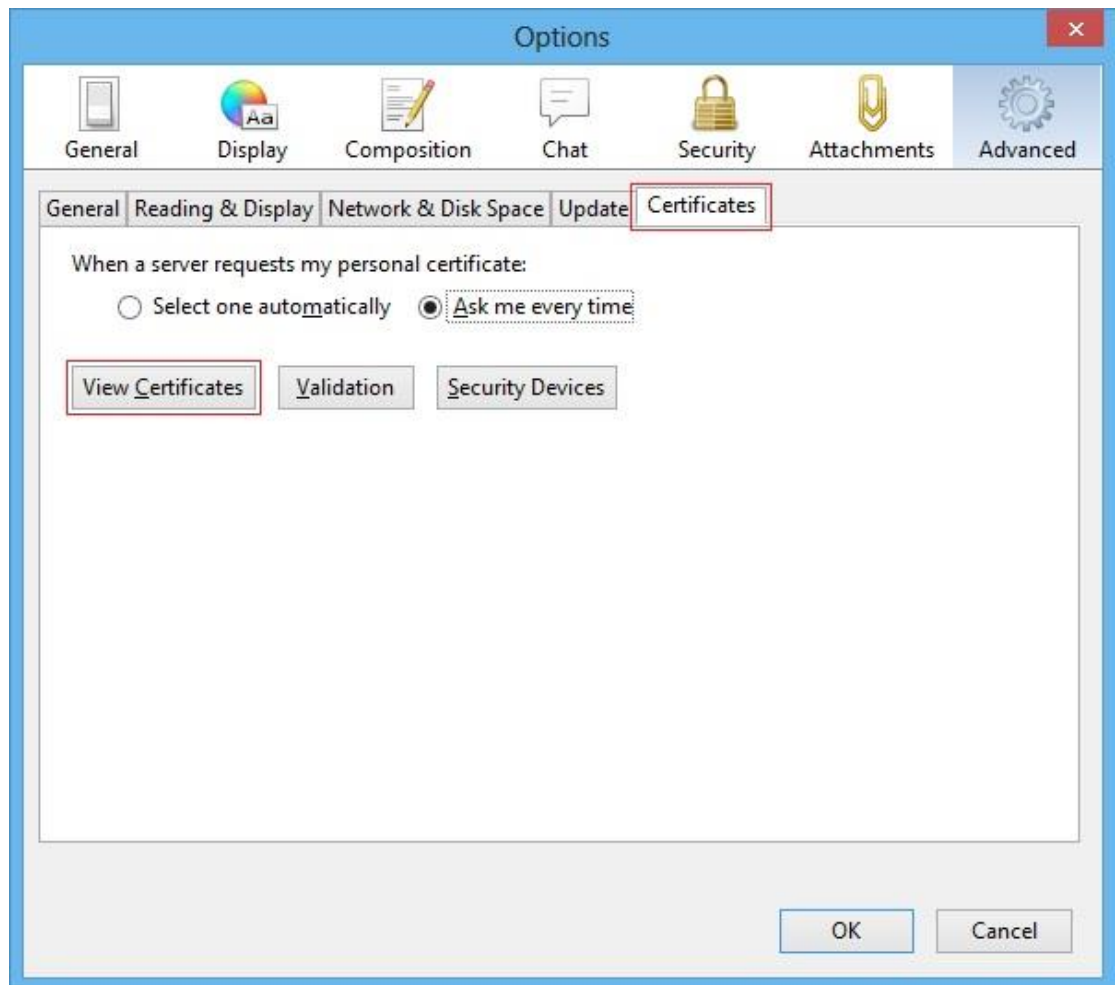


Encryption feature in The Bat! is configured.

