PrivaSuite Help Index

PrivaSuite is a Windows application designed to help you keep your documents safe.

Applications
PrivaMail - For encrypting E-mail and text documents
PrivaFile - For encrypting and compressing files
PrivaSoft - For encrypting Faxes (not available in PrivaSuite for the Internet version)

Tools
Keybook manager - Managing keybooks
Purchase - Purchasing PrivaSuite
PFileDOS - An MS-DOS program compatible with PrivaFile

Misc.
PrivaSuite SmartCard support
PrivaSuite FreeWare mode
PrivaSuite in OS/2
Technical support
About Aliroo LTD.

PrivaMail Help Index

PrivaMail is a Windows application for text security. It can encrypt and decrypt any text, in any language, in any Windows application. The encrypted text can be sent by any Email software.

Encrypting text

Decrypting text

Options

Keybook
Special Security Measures
PrivaMail encryption mechanism
Starting PrivaMail and Automatic Activation
Sending an encrypted E-mail to a non PrivaSuite user
Sending E-Mail using Microsoft Exchange or cc:Mail
Rich Text Format (RTF) and Foreign languages
Using DES
Using Private/Public keys
Multiple encrypted segments
TroubleShooting
PrivaSuite FreeWare mode
Purchase

The PrivaMail encryption mechanism

PrivaMail utilizes several encryptions engines:

1. A proprietary 40 bit engine
2. 56 bit DES engine
3. Private/Public engine

When encrypting with the 40 bit or the DES engines PrivaMail uses a symmetric key mechanism, where the encryption and the decryption are done with the same key. The key can be any alphanumeric string chosen by the encrypting party.

Encrypting with the Private/Public engine is done using a Private or a Public key. This key is used for encrypting a randomly chosen symmetric key which is then used for encrypting the text.

PrivaMail can also sign the message to verify its authenticity using a private key.

A clue for the key can be given to the recipient, to remind her/him of the correct key.

The encrypted text is limited to the 7 bit ASCII characters acceptable in Email correspondence. This feature enables sending text with multi-lingual characters (such as European or Far East languages) across the internet.

Following is an example of an encrypted text, beginning with the key-clue:

>|**Bens last name (6)**|%>@2`GWR5b5 OJGxo/ 3M+qjS Pd4ZFW qvyd/2 0Os9UR b194bb W58df4 YmKufx IlXgCw kwe3ud dZRxz4 NuNaVf J4ICJZ O9ecCb jYGK5C NIeCn1 o8yrVs GgV9hu n1NvBV Zi7a0m Rzj8+5 nTtukg Kw4FsJ OIjm2a JOiTf6 4TXGz5 DSlcQP 3zEiAs e3MW5o kgCCpo H18bZz n3cZKK 8rlGpH 22NJaa dtTcd5 i8Nc7X 7gWJqQ bCEKDm c5kMqK pWLaCw ICrkwP zcydTu 39y163 Guef7/ MEj/Tz vLo9I5 eEh7qQ p9uCWB cnfwg%|

See also:

DES

Private/Public

PrivaSuite FreeWare mode

Starting PrivaMail and Automatic Activation

PrivaMail can be started by double clicking on the PrivaMail icon in the PrivaSuite group. If PrivaMail is set for automatic activation (see tools/ Options), then PrivaMail will be called automatically when the user clicks the **Ctrl-c-c** in any application.

If you fail to activate PrivaMail by typing Ctrl-c-c, enter the Tools/Options menu, and turn the Auto-activate option off, click OK, re-enter the Options dialog, set the Auto-activate option ON and click OK.

Encrypting text

Selecting text to be encrypted
To encrypt text from your host application just copy it to the clipboard and activate PrivaMail from the Program Manager/Start menu.
If you are using the auto-activate feature, pressing Ctrl-c-c from your host application will automatically invoke PrivaMail.

To encrypt a text file use the File/Open menu directly from PrivaMail.

Supply an encryption key and key-clue.
The encryption key can be any alphanumeric string up to 25 characters. The key is case insensitive.
You may provide a key-clue to help the recipient recognize which key you have used.
You can store frequently used keys in the keybook.
If your version support DES, you can select whether to use DES encryption or not.

Note: You cant encrypt using a key from the keybook or use the DES or Private/Public algorithms when PrivaSuite is running in FreeWare mode.

After entering the key press Enter to encrypt the text.

