Jetico

BCTextEncoder

Help File

Introduction

Introduction

BCTextEncoder is a line in BestCrypt family of encryption software products.

BCTextEncoder software provides an easy way of encoding and decoding text data. Plain text data are compressed, encrypted and converted to text format. The result of such conversion may be copied to the clipboard or saved as a text file.

BCTextEncoder uses **public key encryption** methods as well as password based encryption. It uses strong and approved symmetric and public key algorithms for data encryption.

BCTextEncoder is very easy to use and it does not require an installation.

Main Features

Main function of the BCTextEncoder is to provide the user with very simple and fast way to encrypt text information. There are some additional features designed to simplify sending the encoded information by e-mail.

BestCrypt TextEncoder software provides the following functionality:

- Encode/decode text data encrypted with a password.
- Encode/decode text data encrypted with a public key.
- Generate new or import existing public/secret key pair using BestCrypt Key Manager in PKCS-12/X.509 format.

BCTextEncoder Requirements

BCTextEncoder requires the following minimum computer configuration:

Hardware

- PC with 486 or higher processor
- 2 MBytes of free HDD space to run the software.

Software

- Windows 7
- Windows Vista
- Windows XP
- Windows 2000
- Windows Server 2003/2008/2011/2012

BCTextEncoder Specifications

BCTextEncoder utilizes the following encryption algorithms, standards and specifications:

- ZLIB compression algorithm.
- AES(Rijndael) encryption algorithm for password based encryption
- RSA asymmetric encryption algorithm for public key encryption

See also:

Encoded Data Format

How to use BCTextEncoder

BCTextEncoder and its Assistant

BCTextEncoder is intended for fast encoding and decoding text data. So, there must be an easy way to access the program window as soon as the need arises. From the other hand, it is not very good to keep the BCTextEncoder window always opened. To resolve the issue, a special process is used - **BCTextEncoder Assistant**.

The process is always running in the background and monitoring keystrokes on your keyboard to detect pressing the **Hot Key** combination to open BCTextEncoder window.

Additionally, **BCTextEncoder Assistant** is able to show or hide the systray icon and clear all BCTextEncoder settings and modified registry entries. See more information in BCTextEncoder Assistant Options chapter.

See also:

How to use BCTextEncoder
BCTextEncoder Commands and Options
Encoded Data Format
BCTextEncoder Assistant Options
Local Public Key Database and Key Management

Quick Start

Let's assume you were writing an e-mail using your accustomed e-mail application and you decided to encrypt a part of the message. Provided that all needed options have been already set, you will have to make only four simple steps:

1. Select the secret data and put it to clipboard with Ctrl-X;
2. Press a predefined hot key to open BCTextEncoder and click [**Encode**] button;
3. Enter password;
4. Return back to your e-mail and paste the encrypted data from clipboard with Ctrl-V;

The main advantage of BCTextEncoder is support of **public key encryption**. If you have a public key of your recipient, then you may make slightly different steps:

1. Select the secret data and put it to clipboard with Ctrl-X;
2. Press a predefined hot key to open BCTextEncoder
3. Use ***Encode by*** list box, choose the public key of your recipient and click [**Encode**] button;
4. Return back to your e-mail and paste the encrypted data from clipboard with Ctrl-V;

Alternatively, you can write the message directly in BCTextEncoder window or load the text from an existing text file. After encoding the text, it may be sent to the recipient immediately, if corresponding option is enabled. If you encrypted the text with a public key, the e-mail will be read automatically from the key, so you do not have to do anything except confirmation of sending.

See also:

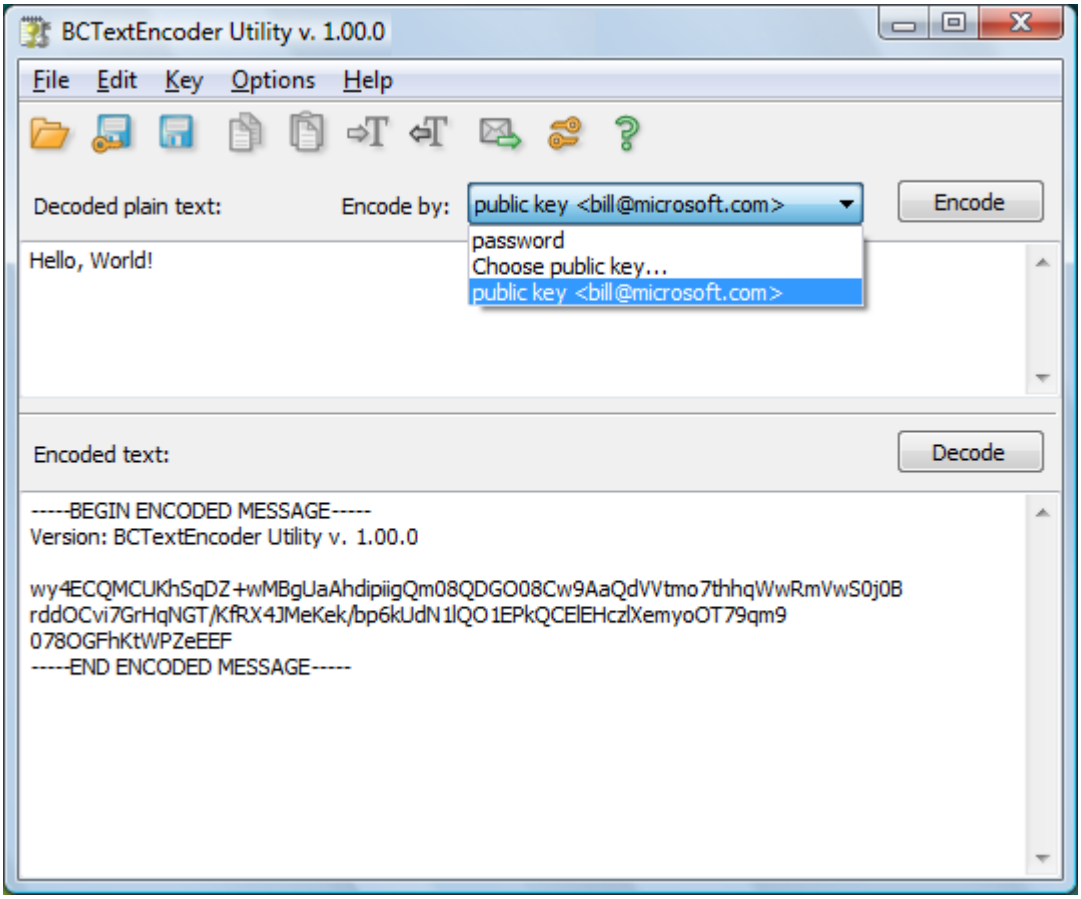
How to use BCTextEncoder
BCTextEncoder Commands and Options
BCTextEncoder Assistant Options
Local Public Key Database and Key Management