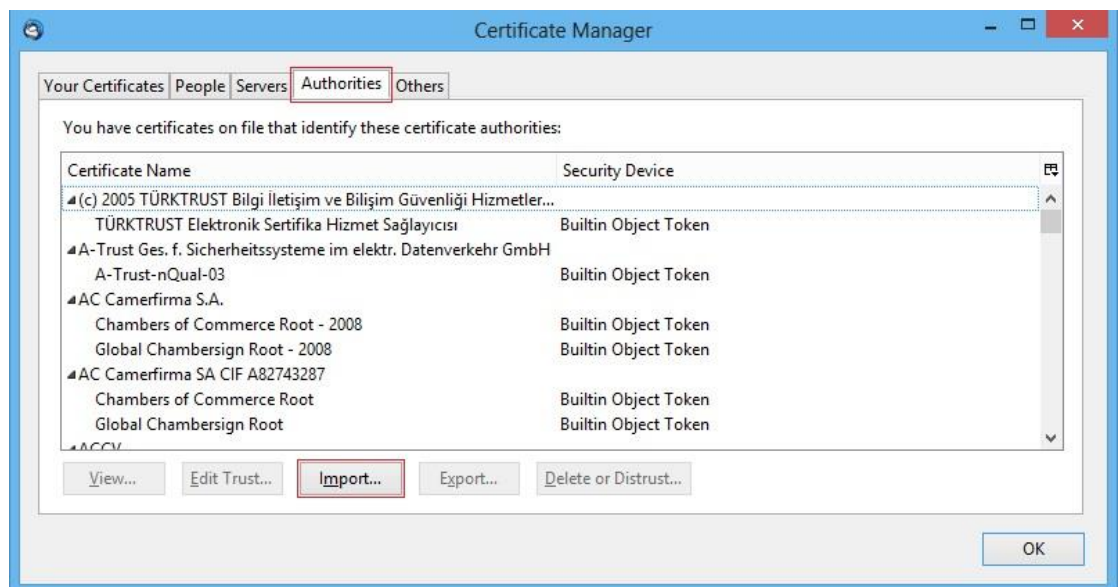
Working with Mozilla Thunderbird

► To configure encryption

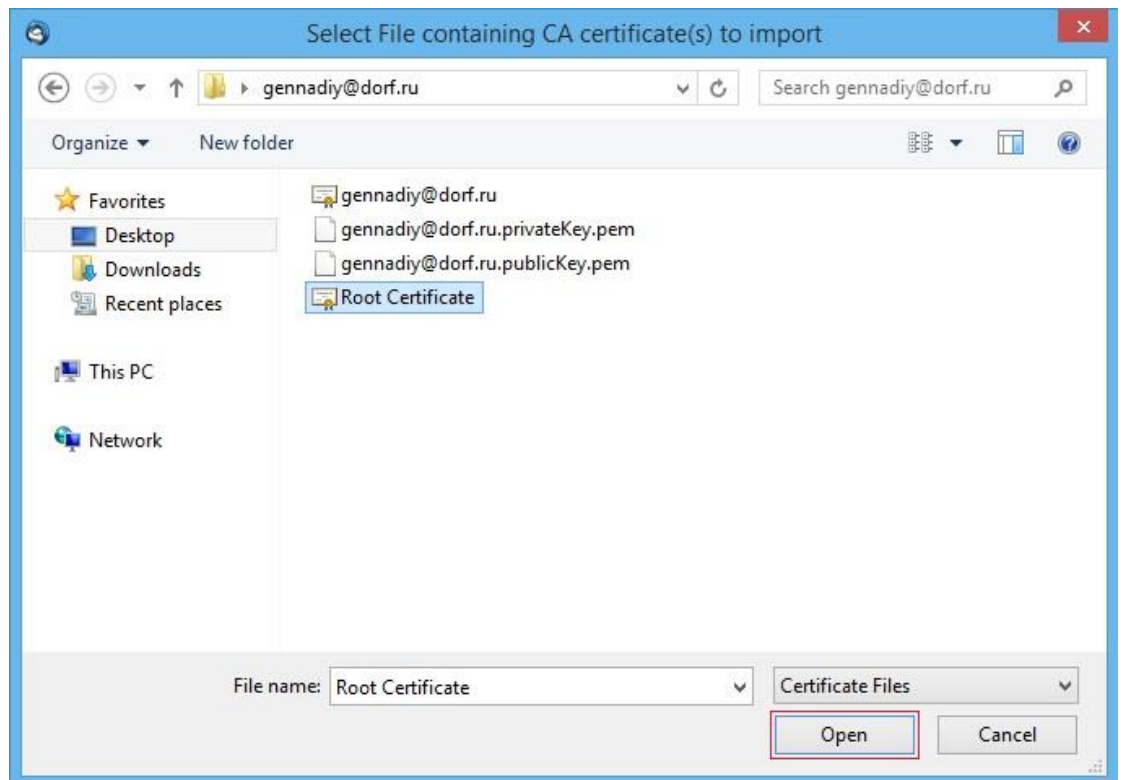
- 1 Open Thunderbird, go to **Address Book > Tools > Options > Advanced > Certificates > View Certificates:**



- 2 The window *Certificate Manager* will be opened. Choose **Authorities > Import:**



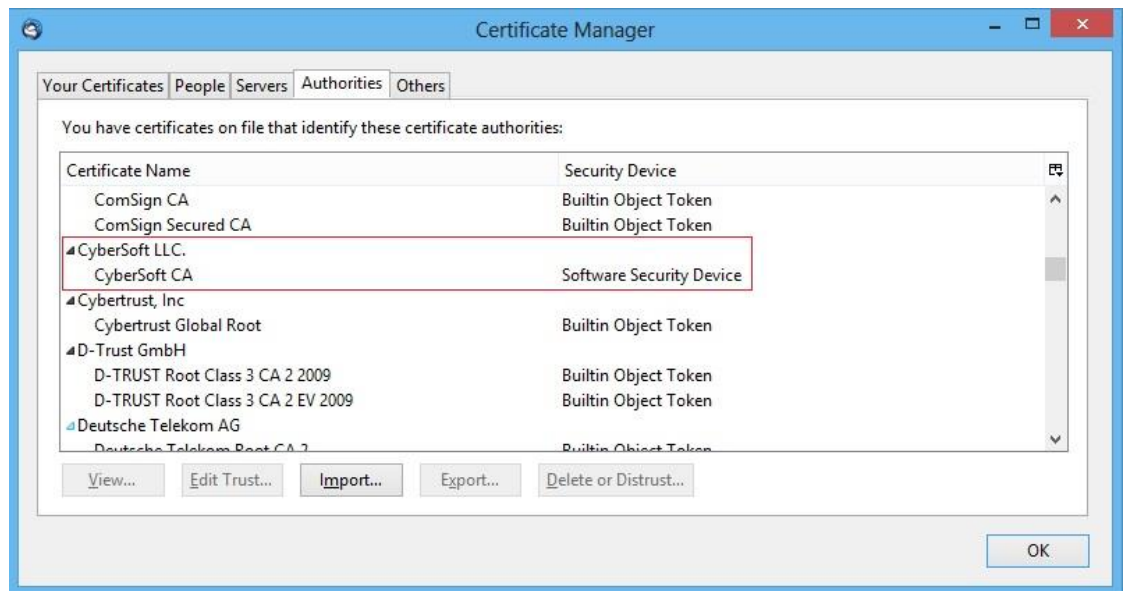
In the next window specify the path to CyberSafe Root Certificate, highlight it and click **Open** (about exporting this file see paragraph “*Exporting Certificates to X.509 and PKCS#12 format*”).



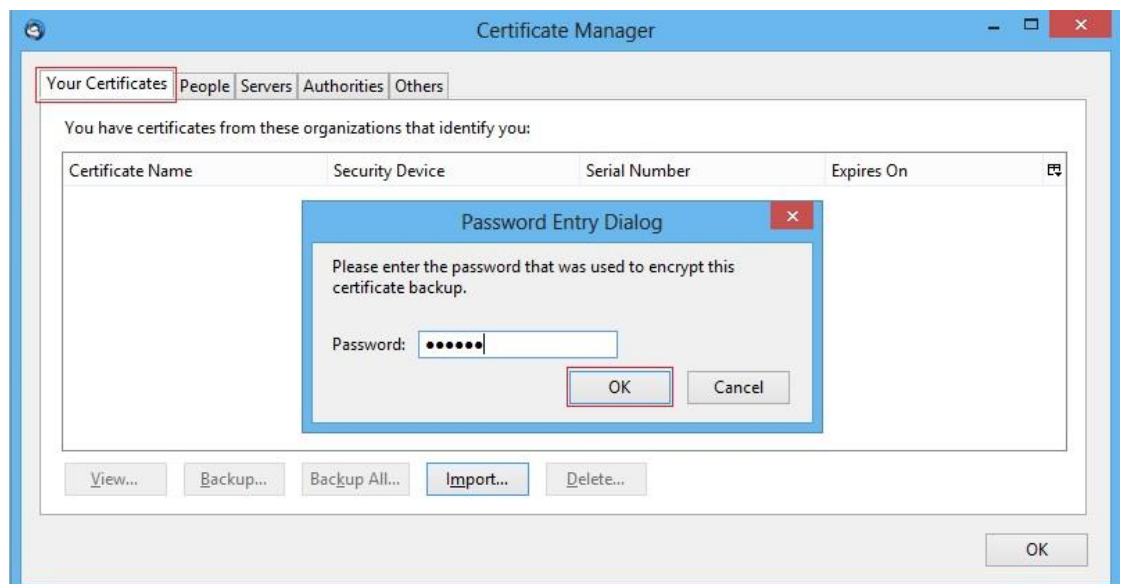
In the next window tick all checkboxes and click **OK**:



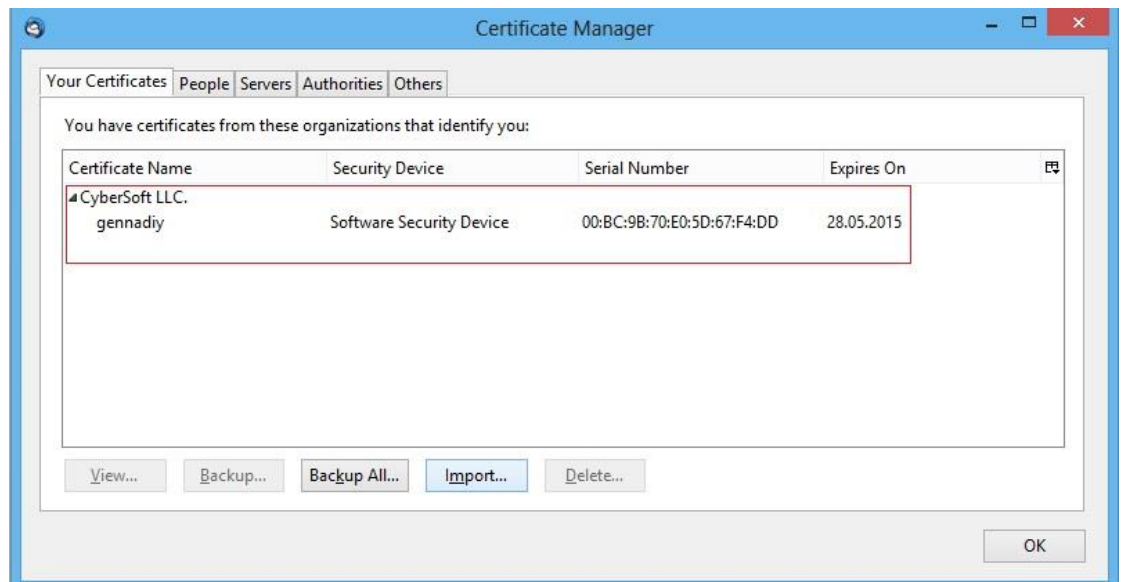
CyberSafe Root Certificate will be imported to the Thunderbird storage:



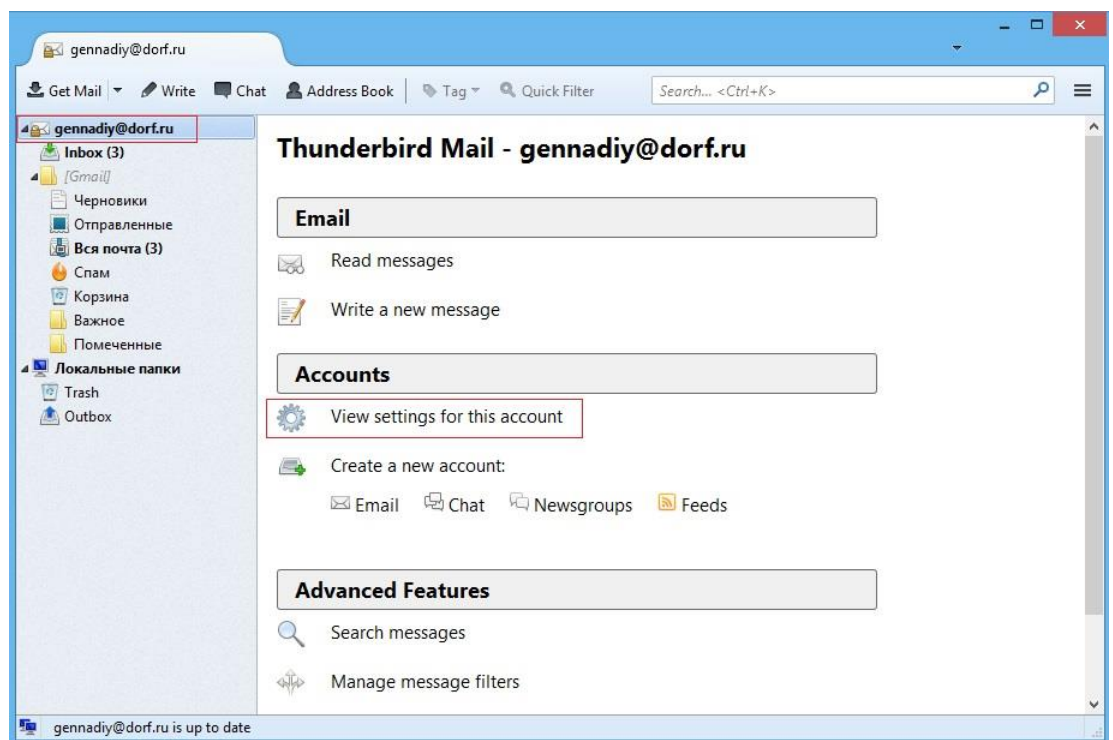
- 3 In the *Certificate Manager* window go to **Your Certificates** > **Import** specify the path to the file with the *. **pfx** extension (about exporting this file see paragraph “*Exporting Certificates to X.509 and PKCS#12 format*”), highlight it and click **Open**. In the next window Enter your password:



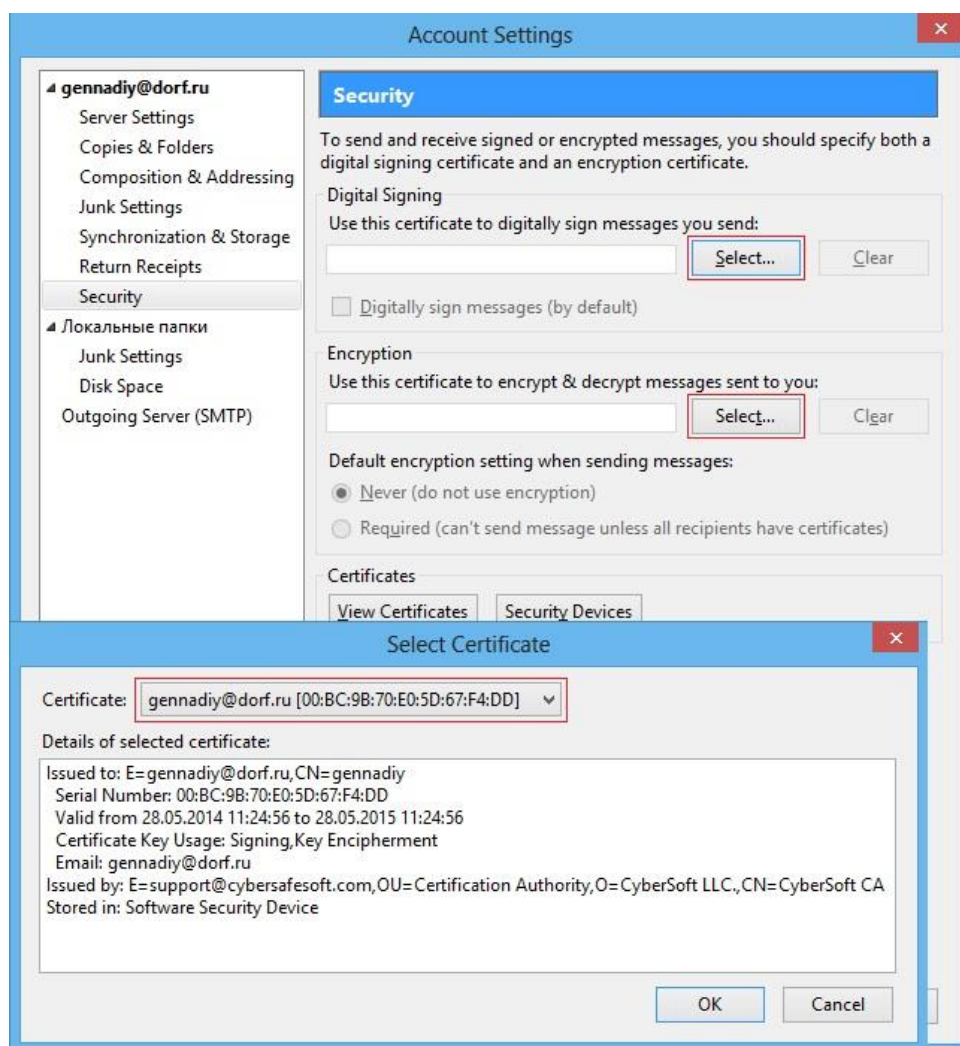
Your PFX-Certificate will be imported to the appropriate section:



- 4 Click your Account name and select **View settings for this account**:



In the next *Account Settings* window select **Security** and specify the personal Certificates for digital signatures and encryption, using **Select** buttons.



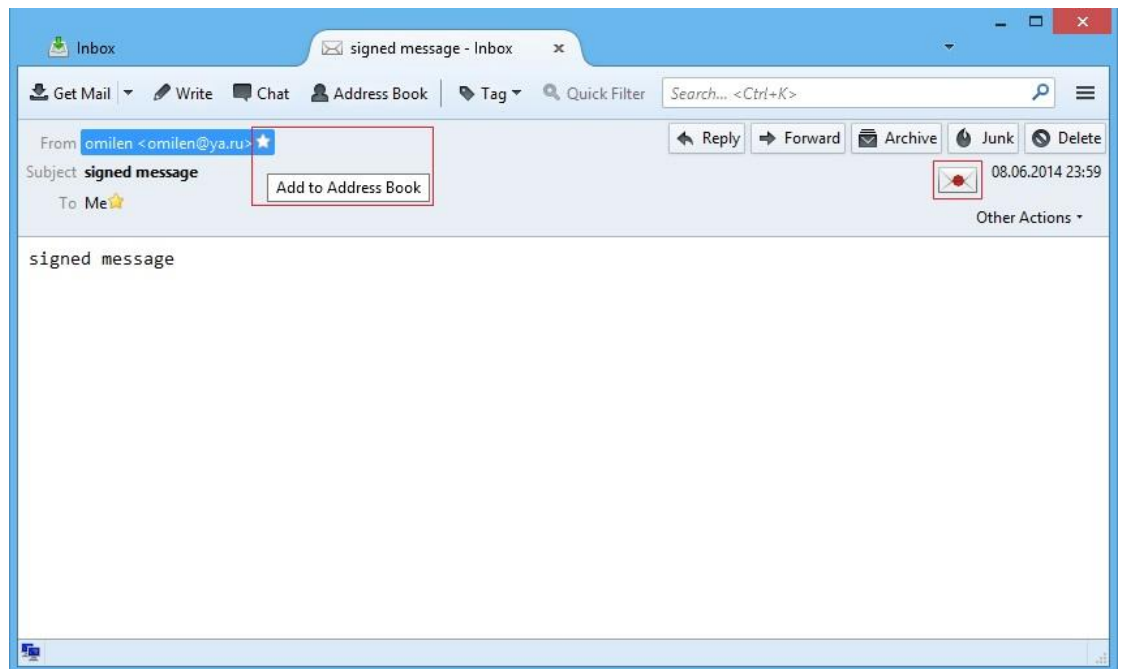
In the appeared window that asks whether you want to use the same certificate when you encrypt and decrypt messages sent to you press **Yes**.

To save settings press **OK**.

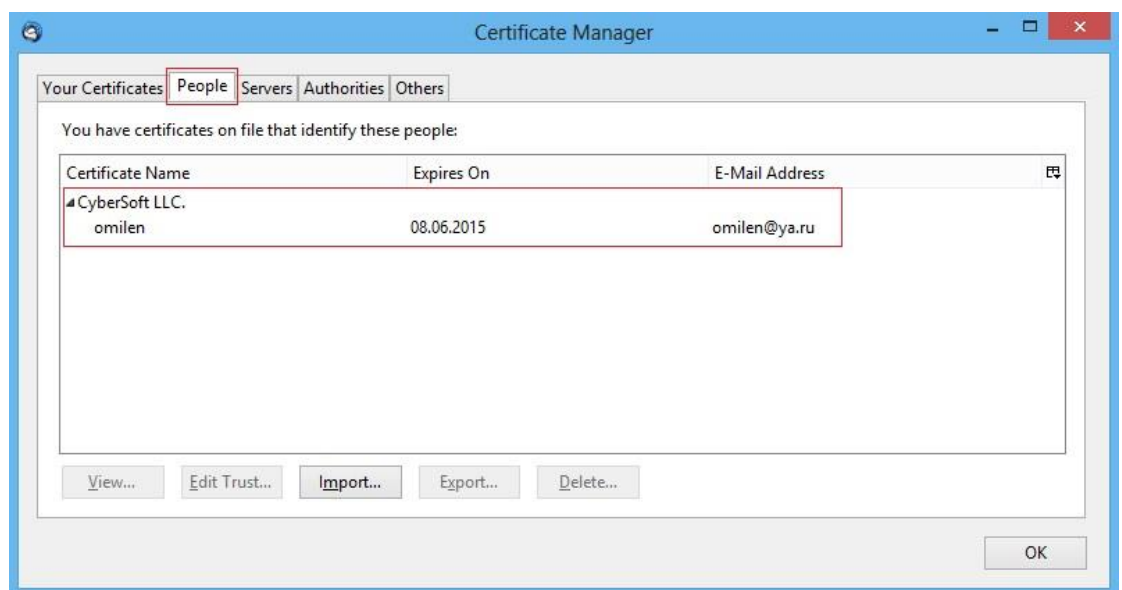
- 5 Please, note that if the user to whom you send an encrypted message haven't got your Public Key yet, he will not be able to decrypt it. So first you have to send to him unencrypted e-mail message containing your Public Key and signed by your digital signature.

User will add you to contact list and similarly will send to you his Public Key.