Signing the message using a Private key
If your version supports Private/Public keys, you can sign the message with your private key for authentication.

Note: You cant sign the message when PrivaSuite is running in FreeWare mode.

Pasting the encrypted text back into the application
If you want the encrypted message to replace the original selected text, you can do a "paste" operation.
The encrypted text can be pasted into any other application, and can be pasted several times.
You can specify to paste the encrypted text automatically into the calling application by selecting Switch back & Paste in the After encryption Options.

Handling encrypted text
The encrypted text may be copied, duplicated, pasted to other applications, moved from one place to another etc. However, encrypted text must not be changed in any way.
Note: Encrypted text that has been modified will not be decrypted, and you may loose its contents.   Do not attempt to select parts of an encrypted segment for further encryption, or modify it manually by deleting or adding characters to it.

See also:
Keybook
Using DES
Using Private/Public keys
PrivaSuite FreeWare mode
Options
Special Security Measures
PrivaMail encryption mechanism
Starting PrivaMail and Automatic Activation
Sending an encrypted Email to a non PrivaSuite user
Sending E-Mail using Microsoft Exchange or cc:Mail
Rich Text Format (RTF) and Foreign languages
Multiple encrypted segments
Viewer
Saving to a file

Sending encrypted E-mail/Files to a user who does not have PrivaSuite

If you need to send an encrypted Email or encrypted files to a recipient who is not yet a PrivaSuite user, send along with it a small executable file named DECRYPT.EXE (in PRIVSUIT/BIN).
This application can decrypt text created by PrivaMail from the clipboard or from a text file and can decrypt files created by PrivaFile.

Sending encrypted E-mail/Files using Microsoft Exchange or cc:Mail

If your computer has a mail client which supports the MAPI (as **Microsoft Exchange**) or VIM (as

cc:Mail) standards the button will appear in the toolbar and the **File/Send...** menu option will be enabled.

Selecting to **Send** will create a message with the text currently in the clipboard (from PrivaMail) or with a file attachment (from PrivaFile) using your installed mail client software.

If you use this option often to send encrypted text, you might want to select the option that PrivaMail will not switch back to the calling application after encrypting or decrypting.

Rich Text Format (RTF) and Foreign languages

Encryption of RTF (Rich Text Format)

RTF is a text format used in MicroSoft Word and in other word processing applications. PrivaMail interprets RTF segments, separating the control strings from the data strings. The data strings are encrypted, while the control strings are left in their place, untouched. This unique feature, serves two important purposes:

1. The clear text to be encrypted does not contain long, predictable text strings that would otherwise make the encryption weaker.

2. The encrypted text maintains the text attributes, such as fonts, colors, justification etc., making the encrypted document resemble, as much as possible, the original text.

Note: The handling of RTF is diabled when PrivaSuite is running in FreeWare mode.

Note: Some applications use customized RTF control strings that are not familiar to PrivaMail. It is highly recommended that you try encrypting and decrypting text in your favorite application to gain confidence that PrivaMail can decrypt you RTF formats.

Important: If you want to copy an encrypted segment from a word processor to a plain text editor (such as your E-mail application) use the Copy and Paste feature.
Dont save the file as a plain ascii file and open it in the text editor because this may corrupt the encrypted segment contents.

Encryption of special characters and foreign languages

PrivaMail is a very effective tool for sending special characters and foreign languages over ordinary Email programs. Email is limited to 7 bit ASCII codes. This does not allow the transmission of text files that include special characters (such as à) as a part of the Email message. PrivaMail converts any text into the Email range of characters. This allows sending any text, in any language, as a regular Email note, without using attachments.

See also:
PrivaSuite FreeWare mode
TroubleShooting

Decrypting text

Selecting text to be decrypted

To decrypt text from your host application just copy it to the clipboard.

If you are using the auto-activate feature, pressing Ctrl-c-c from your host application will automatically invoke PrivaMail.

To decrypt a text file use the File/Open menu directly from PrivaMail.

Note: The selected area must contain the entire encrypted text, but may include some "safety margins" of clear text around it. In the following example, the encrypted text starts with the delimiter **>|** and terminates with the delimiter **%|**.