How to use BCTextEncoder

Opening BCTextEncoder window

To run BCTextEncoder for the first time, you should run BCTextEncoder.exe file which was downloaded from our site. **BCTextEncoder** main window will appear and **BCTextEncoder Assistant** process will start. When BCTextEncoder Assistant is running, you can open the main BCTextEncoder window using the systray icon or predefined Hot Key. See more information in BCTextEncoder Assistant Options chapter.

BCTextEncoder window consists of two panes - **Plain Text** pane and **Encoded Text** pane.



Text Encoding

1. Put the text into **Plain Text** pane. This can be done by three ways:

- Select the text in your e-mail or text editor, copy it to clipboard and open BCTextEncoder. If the option ***Automatically decode encoded text*** is enabled, the contents of the clipboard will be placed to the window automatically. Otherwise, you have to paste it manually.
- Type the text directly in **Plain Text** pane of BCTextEncoder window.
- Open the text file with ***Open*** command from ***File*** menu.

2. Using ***Encode by*** box, choose a type of encryption. You may encode by password or by public key of other person. If you have no a public key, please see BestCrypt Key Manager section to

know how to generate your own key pair and import an existing public key. The Key Manager functions are available in ***Key*** menu of BCTextEncoder window.

3. Use [**Encode**] button to encode the text displayed in **Plain Text** pane. The encoded text in Encoded Text Format will be placed in **Encoded Text** pane.

Text Decoding

To decode a text, copy encoded text to clipboard and open BCTextEncoder. If the option ***Automatically decode encoded text*** is enabled, you will be asked for the password and the decoded text will be placed into **Plain Text** pane. Otherwise, you have to paste encoded text manually and use [**Decode**] button to decode the text.

See also:

BCTextEncoder Assistant Options

BCTextEncoder Commands and Options

Menu Items

- ***File***
  - ***Open*** - open a text file to encode or encoded text to decode
  - ***Save*** - save the current window contents to a file
- ***Edit***
  - Increase Indent - indent the original text with the symbol ">"
  - Decrease Indent - remove symbols ">"
  - Copy to Clipboard
  - Paste from Clipboard
- ***Key***
  - Generate New Public/Secret Key Pair
  - Choose public key for encoding
  - Manage Key Database - opens **Public Key Manager**
- ***Options***
  - Copy decoded text to clipboard after decoding
  - Copy encoded text to clipboard after encoding
  - Send encoded text by e-mail now
    Send encoded text automatically after encoding
  - Clear clipboard
  - Clear clipboard automatically on Exit
  - BCTextEncoder Assistant and Hot Key options
- ***Help***
  - About
  - Help index

Toolbar Buttons

 - read text from existing file;

 - save encoded text to file;

 - save decoded text to file;

 - paste clipboard text to currently focused window;

 - copy currently focused window text to clipboard;

 - increase indent;

 - decrease indent;

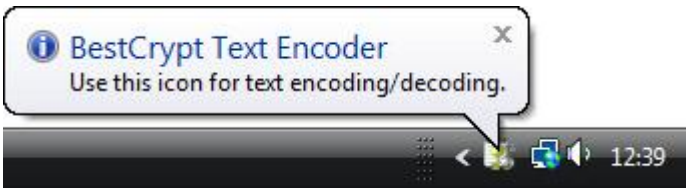
 - send encoded text by e-mail;

 - choose public key for encoding;

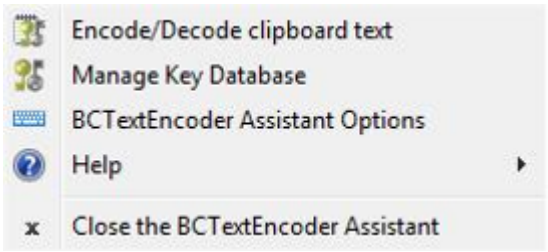
 - about BCTextEncoder;

Sytray Icon Menu.