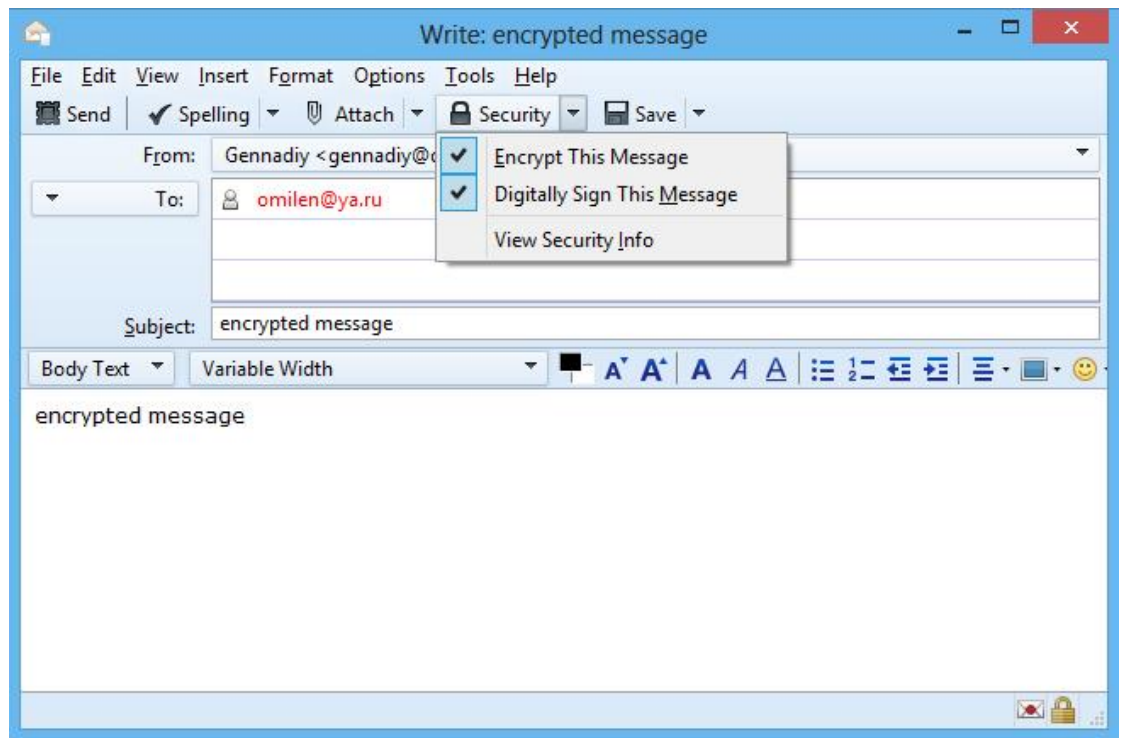
- 6 When message signed by your recipient is received you should add him to the *Address Book*:



Then make sure user's Certificate was imported into Thunderbird storage (People section):



- 7 To send an encrypted message to another user, select **Write**. A new window *Write:* will be opened. On the **Security** tab tick **Encrypt this message** and **Digitally sign this message**.



Encryption feature in Mozilla Thunderbird is configured.

7

Encrypting files with CyberSafe Top Secret

CyberSafe Top Secret gives you the ability to encrypt your files and folders and create self-extracting encrypted zip archives, which is very convenient both in for basic personal use and exchanging data with other users.

In this Section

About file encryption	47
File and Folder Encryption	47
Creating encrypted .zip archives	51
Additional encryption settings	53

About file encryption

Encryption of files and folder is used to protect them against unauthorized access. You can use CyberSafe Top Secret to create, open and edit encrypted files, folders, and zip-archives.

You may need to encrypt a file or folder for two reasons: safe storage on your own computer, or sending to another user.

If you choose to encrypt a file for personal use, it will be encrypted via symmetric key, just like is used in whole disk encryption.

Encryption of files has its advantages over whole disk encryption or creating virtual disks. For example, if you have an encrypted virtual disk with 100 encrypted files when you need to access one of these files the disk is decrypted and becomes unprotected as well as the other 99 files. But if you encrypt files individually, working with one of them does not affect the security of all the rest -these files will still be intact, fully protected and encrypted.

If you want to encrypt files to send them to other users, they will be encrypted via Public Key. To do this, you must have these users' Certificates in your computer's local certificate database. If you do not have a particular user's Certificate you can try to find it on the CyberSafe Top Secret Server by email address, using the search function.

File and Folder Encryption

With CyberSafe Top Secret you can encrypt files and folders in three ways: using PKI, by password or by creating self-extracting encrypted zip-archives.

Public Key Infrastructure Based Encryption

Use PKI-based encryption to:

- Ensure the highest degree of file protection.
- Encrypt files to share with users who have installed CyberSafe Top Secret (you have to have their Public Keys on your key ring).
- When you do not want to give the recipient the password to files you send.

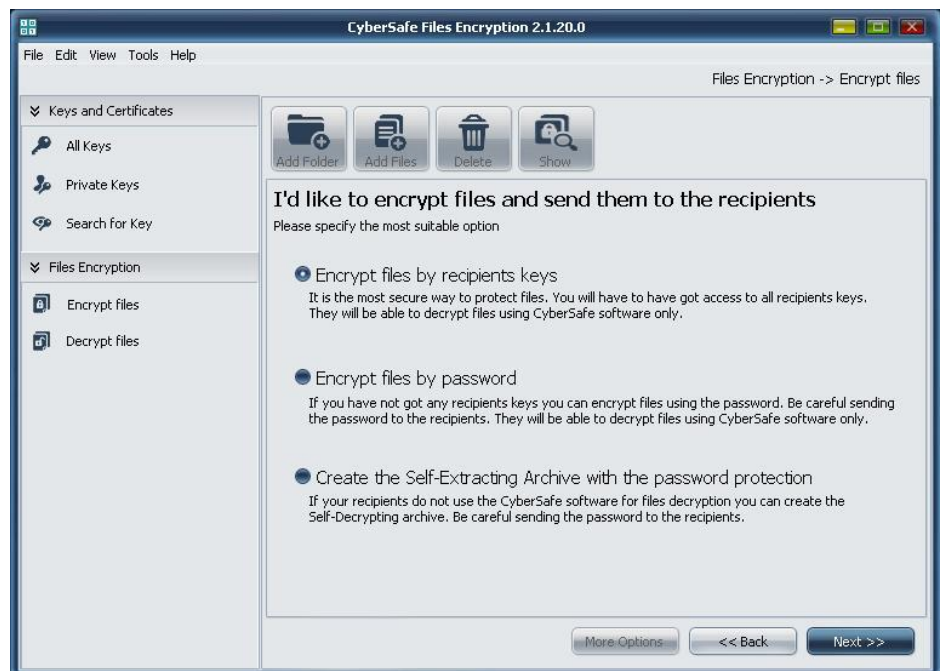
If you send a file to others, Public Key Infrastructure based encryption is the best solution, which should be your first choice if you need the highest degree of security.

As soon as the necessary files are encrypted, you can send them to other users. After receiving the files, the user will be able to decrypt them using CyberSafe Top

Secret and his Private Key. Files can be decrypted by any user whose public keys you used when encrypting. As a result, each of the users will receive the same files.