Upon reception or retrieval of >|**Bens last name (6)|**%>@2`GWR5b5 OJGxo/ 3M+qjS Pd4ZFW qvyd/2 0Os9UR b194bb W58df4 YmKufx IlXgCw kwe3ud dZRxz4 NuNaVf J4ICJZ O9ecCb jYGK5C NIeCn1 o8yrVs GgV9hu n1NvBV Zi7a0m Rzj8+5 nTtukg Kw4FsJ OIjm2a JOiTf6 4TXGz5 DSlcQP 3zEiAs e3MW5o kgCCpo H18bZz n3cZKK 8rIGpH 22NJaa dtTcd5 i8Nc7X 7gWJqQ bCEKDm c5kMqK pWLaCw ICrkwP zcydTu 39y163 Guef7/ MEj/Tz vLo9I5 eEh7qQ p9uCWB cnfwg%| at the beginning of the text, depress left

Determining the decryption key

The decrypting party has to know the decryption key. The key may be coordinated between the parties in advance, or the sending party can describe it using a private clue, that cannot practically be interpreted by strangers.

Automatic recognition of key-clues

If the key clue is identical to any of the keys in the keybook, then PrivaFile will recognize it automatically and place the correct key in the key field. In this case you do not need to type the key. If the "Protect key book" option is activated, then you will be asked to type in the keybook password before the key is extracted from the key book.

Pasting the decrypted text back into the application

If you want the decrypted message to replace the original selected text, you can do a "paste" operation. The decrypted text can be pasted into any other application.

You can specify to paste the decrypted text automatically into the calling application by selecting Switch back & Paste in the After decryption Options.

Note: Usually E-mail programs marks incoming mail as Read Only so you will not be able to paste the decrypted text back to the incoming message. Instead, you can use the PrivaMail viewer.

See also:
Keybook
Options
Special Security Measures
Starting PrivaMail and Automatic Activation
Rich Text Format (RTF) and Foreign languages
Multiple encrypted segments
Viewer
Saving to a file

Multiple encrypted segments

Multiple text segments in one document

You may select and encrypt multiple segments in the same document. The segments must be encrypted one at a time. Each segment can be encrypted with a different key. A segment to be encrypted may include any combination of clear and encrypted text.

Encrypting an encrypted text

If the selected text includes one or more encrypted segments, then PrivaMail will be set for decryption by default, but you have the option to ask to execute a further encryption, and after confirming that this is indeed the intention - PrivaMail will do a further encryption.

Note: You cant encrypt an encrypted text when PrivaSuite is running in FreeWare mode.

Note: The previously encrypted segments should be well contained within the selected segment.

Decryption of text with multiple encrypted segments

The selected text may contain any number of encrypted segments. These segments may use the same key or different keys. The number of encrypted segments found will be displayed at the left side of the screen, between the two triangular arrow buttons. PrivaMail will highlight the encrypted segments one by one, prompting you with the key clue for that segment and waiting for you to enter the key. When all segments have been decrypted, PrivaMail will notify on termination. If you do not know the key or do not want to encrypt a given segment, you may skip it by clicking on the triangular arrow buttons at the left side of the screen. This will scroll the encrypted text to the next (or previous) encrypted segment.

See also:
PrivaSuite FreeWare mode

At any point you can save the text (File/Save_as menu) in the clipboard to a text file.
If the text was copied from a word processor which supports RTF you may be able to save the text in RTF format. Click the **Save file as type:** combo box to see if RTF format is available.
Saving is also available from the Viewer.

Viewing the decrypted text

When the document containing the encrypted text is a "read only" document and can not accept a "paste" operation, or when you dont want to create a document with the decrypted text in it you can use the viewer.

The viewer allows viewing of the decrypted text, printing and saving it. You can delete the text from the clipboard by clicking on the "Delete" icon.

If you tend to use the viewer often you may opt to switch to the viewer automatically after decryption (in Tools/Options)

Special Security Measures

PrivaMail offers some measures to enhance the security of the user:

Encrypt Key-book
You can encrypt the keybook(see Keybook manager).

Use the DES encryption

Multiple keys
Do not use the same key for everybody. Determine specific keys for specific projects and specific recipients. PrivaMail unique key-clue system will protect you from "loosing the key".

Change keys often
Do not maintain one key for a long period. Changing the key is very easy, and the key-book relieves you from the need to memorize the keys. Frequent exchange of keys is a highly recommended measure of security.

Do not choose predictable keys
Keys like your name, your town, names of NBA stars or movie actresses are among the first keys that your opponent may guess. Do not use predictable keys. Better still - avoid using meaningful keys whatsoever. A short, meaningless key like SG20K17 is much better than a long but meaningful key like SHARON_STONE.