When you start BCTextEncoder for the first time, **BCTextEncoder Assistant** starts and creates the icon in System Tray area and shows the balloon.



The Systray Icon has the following pop-up menu:

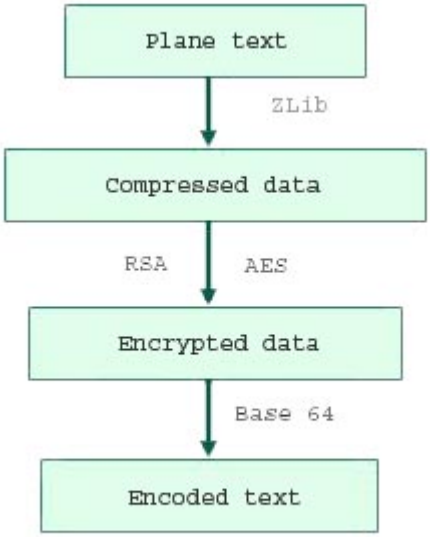


See also:

How to use BCTextEncoder
BCTextEncoder Assistant Options
Local Public Key Database and Key Management

Encoded Data Format

BCTextEncoder not only encrypts, but also compresses the data.
First, plain text data is compressed by **ZLIB** compression algorithm. The compressed data is encrypted by choosen public key or by password. At this step, BCTextEncoder utilizes **RSA** asymmetric algorithm for public key encryption and **AES(Rijndael)** algorithm with 256-bit key for password-based encryption. Finally, encrypted data is encoded by **BASE64** encoding algorithm to text format.
The picture illustrates the process of data transformation:



Example:
The 'Hello, Word!' plain text encoded by password 'password' looks like:

-----BEGIN ENCODED MESSAGE-----
Version: BC Text Encoder Utility v. 1.00.0 (beta)

wy4ECQMC6J8Np1DDfutgzFNqgHsDsam9CbC/QJ3pg8oV7nFbbtQrfygrLRoh/y/10j0B
2hHwpqOX5ACgP4tgt/D9RQmOQSON92mSSvoMVEnm9yq/hIO/XJ0lIi+VsWNpaBBs
mVvhD6VocCAzWJiz
-----END ENCODED MESSAGE-----

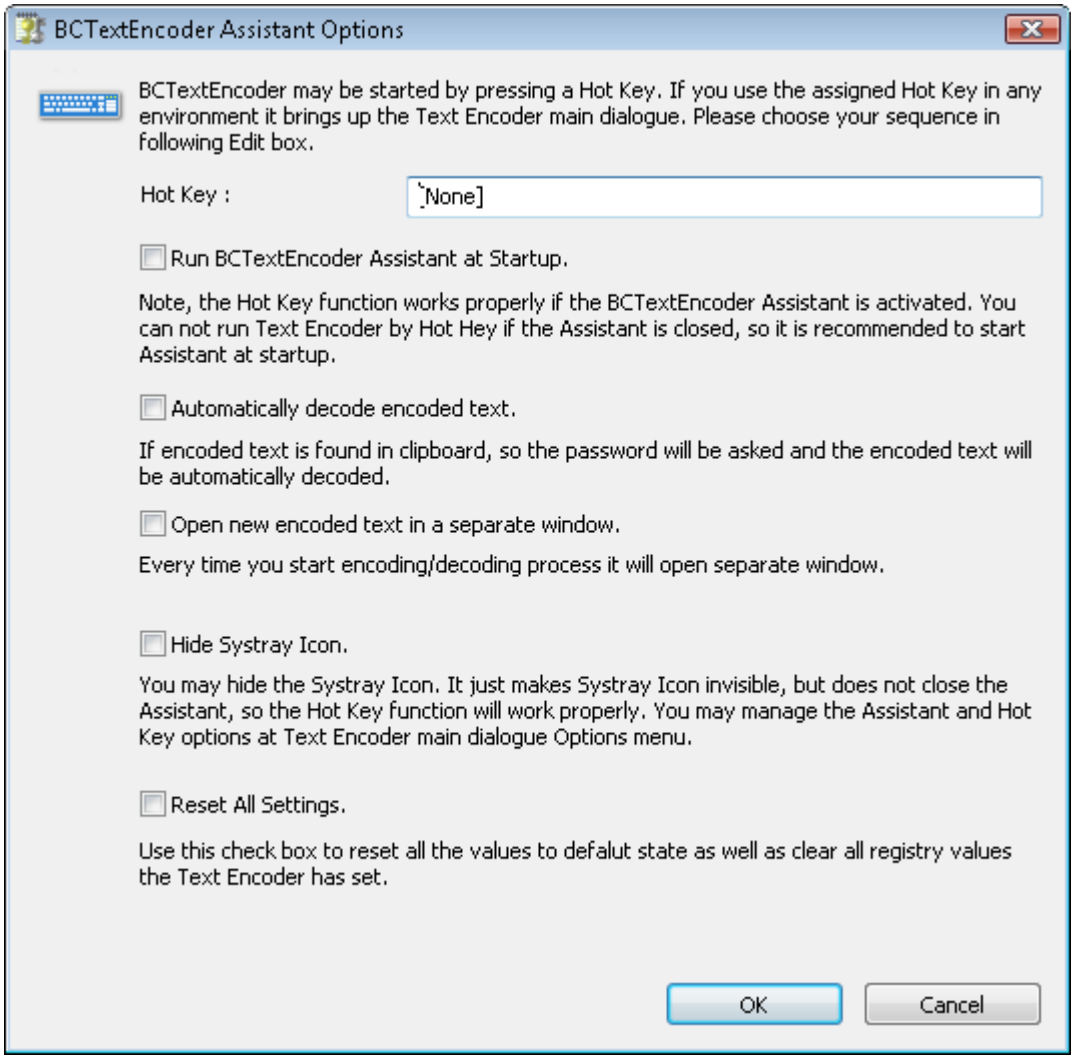
So resulting text contains only valid characters and may be sent by e-Mail or saved as a text file.