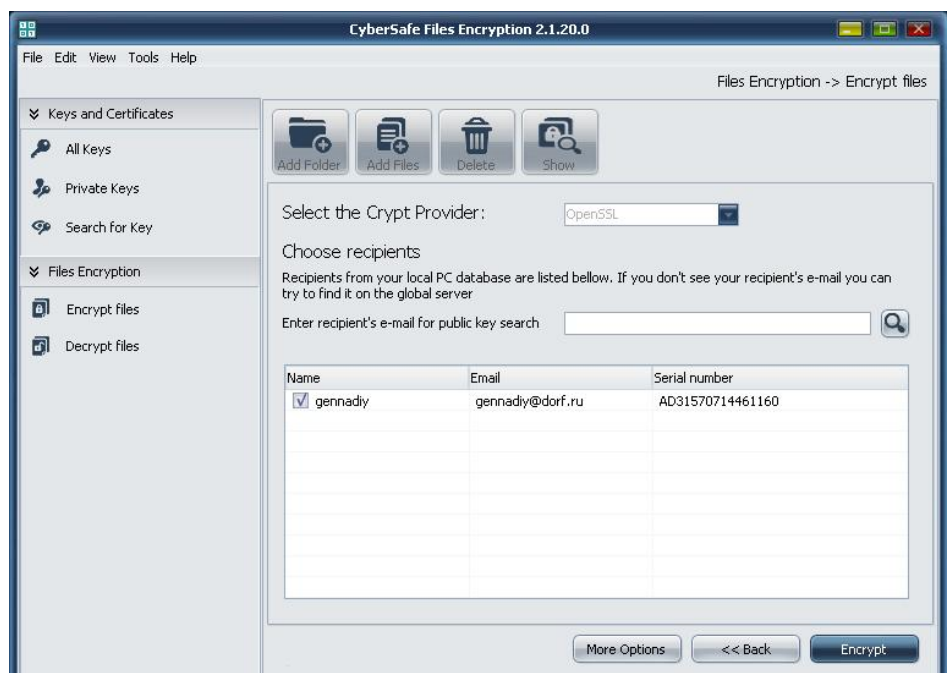
► **How to use PKI-based encryption**

- 1 Open CyberSafe Top Secret, go to the *File Encryption* box and select the option **Encrypt Files**.
- 2 In the *Options Menu* select **Add Folder** or **Add Files** to add files or folders to be encrypted (or simply drag and drop them into the *Work Area*). After the necessary data is added, click **Next**.
- 3 In the next window tick **Encrypt files by recipients' keys** and click **Next**:

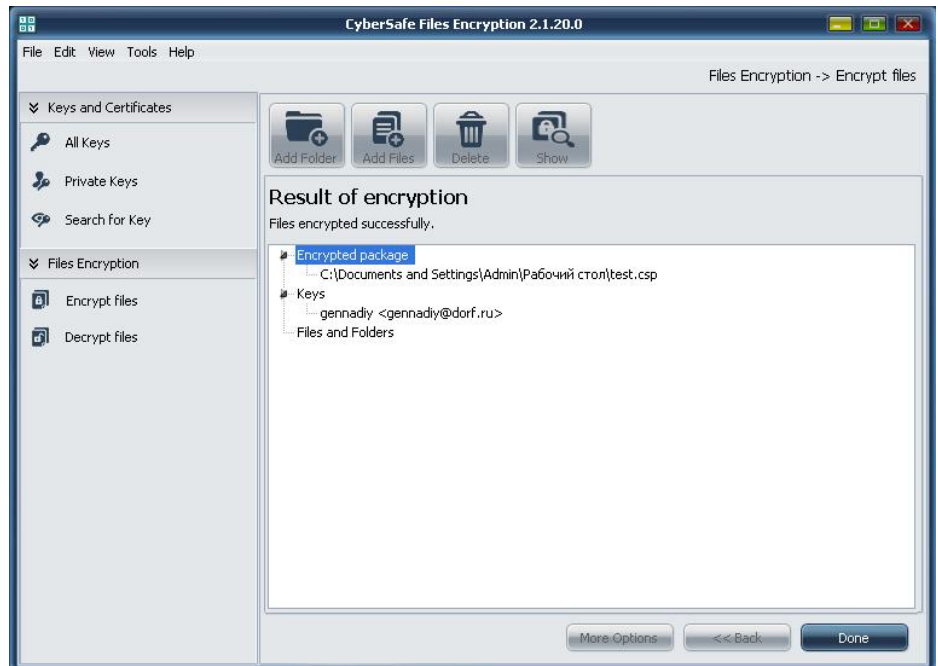


- 4 In the next window from the drop-down list select the Cryptoprotider that will be used for encryption.

From the list select the users whose Public Keys will be used for encryption. If user is not listed use the search function to find his Public Key on the CyberSafe Top Secret Server. Then press **Encrypt**.



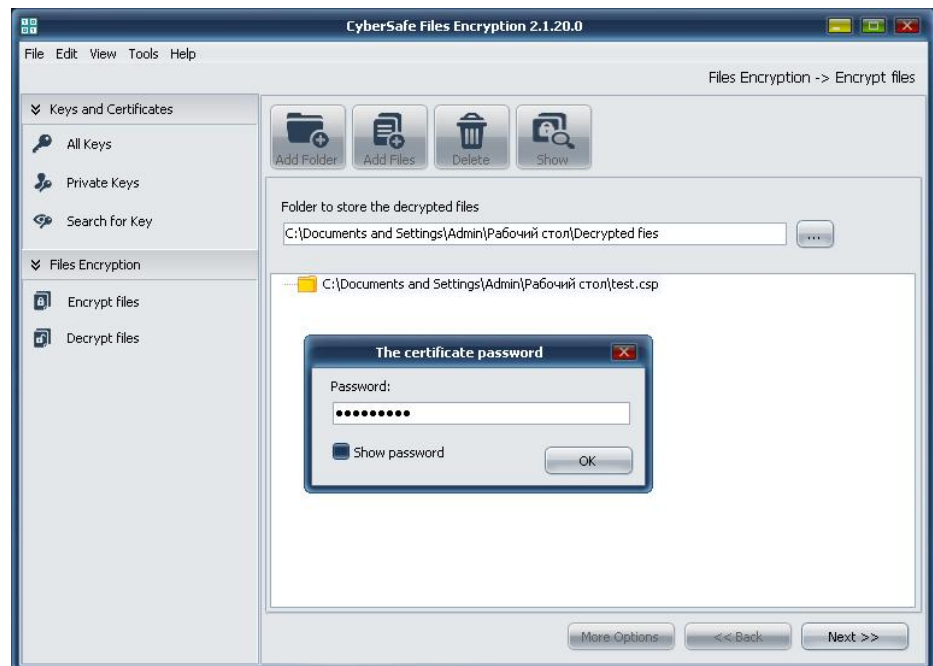
- 5 Added files will be encrypted. After encryption is completed you will see the following window:



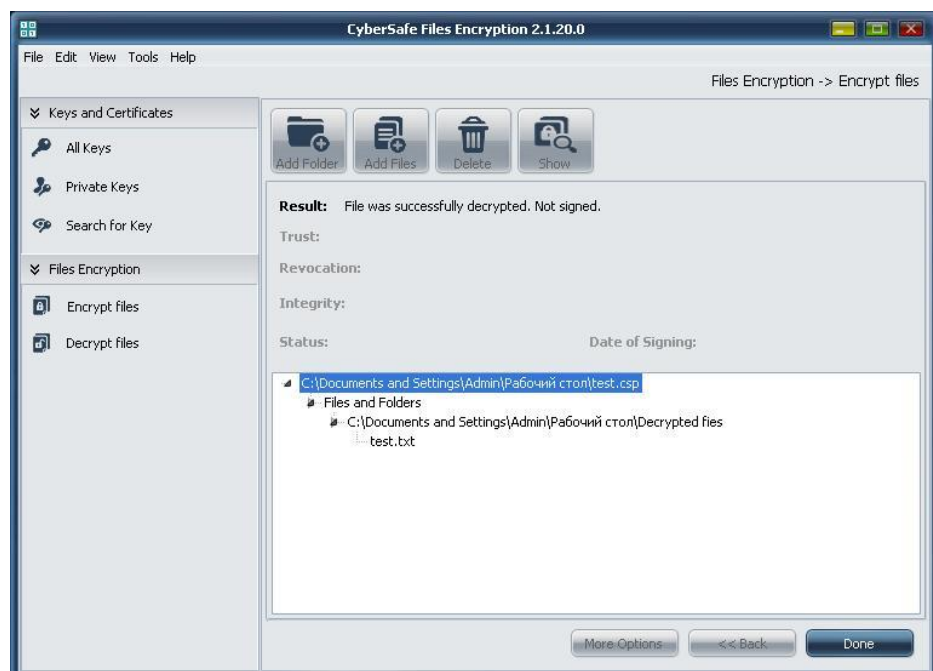
- 6 The path to the encrypted files is displayed in the *Encrypted Package* section. In the *User Keys* section, the recipients' certificates are displayed. Information about the digital signatures is displayed in the *Singing* section. A list of encrypted files is displayed in the *Files and Folders* section.
- To open the folder that contains the encrypted files in the *Options Menu* click **Show**. Press **Done** to exit.
- PKI-based file encryption is completed.

► To decrypt files

- 1 Open CyberSafe Top Secret, go to the *File Encryption* box and select **Decrypt Files**. In the *Folder to store decrypted files* field specify the place where the decrypted files should be placed (by default it will be the folder the encrypted files came from).
- 2 In the *Options Menu* press **Add Files** to add files that should be decrypted (or simply drag and drop them into the *Work Area*). After the necessary data is added, click **Next**.
- 3 In the next window enter your password for the Private Key that will be used for decryption and press **OK**:



The files you add will be decrypted. After decryption is complete you will see the following window:



- 4 To open the folder containing the decrypted files in the *Options Menu* click **Show**. Press **Done** to exit.
PKI-based file decryption is completed.

Encryption by password

Use password encryption if:

- You want to encrypt files without using your Private Key or other users' Public Keys (this may be a less reliable method of protection but, nevertheless, it is fairly reliable).
- Each of the recipients has CyberSafe Top Secret installed on their computer.
- You want recipients know the password to the encrypted files.

- You do not have all the recipients' Public Keys and you also cannot find them on the CyberSafe Top Secret Server.

Note. Encryption by password is one of the traditional encryption methods.

Encrypting files by password can ensure a very high degree of protection, especially if your password was selected properly. However, PKI-based encryption provides a higher level of protection, because the user not only has to have the password, but the Private Key as well to decrypt files.

If a file is encrypted by password it can be decrypted by any user who knows the password and has CyberSafe Top Secret installed on their computer. A Private Key is not required in this case.

Warning. Take all possible measures to keep your password from outsiders. It should be known only to recipients of the encrypted files. If the password is known to outsiders, encrypt the files again using a different password. However, keep in mind that you cannot do anything in order to provide more protection for the files encrypted originally.

► How to encrypt files by password

- 1 Open CyberSafe Top Secret, go to the *File Encryption* box and select **Encrypt Files**.
- 2 In the *Options Menu* select **Add Folder** or **Add Files** to add files or folders to be encrypted (or simply drag and drop them into the *Work Area*). After the necessary data has been added, click **Next**.
- 3 In the next window tick **Encrypt files by password** and click **Next**:



- 4 In the next window enter the password that will be used to encrypt the files. To display the password click *Show password*. In the *Password* field enter the password you want to use to encrypt files. A special indicator under the entered password will help you to evaluate its reliability. Your password will be evaluated through a comparison of the entropy characters you have entered with a random 128-bit sequence (an AES128 key has the same entropy value).
- 5 Enter your password again in the field **Confirm Password**.
- 6 Click **Next**. In the next window create a digital signature if necessary. To do this select the Private Key that will be used to create the signature. The recipient will be able to verify your signature using your Public Key and make sure that these files have been received from you.
 - If you do not want to sign the encrypted files, choose **None**.

- If you want to sign files select your Private Key from the list of keys and enter your password for this key (please note that this is not the password used to encrypt the files).
- 7 Click **Next**. The files added will be encrypted. Click **Done** to exit. Encryption by password is completed.
 - 8 Encrypted files are ready to be sent to other users. Do not forget to tell them the password to these files so they will be able to decrypt them.

Creating Encrypted .zip archives

A CyberSafe Top Secret .zip archive is an individual file encrypted and compressed for easy transfer or backup. These archives can store any number of different files and/or folders, which is especially convenient for backups, or safely sending files to other users.

If you received an encrypted .zip archive you can:

- Extract all files and/or folders from the archive.
- Extract some files and/or folders from the archive.
- Add new files and/or folders to the archive.

You should use .zip archives if:

- You want to create a Self-Extracting zip-archive without using a user's Public Key (it may be a less reliable method of protection, but nevertheless it is quite reliable).
- The recipient doesn't have CyberSafe Top Secret on his computer, but he uses Windows.
- You want recipients to know the password to the encrypted files.
- You don't have the Public Key of some of the users and you cannot find it on the CyberSafe Top Secret Server.

A .zip archive created using CyberSafe Top Secret can be opened only on Windows. It is a standard executable file, which that can be extracted after double-clicking.

Self-extracting encrypted zip files are larger than normally encrypted files because the automatic extraction "mechanism" also takes up a certain amount of space (usually about 100 KB).

Once you've created an encrypted .zip-archive, send it to another user. Any user who receives this archive will see the same files after the opening it. If you want to send different files to different users, you should create separate files for each of them.

Warning. Take all possible measures to keep your password from outsiders. It should be known only to the recipients of the encrypted files. If the password is known to outsiders, encrypt the files again using a different password. However, keep in mind that you cannot do anything to provide more protection to the originally encrypted files.

► How to create an encrypted .zip archive

- 1 Open CyberSafe Top Secret, go to the *File Encryption* box and select **Encrypt Files**.
- 2 In the *Options Menu* select **Add Folder** or **Add Files** to add files or folders to be encrypted (or simply drag and drop them into the *Work Area*). After the necessary data has been added, click **Next**.
- 3 In the next window tick **Create a password protected self-decrypting** and click **Next**:



- 4 In the next window enter your password that will be used to encrypt the files. To display the password click *Show password*. In the *Password* field enter the password you want to use to encrypt the files. A special indicator under the entered password will help you to evaluate its reliability. Your password will be evaluated through a comparison of the entropy of the characters you have entered with a random 128-bit sequence (an AES128 key has the same entropy value).
- 5 An encrypted *.exe archive will be created. It will be placed the folder the source file came from.
If the archive contains more than one file the archive will be named after one of these files by default.
- 6 The next window will show you the path the encrypted archive. Press **Done** to exit.