Do not use obvious key clues
A good key may be spoiled if described by an obvious key-clue. The key clue can be creative, but you have to be sure that nobody, but the recipient, will be able to interpret it. Clues like "the first 8 digits of Pi", "the day Kennedy was shot" or "The city of the 1996 Olympics" are very poor clues. Clues like "The last three words in the second paragraph of your last letter", "The telephone number of your mother-in-law" or "The serial number of the VCR I sold you" may be better.

Do not save decrypted messages
Decryption with PrivaMail is so easy, if you know the key, that you should think twice before replacing encrypted text in a document with its decrypted version. In most cases, the reasons for keeping it encrypted prevail after you read it. It is a good habit to read the encrypted text in the PrivaMail viewer. If you will ever need to read it again for reference - decrypt it again!.

Do not leave encrypted text in the clipboard
This is much less risky than saving the decrypted text, but is still something to be avoided if other people have access to your computer. You can delete the text from the clipboard before leaving the viewer. You can ensure that the clear message will not stay accessible by selecting the "Close after termination" option in the PrivaMail Tools/Options menu.

Wipe original after encryption
When you encrypt a file for file transfer purposes, you may want to leave the clear version of the file on your computer. However, when you encrypt a file for archiving purposes, you definitely do not want to leave a clear copy of the file on your disk - this will be a waste of file space and a breach of security. If you encrypt for archiving, you should use the "Wipe original after encryption" option (Tools/Options dialog box), to wipe the original file.
Moreover, very often in the course of handling a file, you create - deliberately or accidentally - more than one copy of the file in few directories. You may want to see if there are any copies of the file left. This can be done by typing the following DOS command in the route directory:
C:\ dir filename*.* /s

PrivaMail Options

Notify completion using
This controls how PrivaMail will notify you upon successful encryption/decryption.

After encryption
Stay in PrivaMail - After encryption the focus will remain in PrivaMail. Useful if you want to send the encrypted text directly using your mail client.

Switch Back - After encryption the focus will return to the calling application.

Switch Back & Paste- After encryption the focus will return to the calling application and a CTRL-V (Paste) will be performed.

Close PrivaMail - PrivaMail will close after encryption.

After decryption
View in PrivaMail - The Viewer will be automatically called after decryption. Usefull when reading encrypted E-mails that cant be pasted back.

Switch Back - After decryption the focus will return to the calling application.

Switch Back & Paste - After decryption the focus will return to the calling application and a CTRL-V (Paste) will be performed.
Note: Usually E-mail programs marks incoming mail as Read Only so you will not be able to paste the decrypted text back to the incoming message. Instead, you can use the **View in PrivaMail** option.

Close PrivaMail - PrivaMail will close after decryption.

Misc.

Auto Activate
PrivaMail can be automatically activated if you copy the same text twice to the clipboard in less than two seconds. This effect can be achieved by pressing CTRL-C-C.
If you fail to activate PrivaMail by typing Ctrl-c-c enter the Tools/Options menu, and turn the Auto-activate option off, click OK, re-enter the Options dialog, set the Auto-activate option ON and click OK.
Add Key structure to the Keyclue - If this option is enabled the key structure will be added to the keyclue. ex.: For the key BIG_BEN the keyclue will be added with (3+3).
The key structure will not be added if no keyclue is specified.
Limit encrypted line - If your E-mail program has problems to deal with long lines, you can limit the line length of the encrypted segment. A value of Zero (the default) means no limit.

Using DES

PrivaSuite DES version implements the DES-CBC symmetric encryption engine as specified in the U.S. Department of commerce FIPS PUB 46-2 .
This version can be distributoed freely in the U.S., Canada and Israel and to financial institutions (banks, insurance companies etc.) worldwide.

In the DES enabled version a 'DES' checkbox is added next to the key field in PrivaMail and PrivaFile. To encrypt the text/file using DES-CBC check this box. Leave the box clear to encrypt using the international 40 bit engine.

When decrypting the DES checkbox will automatically reflect whether the encrypted text/file was encrypted using DES.

See also:
Managing keys in the keybook

Private/Public keys

The Private/Public modules are under development.

Trouble Shooting

You are using the WRONG KEY
You have inserted the wrong key. Check the key clue to verify that you have entered the correct key and re-type it.