NOTE: BCTextEncoder is compatible with well known **PGP utility**. It means that it can decode messages encoded by PGP

BCTextEncoder Assistant Options

BCTextEncoder Assistant Options dialog is used to change settings concerning BCTextEncoder Assistant activity. To open the dialog you should run the command ***BCTextEncoder Assistant Options*** in ***Options*** menu of BCTextEncoder window OR in **Systray Icon** pop-up menu.

The following window will appear:



Hot Key

You can start BTextEncoder main window by pressing the specified Hot Key from any environment.
Type your key sequence in ***Hot Key***: edit box, f.e. 'Ctrl+Alt+H'.
If you want to disable the Hot Key functionality, just delete all symbols with `Backspace` button.

Run BCTextEncoder Assistant at Startup

Note, you cannot run BCTextEncoder by Hot Hey if the Assistant is not running, so it is recommended to start the BCTextEncoder Assistant at system startup.

Automatically decode encoded text

The option allows to decrease amount of steps for decoding to minimum. If you see encoded text, you just copy it to clipboard and press the hot key you've previously assigned. BCTextEncoder automatically detects encoded text in clipboard, asks for the password and shows decoded text. If encoding signatures are not found, the text is considered as plain text you are going to encode. So the text is placed to **Decoded plain text** window, you need to choose encoding options and click **[Encode]** to encode the text.
If you set options ***Copy encoded text to clipboard after encoding*** and ***Copy decoded text to clipboard after decoding*** you will minimize the operation steps even more.

Open new encoded text in a separate window
Every time you start encoding/decoding process, it will open a separate window, so you can work with several documents simultaneously.

Hide Systray Icon
Since you assign the Hot Key, you may hide the **BCTextEncoder Systray Icon**. It just makes the icon invisible, but it does not kill the BCTextEncoder Assistant process, so the Hot Key function will work properly. In that case, you will get access to this dialog through ***Options*** menu of BCTextEncoder main window.

Reset All Settings
Please use this check box to return all settings to default state. The command also clears all the registry entries BCTextEncoder has set.

See also:

How to use BCTextEncoder
BCTextEncoder Commands and Options

Local Public Key Database and Key Management

Local Public Key Database and Key Management

A lot of people around the world have their **secret(private)** and **public** keys. They make their public keys opened for everyone and keep corresponding private keys in a secure place. Public key can be used by anyone to encrypt data, but only an owner of corresponding private key can decrypt the data.

For example, you decide to send an encrypted container to your friend John. John may have his public key created earlier and stored on a **Public Key Server** in Internet. John may also send you his public key attached to e-mail. As soon as you get John's public key, you can encrypt the container with this key and send it to John. After receiving the container John will be able to access data with his **secret** key.

BCArchive includes the **BC Key Manager** utility to manage your own public/secret key pair as well as public keys you have received from other people. You can run **Key Manager** utility from BCArchive Program Folder or using ***Manage Key Database*** command in ***Archive*** menu of BCArchive main window.

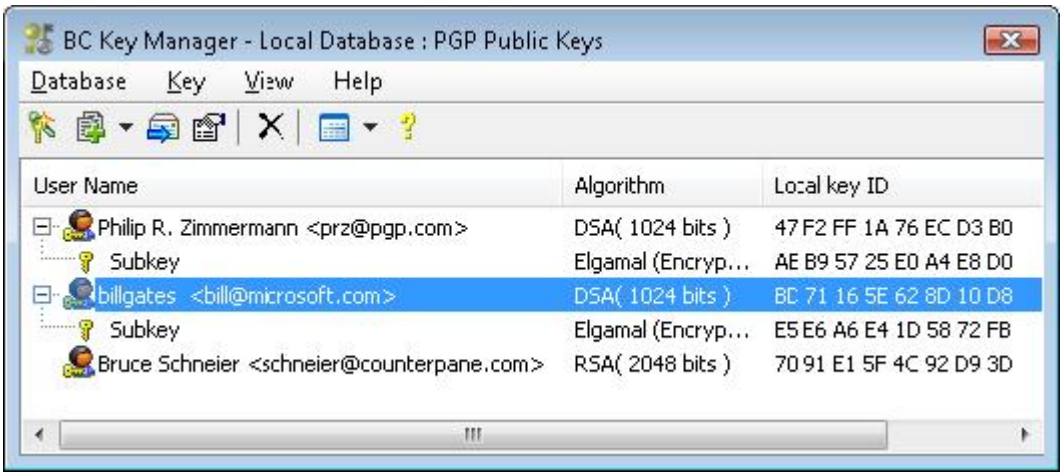
See also:

Create or import Secret/Public Key Pair
Add Public Key to Local Public Key Database
Backup/Restore Local Key Database

Create or import Secret/Public Key Pair

BC Key Manager utility allows you to create your own public/secret key pair. It may be useful if you decide to send your public key to other people so that they will be able to encrypt some information for you using your public key. As soon as you receive the information encrypted by your public key, you can decrypt it using your private key. Any other person, who has not your secret key and does not know the password for it, will not be able to decrypt the information.

It is also possible that you have already had the public/secret key pair generated earlier, for example, with a help of the **Pretty Good Privacy (PGP)** software. Since **BC Key Manager** understands a number of formats, you can import the key pair from the file created by other software.
The main window of BC Key Manager looks like:

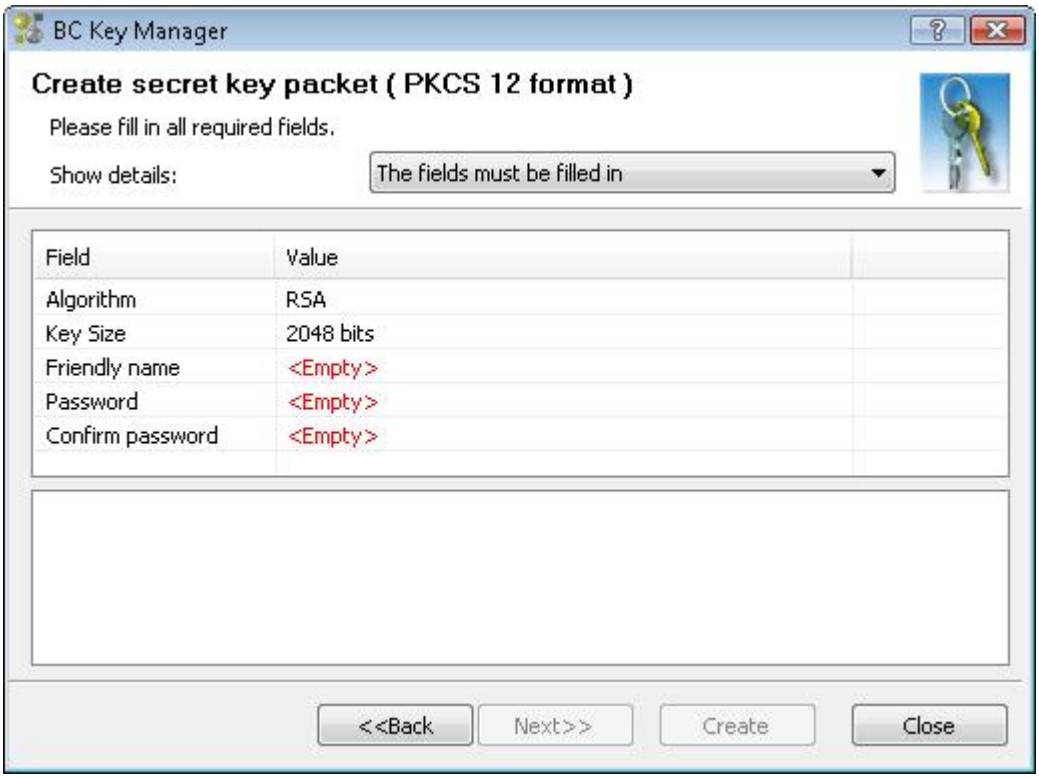


To create or import your public/secret key pair, run the ***Generate New Public/Secret Pair*** command from the ***Key*** menu in the BC Key Manager utility. The following window will appear:

In the BC Key Manager window select ***Generate new private key*** if you wish to create new key pair or the ***Import existing private key*** option if you want to use existing key pair you have created earlier using BC Key Manager or some other program.
When BC Key Manager finishes the key pair generating process, it can do all or some of the selected actions depending on the options you choose in the first BC Key Manager window:

- ***Create file with your secret key in PKCS#12 format.*** The key will be protected by password and you can save the file in any place you wish for later use or backup purposes.
- ***Create file with your public key in X.509 format.*** As soon as you create such file, you can send it to other people so that they will be able to send encrypted information to you (as it was mentioned in the beginning of the chapter).
- If you create new key pair or import existing one, Key Manager will save it in its **Local Key Database** if the ***Local Public/Secret Key Database*** option is set.
- The key pair can also be saved in a separate file in internal BC Key Manager format for backup purposes if you select the ***Files chosen later*** option.

After selecting all the option you want, click **`Next>>`** in the BC Key Manager window. The following window will appear:



In the **Create Secret packet** window you can choose the settings for creation a secret key for you. The program shows the field you must fill in drawn by red color and it means that the user should enter some strings into the fields:

- ***Friendly name***. It is the information that will be used to identify your public key among the keys of other people. For example, if you enter the **'John Smith - JohnSmith@my_email.com'** string, your friend can easily find your public key in the list of public keys of other people he/she has on his/her computer.