Additional encryption settings

When you select any of the encryption methods, (PKI, password or encrypted .zip archive) before you click **Encrypt** you can open the advanced settings window using the **More options** button:



In this window you can:

- Select the Private Key used to digitally sign files.
- Change the default encryption algorithm, the level of protection and hashing algorithm.
- Control other additional settings.

8

Working with passwords and passphrases

Passwords and passphrases are used to protect data. As a rule, passphrases are longer and contain a much broader range of characters in comparison with passwords.

For example, a simple password can be a combination of two words, for example: "goodwork" without quotes. More reliable passwords can contain uppercase characters, for example: "GoodWork". More secure password may include numbers, such as: "Good7Work2".

Passphrases are longer than passwords and include a wider variety of characters. For example, a simple keyword phrase might be "Eh2H,to&LF" without quotes. This passphrase might seem hard to remember, but in reality it is based on a simple phrase, which is much easier to remember.

A passphrase may also consist of simple phrases, for example, from a favorite book, including punctuation and capital letters: "*In this world, nothing is certain but death and taxes,*" including the quotation marks. Despite the fact that this passphrase is not very reliable, it is actually at least two times more secure than any of passwords given above.

This section describes the differences between the passwords and passphrases, and explains password strength indicator used in CyberSafe Top Secret, as well as giving some advice on creating strong passwords.

In this Section

What to use: password or passphrase?	55
Password strength indicator	56
Creating a strong password.....	56

What to use: password or passphrase?

So, you know what's best for keeping your data secure: a password or a passphrase? That all depends on what you are trying to protect. The more valuable the protected information, the stronger the protection should be.

The majority of documents around the world are not protected at all; the information contained in them is not so valuable and its protection does not justify much effort. When you use online banking, some banks require only a PIN, consisting of only four digits. Depending on the amount of money on the account, this may not be quite as secure as you need. You can use a Hotmail account for unimportant emails, and in this case, a simple password is quite enough.

In CyberSafe Top Secret, for example, you create a password for your Key pair and for virtual disks. If you create a weak password for your Key pair and hackers get ahold of your Private Key, all they would need is to read your messages and send messages on your behalf is to figure out your password.

Password strength indicator

When you create a password in CyberSafe Top Secret, the password strength Indicator is the main reference point that illustrates how strong the password you've created is. It works much better than simply counting the number of characters.

Basically, the fuller the password strength scale, the better. However, does this scale really mean? The password strength indicator compares the value of the random variables (entropy) in the password with a 128-bit random sequence (the same entropy value as the AES128 key). This is called a 128-bit entropy. Entropy is the value that determines a password's capacity to resist hacking attempts.

Thus, if you created a password and the indicator is about half way filled, this means that it has approximately 64 bits of entropy. But if you created a password and the indicator is full, this means that it has approximately 128 bits of entropy.

However, how strong is a password with 128 bits of entropy? In the late 1990s special computers called "DES-crackers" were created that could guess a DES-key in a few hours by going through all possible key values.

If we assume that someone is able to create a computer that can crack a DES key not in several hours but in one second (the computer would have to handle 255 keys per second), then it would take approximately 149 trillion (a thousand billion) years to crack a 128-bit AES key. For comparison: it is thought that our universe came into existence less than 20 billion years ago.

What is the impact on the entropy of different characters? The more extensive the range of characters included in the composition of the password, the greater the entropy. For example, if you need to create a PIN code from numbers, this means that you can use only 10 characters. This is a very small range and, therefore the entropy of all the characters together is extremely low.

However, if you are using the English version of the CyberSafe Top Secret, everything is different. You have three character sets from which to choose: uppercase and lowercase letters (52 characters), the numbers from zero to nine (10 characters), as well as punctuation marks and other symbols (32 characters). When you enter one of these characters, CyberSafe Top Secret sets the entry value based on the range, from which it was selected and displays this on the scale that shows the password strength.

The same applies to characters in other languages - the larger the range, the more entropy per symbol.

Creating a strong password

A good password combines the optimal balance between ease of use and reliability. Long passwords, which consist of upper and lower case characters, numbers and symbols are stronger, but at the same time they are more complex.

Practice shows that the passwords that are difficult to remember are often written down, which is utterly counterproductive to creating a secure password. It is much better to have a shorter password that you can easily remember, than a longer one you have to write down or, even worse, forget.

A general formula for creating strong passwords is that some phrase should be reduced to a set of individual characters. For example, the phrase:

Everyone has two homelands, their own and La

France. becomes the passphrase:

Eh2H,to&LF

This passphrase has 10 characters, uppercase and lowercase letters, numbers, and punctuation. 10 characters is a relatively short passphrase. If you think that's not enough, come up with another passphrase, using the same method and combine it with the existing one.

Another approach to using easy to remember passwords involves the use of punctuation and capital letters

For example:

I never think of the future. It arrives soon enough. (Albert Einstein)

This phrase is not very difficult to remember, but, nevertheless, it is strong. If you decide to use a phrase from an existing books, try not to lose the book

itself.

Another approach is to combine a lot of short-familiar words. This approach is

called Diceware. It uses dice to randomly select words from a special list called the Diceware Word list, which consists of 7776 short English words, acronyms, and easily memorable character strings. If you gather together a sufficient number of these short words, you can create a strong password. In their FAQ, the creators of Diceware claim that you can reach 128 bits of entropy using 10 words from their list.

For more information about Diceware, visit their website (<http://world.std.com/~reinhold/diceware.html>).

When it comes to creating a password, here are a few things you should do:

- Use phrases that are already in your long-term memory. This makes it much less likely that you'll forget it.
- Create a password of at least eight characters. Password length is not the main indicator of reliability, but all the same, a password should not be short.
- Use a combination of uppercase and lowercase letters, numbers, and symbols in your passphrase.

Warning. Try to use only ASCII characters if possible. This is especially important when using foreign keyboards that contain some special characters that are not supported (for example, the character "§").

- Change your password periodically. It is best to do it once every three months. The longer you use the same password, the more likely it is that someone figures it out.

Here are some things you should not do when creating passwords:

- Don't write down your password or passphrase.
- Don't disclose your password to anyone.
- Don't let anyone see you enter your password.
- Don't use templates such as "abcdefgh" or "123456789" or "qwerty" or "7777777 " or "gggggg".
- Don't use common words . Almost every experienced hacker uses a program to crack passwords based on the dictionary. Do not combine two common words together, do not use the plural of common words, do not use common words with the first letter capitalized.
- Don't use numbers that have some relation to you. If anyone knows these numbers the attacker might know them as well. Do not use your birth date, phone number, social security number, address , etc.
- Don't use names. Neither the names of people, nor the names of fictional characters or pet names. Don't even use the name of the place you vacationed last summer, your login or your company name. Do not use the name of your favorite sports team, or names from any books, especially from the Bible.
- Don't use words written in reverse or words with all their letters replaced by numbers.