The encrypted text is illegal... error message
The encrypted text was altered after its creation. If you accidentally added or deleted the encrypted segment undo the changes. If you didnt change anything you should ask the sending party to re-encrypt the message and sent it again.
Note: When re-sending an encrypted message via E-mail, some E-mail programs add a mark (usually the > character) to the beginning of each line. PrivaMail skips any > character but if anything else was added (such as IP>) then the decryption will fail unless you delete this added characters yourself.

RTF limitations:
Cant paste encrypted text back into a table.
There are two ways to encrypt text in a table:
To encrypt the entire table, make a selection from one line above the table to one line below it.
To encrypt a single cell in the table, select the text inside the cell and not the entire cell itself.

Cant paste decrypted text back into a table.
Select from one line above the table to one line below it.

When decrypting a segment with the right key the Encrypted text is illegal error message sometimes appears.
You usually get this message if the encrypted segment was created in a word processor, then saved as an ascii file and opened by your E-mail program..
If you want to encrypt a segment from a word processor and then sent it by E-mail you should do one of the following:
1. Select the area in your word processor, encrypt it and Paste it directly to the E-mail application.
2. If the segment is already encrypted, Copy and Paste it directly to the E-mail program.
Dont save the file as a plain ascii file and open it in the text editor because this may corrupt the encrypted segment contents.

PrivaFile Help Index

PrivaFile is a Windows application for file security and economy. It can encrypt & compress any file. It is a part of the PrivaSuite privacy software package. PrivaFile is useful in file transfers and in digital archiving.

Encrypting a file

Decrypting a file

Options

Keybook

Special Security Measures

Sending an encrypted Email to a non PrivaSuite user

Sending Files in E-Mail using Microsoft Exchange or cc:Mail

PrivaSuite FreeWare mode

Purchase

Encrypting files

Selecting file/s to be encrypted
The file/s to be encrypted are selected using tools similar to the standard Windows tool for file selection. You can select multiple files by holding down the CTRL key and repeatedly pressing the left mouse button.
In Windows 95, if you are using the auto-activate feature, pressing Ctrl-c-c when a file is selected in the explorer will automatically invoke PrivaFile.
You can select to encrypt an entire directory (including its subdirectories) by selecting the All files of specified type check box.

Choosing a name for the encrypted file/s
You can choose (Tools/Options) between automatic naming, manual naming and original naming. The automatic name will be the original name of the file, with the extension ".cry". If the file with the .cry extension already exists, you will be asked to confirm the file name.

Choosing the location of the encrypted file/s
The encrypted file/s can be created in the same directory where the original file/s are located, or in a different directory. This option is specified in the (Tools/Options) dialog box.

Supply an encryption key and key-clue.
The encryption key can be any alphanumeric string up to 25 characters. The key is case insensitive.
If your version support DES, you can select whether to use DES encryption or not.
You may provide a key-clue to help the recipient recognize which key you have used.
You can store frequently used keys in the keybook.
Note: You cant encrypt using a key from the keybook or use the DES or Private/Public algorithms when PrivaSuite is running in FreeWare mode.

Signing the file using a Private key
If your version supports Private/Public keys, you can sign the file with your private key for authentication.
Note: You cant sign the message when PrivaSuite is running in FreeWare mode.

Triggering the encryption
The selected file will be encrypted when you click on Encrypt tool-bar icon.
Note that you can choose to wipe the original file after encryption in the Tools/Options dialog box.
A message box will notify you that the encryption has been completed and the new file has been created.

See also:
Keybook
PrivaSuite FreeWare mode
Options
Special Security Measures
Sending an encrypted Email to a non PrivaSuite user
Sending Files in E-Mail using Microsoft Exchange or cc:Mail

Decrypting files

Selecting file/s to be decrypted
Double clicking a file with the CRY extension in Windows File Manager or Windows 95 Explorer will automatically activate PrivaFile.
Selection of a file for decryption is done using tools similar to the standard Windows tool for file selection. Only one file can be decrypted at a time.
Note that you can use the file filter to display only *.CRY files, making it very easy to recognize the encrypted files.
You can select to decrypt an entire directory (including its subdirectories) by selecting the All files of specified type check box.

Checking the "ID Card" of the encrypted file
The original file name and its size are displayed in the status bar and the key clue is displayed in the Key clue field. Additional information such as the date and time of encryption and the encryptor users name is

presented in the File/Info dialog box   . This information is useful for handling of the file by users who are not authorized to decrypt it.