- ***Password and Confirm password***. Enter a password for your secret key into the ***Password*** field and enter the same password again into the ***Confirm password*** field again to verify that you have typed a correct password. The password will protect your secret key so that if even someone steals a file with your secret key, the intruder will not be able to use the file to decrypt information, encrypted by your public key.

It is also recommended to pay attention to the ***Key Size*** field in the Create secret packet dialog window. Public/secret key algorithm can be used with different key sizes and it is recommended to use the algorithm with key size equal to at least 2048 bits.

If you click **Next>>** , the **Create Certificate** window will appear. **Certificate**(as it is understood in the context of the public/secret key encryption technology) is the file with text information about your public key. Since you are going to send the public key to other people for using it on other computers with probably other software, information about your public key should be sent together with other technical information, like name of the encryption and secure hash algorithms, key size, format of the file where the key is stored and other.

The **Create Certificate** window shows you the information, which will be stored in the certificate file created for your public key. Please note that you should enter the information required in the ***Subject*** field. When you double-click on the field and start to edit it, the **Get certificate subject** dialog window will appear.

The dialog window contains a number of fields you may fill in to identify your public key among thousands of public keys created by other people. Please note that entering such information is specific for the BC Key Manager software only. It is a common practice for software that uses public/secret key technology and conforming the X.509 standard. You can fill in not all the fields in the Get certificate subject dialog window, but BC Key Manager requires the information be entered to at least one field of the window.

After entering the information click **OK** in the Get certificate subject window, and then Create button in the Create Certificate window. After that BC Key Manager will generate a public/secret key pair for you and save it to your **Local Public/Secret Key Database**.

See also:

Add Public Key to Local Public Key Database
Backup/Restore Local Key Database

Send your public key to another person

If you want to receive encrypted data from another person, the data have to be encrypted by your public key, so you should send the public key to the person. You can use BestCrypt Text Encoder to simplify the process of sending the public key by e-mail in the following way.

Please run Run BC Text Encoder and choose Manage Key Database menu. It bring up the **BC Key Manager** dialogue. Run the ***Send Public Key to E-Mail Recipient*** command from the ***Key*** menu. BC Key Manager will show you a list of all public keys in your Local Public Key Database. Select your public key from the list and click **OK** .

BC Key Manager will run your default e-mail program and prepare e-mail with empty recipient and encoded public key, written in the PKCS#12 format (so called x.509 certificate). All that you have to do is to enter e-mail address of the recipient and send the e-mail.
What your recipient should to do when he/she receives public key attached to e-mail?

The recipient should add the attached public key to the BC Key Manager **Local Key Database** on his/her computer in the following way:

- Save the attached public key certificate file to some folder.
- Run the **BC Key Manager** utility.
  The following Jetico's products BestCrypt, BCArchive and/or BC Text Encoder contain **BC Key Manager** utility. If no one from the products was installed before, it may be downloaded from our WWW-site:
  http://www.jetico.com/download.htm
- Run the ***Key -> Add Existing Public Key -> Browse For Files*** command.
- BCArchive **Choose Public Key** dialog window will appear.
- Browse the folder where you have saved the certificate file with the public key, select the file and click [**Get It**].

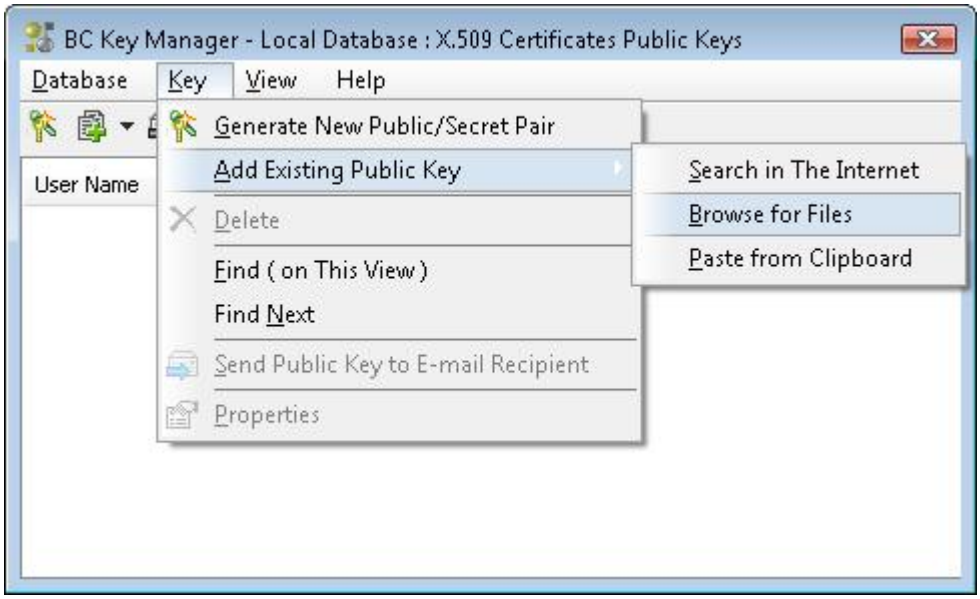
See also:

Create or import Secret/Public Key Pair
Add Public Key to Local Public Key Database
Backup/Restore Local Key Database

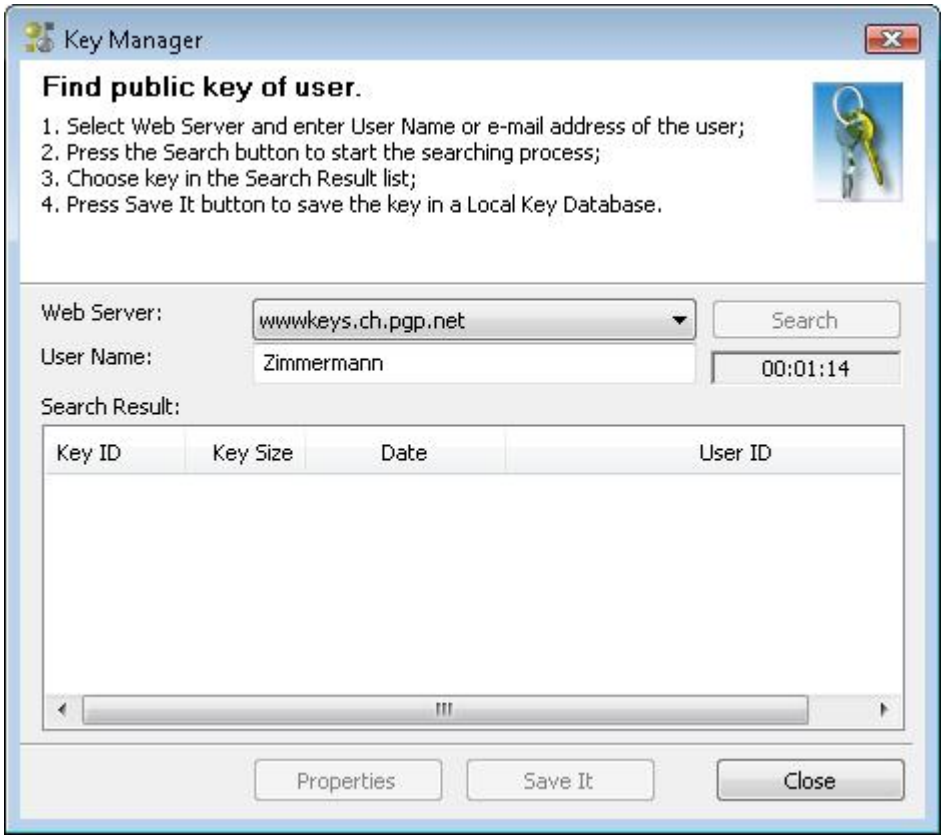
Add Public Key to Local Public Key Database

You can send compressed archive to another person encrypted by public key of the person. If you are going to send encrypted information to a person continuously, you should save the public key in your **Local Public Key Database**. To add a public key to the database use one of the following ways:

1. Load the key from file, where the public key is stored. The person, you are going to correspond with, can send you the file with his/her public key. Key Manager supports **PKCS 12** format as well as **Key Ring** format of the **Pretty Good Privacy (PGP)** software. To save public key from the file in one of the formats, run the Key Manager utility from BestCrypt Program Folder or from ***Utilities*** menu of BestCrypt Control Panel. Then run ***Add Existing Public Key -> Browse for File*** command from the ***Key*** menu and browse the file where the public key is stored. The following picture illustrates the method:



2. Your correspondent may have his/her public key stored on some **Public Key Server(s)** in Internet. In this case you can run the process of searching the public key in Internet. If you run the ***Add Existing Public Key -> Search in the Internet*** command from the ***Key*** menu, the following window will appear:



Select one of the Web servers where the public key may be stored in the **Web server** edit box, enter name of the person or his/her e-mail address in the **User Name** edit box and click **Search**. BC Key Manager will start to look for the user's public key and if there are a number of people whose names are the same as the name of your friend, BC Key Manager will display all of them in the Search result list. Select the string from the list, corresponding to the person you are looking for and click [**Save It**] to save the public key in your **Local Key Database**.

See also:

- Create or import Secret/Public Key Pair
- Send your public key to another person
- Backup/Restore Local Key Database

Backup/Restore Local Key Database

Local Public Key Database saves your time, because when you add public key of other user to encrypted container, you do not need in accessing Internet to download the public key again. It is recommended to backup (or export) the database file regularly and save the file on a reliable storage medium. If in future you decide to change your computer or reinstall the software, you can restore (or import) the database from the backup copy.

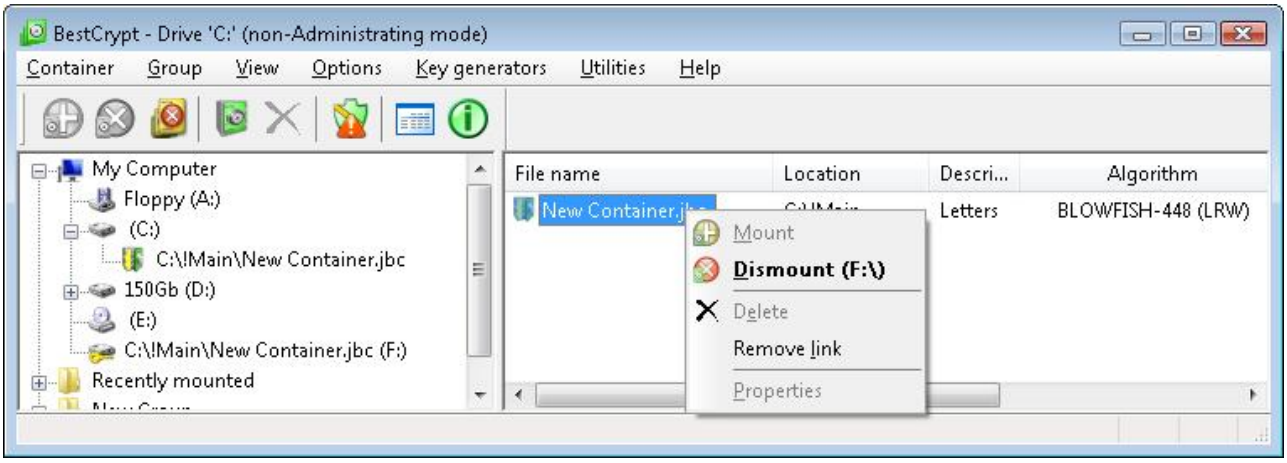
To **save (export)** Local Key Database run **Public Key Manager** utility from BestCrypt Program Folder or from ***Utilities*** menu of BestCrypt Control Panel. In the main window of the program run the ***Export to File*** command from the ***Database*** menu. BC Key Manager will ask you to enter path and name for the file where you want to save your **Local Public Key Database**.

To **restore** Local Key Database from earlier saved (exported) database, run the ***Import from File*** command from the ***Database*** menu. The program will ask you to enter path and name for the database file. After that BC Key Manager will copy the database to the folder where the software is installed and start to use the database you have imported.

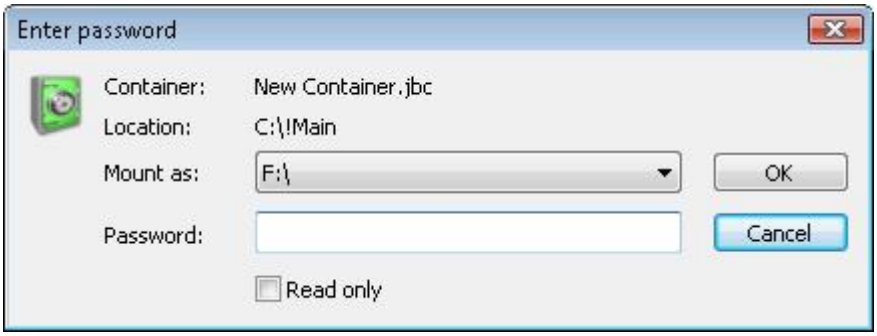
You can also **change the location** of the Local Key Database by running the ***Choose Store Folder*** command from the ***Database*** menu of the BC Key Manager utility.

What is the BestCrypt Data Encryption System?

BCTextEncoder is also distributed as a part of **BestCrypt Data Encryption System**.
BestCrypt Data Encryption System for Windows and Linux operating systems allows users to keep any form of data (files, letters, pictures, databases) in encrypted form on the hard disk, networks disks, removable disks, CD-ROM's and floppies. BestCrypt then lets user access it from any application.
Using **BestCrypt** you can create a container file (for example, you may create a 5Mbyte container file called LETTERS.jbc). Then you can mount this container as an additional logical drive: it will show up in Windows as an additional 5Mbyte virtual disk. When mounted, this logical drive looks and operates just like an ordinary disk drive: you can store your files on it. All files stored on the disk are automatically encrypted. Every read operation, which addresses the drive, causes decryption of the data, and every write operation causes encryption of data to be written. This approach is called transparent encryption. Using this system, your data are always stored in encrypted form and appear decrypted only in the application you use to process them, and only while they are being processed.
The following picture shows the **BestCrypt Control Panel**, used to perform all control operations (creating and mounting containers, setting BestCrypt options and so on):



BestCrypt uses encrypted logical disks technology to provide transparent encryption of your data. You only need to choose a drive letter and a password for your new **BestCrypt logical drive**. After password verification encrypted data become transparent for any pplication.



BestCrypt has a number of additional features like Keyboard Filter, Container's Guard Utility, HOTKEY and TIMEOUT options that allow a convenient work with encrypted data.
The common BestCrypt package contains additional utilities like BC Volume Encryption, wiping utility (BCWipe), compressed and encrypted archives (BCArchive) and BCTextEncoder.
We invite you to try a free trial of **BestCrypt** . You can download the fully-functional trial version of BestCrypt from our WWW-site:
http://www.jetico.com/download.htm

If You Want to Comment on the Software

If you have a product suggestion or comments on how to make BCTextEncoder documentation better, send us E-mail at this Internet address:
support@jetico.com

Be sure to include your name, e-mail, version number of BCTextEncoder. Please visit Jetico WWW-site to get information about our other products, Frequently Asked Questions lists, Download Evaluation Software page and other:

http://www.jetico.com

We are always trying to improve our products. User feedback is important and extremely valuable to the development team.
Thank you for your time!
Jetico Team