Determining the decryption key
The decrypting party has to know the decryption key. The key may be coordinated between the parties in advance, or the sending party can describe it using a private clue, that cannot practically be interpreted by strangers.

Automatic recognition of key-clues
If the key clue is identical to any of the keys in the keybook, then PrivaFile will recognize it automatically and place the correct key in the key field. In this case you do not need to type the key. If the "Protect key book" option is activated, then you will be asked to type in the key-book password before the key is extracted from the key book.

Choosing a name for the decrypted file/s
You can choose (Tools/Options) between automatic naming, manual naming and original naming. The automatic name will be the original name of the file. If a file with the same name already exists, you will be asked to confirm the file name.

Choosing the location of the decrypted file/s
The decrypted file can be created in the same directory where the original file is located, or in a different directory. This option is specified in the (Tools/Options) dialog box.

Triggering the decryption process
The decryption is triggered by clicking on the Decrypt icon in the tool-bar.
A message box will notify you that the encryption has been completed and the new file has been created.

See also:
Keybook
Options
Special Security Measures
Sending an encrypted Email to a non PrivaSuite user

PrivaFile Options

Open decrypted file
If the decrypted file is associated with an application (ex.: DOC file is associated with Microsoft Word) PrivaFile can open the document in that application.
You can select to:
No - Never open the decrypted file
Ask - If an association exists, ask if you want to open the decrypted file
Yes - If an association exists open the decrypted file without asking

File management
Wipe original file after encryption - If enabled will wipe the original file after the encryption process is complete. This is good practice when you are encrypting files for archiving purposes.
Delete encrypted file after decryption - If enabled will delete the encrypted file after the decryption process is complete. This is good practice when the decrypted file was sent to you by E-mail/FTP.

File naming
Automatic (.cry/original name) - If selected, PrivaFile will try to use the .CRY extension when creating encrypted files and the original name when creating decrypted files. If a file by that name already exists, you will be asked to confirm the file name.
Prompt for destination file name - If selected, PrivaFile will always ask you for the name of the newly created encrypted file (when encrypting) and the name of the decrypted file (when decrypting).
Same as source name - If selected, the created encrypted/decrypted file will have the same file name as the source file. Note that if decrypting an .CRY extension, PrivaFile will try using the original file name instead.

File Location
Source directory - If selected, files will be created at the same directory where the original files are located.
Prompt for output directory - If selected, PrivaFile will prompt the user for the location of the created files.

Misc.
Compress files
PrivaFile can compress the file before encrypting it to conserve disk space and transmission time.
Never - Never compress
If not with extension -Files with the specified extensions will not be compressed when encrypted. This is usefull when encrypting files which are already compressed such as ZIP, ARJ, JPG, GIF etc. You can add/remove file types from the list.
Always - Always compress

Note: Compression is disabled when PrivaSuite is running in FreeWare mode.

Add Key structure to the Keyclue - If this option is enabled the key structure will be added to the keyclue. ex.: For the key BIG_BEN the keyclue will be added with (3+3)
The key structure will not be added if no keyclue is specified.

Key Clue

The **Keyclue** is a short sentence intended to help the recepient of the messages understand which key was used for encryption.

When decrypting in PrivaMail or PrivaFile the keybook is searched for a key matching the encrypted text/file keyclue. If one is found, it is automatically placed in the Key field.

The keyclue can be a reference to a key list (i.e.: Key #12 in April key list), a logical name (i.e.: Ben Smith Public key), a reference to a fact known to both parties (i.e.: Place where we met) etc.

Note that using a trivial key/keyclue combination may disclose the key to an unwanted third party.

Here are some Key / Key Clue combinations. The Strength column represents how easy it is to a third party to decrypt the message using the keyclue.

Key	Key Clue	Strength
Bill_Clinton	USA President	Easy
spaghetti	my favorite food	Medium
Holland	last vacation	Medium
970135	Old phone number	Medium
05893-53457	Key #12 in our list	Impossible
FAPFKEG…	Ben Smith Public key	Impossible

PFileDOS

PFileDOS is an MS-DOS program for encrypting and decrypting files.

Its format is compatible to that of PrivaFile so that files encrypted with PrivaFile can be decrypted by PFileDOS and vice-versa.

PFileDOS does not support Private/Public encryption but there is a version which support DES.

PFileDOS can be run either from a batch file with command line switches or interactively.

When executing the program the command line switches are displayed on screen for reference.

To use a keybook with PFileDOS you will need to generate it using the keybook wizard. The keybook itself is a simple text file with the following structure:

line 1 : a no. designating the default line number to use when no key is specified

line 2 - … : a key record <Key>,<Key clue>

Keybook

Using Keybooks

For convenience, frequently used keys and key-clues can be stored in keybooks, and called upon when needed.

Calling an entry from the key book will place the key in the "key" field, and the key-clue in the "key clue" field. The keybook may also have a default key which will be placed in the Key field upon activation.

Note: You cant encrypt using a key from the keybook when PrivaSuite is running in FreeWare mode.

See also:

Keybook Manager

Keybook Manager

The Keybook Manager lets you maintain keybook files.
You can create as many keybooks as you want and place them anywhere on your local, network or floppy drives.

You can have many keybooks open simultaneously, enabling you to easily move keys from one keybook to another using the cllipboard or drag and drop.
Upon startup the quick access menu and the quick access toolbar buttons are set to the keybooks specified in the keybooks connections dialog.
To switch between the open keybook use the Window menu option.

See also:
Creating, Loading and Saving a keybook
Keybook options
Keybook security options
Managing keys in the keybook
Creating a Private/Public key pair
Using the clipboard
Importing/Exporting keys
Key Wizard
Keybook Connections
Downloading remote keybooks

Smartcards:
PrivaSuite SmartCard support
Keybook SmartCard options
Initializing SmartCard keybook

Creating, Loading and saving keybooks

The keybook manager allows you to manipulate many keybooks simultaneously, enabling you to easily move keys from one keybook to another using the cllipboard or drag and drop.
Upon startup the quick access menu and the quick access toolbar buttons are set to the keybooks specified in the keybooks connections dialog.
To switch between the open keybook use the Window menu option.

To create a new keybook select File/New keybook from the menu or click the □ button.
To load a keybook select File/Open a keybook from the menu or click the 📂 button.
To save the current keybook select File/Save from the menu or click the 💾 button.
To save the current keybook under a new name select the File/Save as… from the menu.
To close the current keybook select File/Close from the menu or click the 📁 button.
To access the keybook on a SmartCard select 'View/Smartcard' from the menu or click the 🔲 button.

Managing keys in the keybook

The keys in the keybook are displayed in the list in three columns: Description, Key and Keyclue.
If your PrivaSuite version supports <u>DES</u> a small bitmap will be denoting the encryption engine to be used with the key:
40 - 40 Bit engine
DES - 56 Bit DES key

If your PrivaSuite version supports <u>Private/Public keys</u> a small bitmap will be displayed denoting the encryption method used with the key:
On - Symmetric encryption
PUB On - Encryption with a Public key
PRV On - Encryption with a Private key

When editing a keybook on a <u>SmartCard</u> the key can be preceeded with on of the following bitmaps:
- Key is encrypted and cannot be modified until the encryption key is submitted.
- Key is kept encrypted on the SmartCard but can currently be modified (encryption key submitted)
- Key is protected and cannot be modified until the protection key is submitted.
- Key is kept protected on the SmartCard but can currently be modified (protection key submitted)

To add a symmetric key select the Edit/Add menu option, or click the ✚ toolbar button, or click the right mouse button over the list and select Add.
Each symmetric key record contains:

Description:	Text describing the key. ex.: Key for George
Key:	The actual key (5-25 characters)
Key clue:	The keyclue
DES (where applicable):	Use DES encryption
E-mail:	A strings (with wildcards) with e-mail addresses

To create a <u>Private/Public</u> key pair look at <u>Creating a Private/Public key pair</u>
To Edit a key select the key in the list, then select Edit/Edit menu option, or click the ↘ toolbar button, or click the right mouse button over the key and select Edit.

To Delete keys select them in the list, then select Edit/Delete from the menu, or click the ✗ toolbar button, or click the right mouse button and select Delete.

Each symmetric key record contains:

Description:	Text describing the key. ex.: Key for George
Key:	The actual key (5-25 characters)
Key clue:	The keyclue
DES (where applicable):	Use DES encryption
E-mail:	A strings (with wildcards) with e-mail addresses

The keybook may also have a **default key** which will be placed in the Key field upon activation.

When decrypting in PrivaMail or PrivaFile the keybook is searched for a key matching the encrypted text/file keyclue. If one is found, it is automatically placed in the Key field.

If the keybook is **encrypted**, you have to enter the keybook password whenever you enter PrivaMail, PrivaFile, PrivaSuite or the Keybook manager itself.

If the keybook is **protected**, you have to enter the protection password whenever you will want to change the keybook entries.

You can **export** the keybook as a simple text file in the following format:
Description,Key,Key clue,DES <CR/LF>

You can **Import** entries to the keybook from a simple text file in the same format used for exporting (see above).

All changes to the keybook will be done after you select to **Save** the keybook. If you have made a mistake you can select to **Exit** and discard the changes.

Creating a Private/Public key pair

To create a Private/Public key pair select the Edit/Private-Public/Create from the menu.
You will be asked to enter the Keyclue and Description for both the Private and the Public keys as well as the E-mail address and whether you want to use DES with those keys.
After select the length of the key (in bits) go to the buttom field and start typing. The contents of what you type as well as the interval between the keystrokes will be used as input to the key creation algorithm.
After you have typed enough characters click the Create button for creating the Private/Public key pair.
Note that this is a lengthy process which may take up to a few minutes (depending on the type of CPU you have and the length of the keys).

Using the clipboard and drag-and-drop in the Keybook Manager

You can use the clipboard or the drag-and-drop feature for transferring keys between the keybooks currently opened in the keybook manager and with other applications.

To copy symmetric keys select them in the keybook manager and press Ctrl-C.

To copy a Private or Public key select the key and select the Edit/Private-Public/Copy key to clipboard menu option.

To paste the keys into a different keybook or into a word processor/spread sheet application switch to the keybook/application and press Ctrl-V.

Example of three symmetric keys copied to the clipboard and pasted into a wordprocessor:

Example1	CBR600	My motorcycle	Y
Example2	6873-6974-1021	Key no. 19 in January list	N
Example3	CINDY_CRAWFORD	Your last key	N

Keybook Options

Encrypt only with keys from keybook

   If this option is enabled you will be able to encrypt only with keys from the keybook. This prevents key typing errors and unauthorised encryption when combined with the Protected update option.

Download remote keybooks

   Specify how often you want to download remote keybooks to your computer.

Default key

   Select how to choose the default key from the current keybook.

See also:

Keybook Security Options
Keybook SmartCard options
Downloading remote keybooks

Keybook Security Options

Protected Update
> This option allows you to protect the keybook from unauthorized/accidental modification.
> While the keybook is protected you wont be able to add, edit or delete entries.
> Also, the key field in the keybook manager will not display the key.
> To allow modification of the keybook without removing the protection select Edit/Unprotect and enter the password.
> **Note:** . If you forget the password you can select to Reset the keybook which will remove the password but will also **DELETE THE KEYBOOK**.

Encrypt keybook
> Since the keybook contain your keys, youll probably want to secure it. You can encrypt the keybook by selecting this option.
> You will be asked to provide the password whenever youll enter PrivaMail, PrivaFile, PrivaSoft or the Keybook Manager.
> **Note:** . If you forget the password you can select to Reset the keybook which will remove the password but will also **DELETE THE KEYBOOK**.

Ask for password
> Select how often youll need to enter the keybook password

Keybook Connections

To open the keybooks connections select the View/Connections menu option or click the 🔳 button.
In this screen you specify which keybooks you want to appear in the keybook list in PrivaMail, PrivaFile and PrivaSoft.
You can connect to keybooks anywhere on your computer, on your diskette drive or on a network drive (Providing that you have a read permission).
Each time you start one of these programs a connection is made to the keybooks and its contents is loaded to memory.
The order of the keybooks in this list is the order of their appearance in the keybooks list.
The first keybook in the list is the main keybook. If this keybook has a default key, it will be selected upon activation.

See also:
Keybook Download

Keybook Import/Export

You have several ways in which you can share your keys with another user and import another users keys into your keybooks.

You can export keys from your keybooks in one of two ways:
1. Create a new keybook; use the clipboard to copy the keys you want to export from their original keybooks to the newly created keybook; save the keybook and send it to whomever you want.
   Note that for copying a <u>Private or a Public key</u> you will have to use the Edit/Private-Public/Copy key to clipboard and Edit/Private-Public/Paste key from clipboard menu options rather than the normal Copy (CTRL-C) operation.
2. Export the contents of the keybook to a text file.
   Each record in the export file has the following structure:
   <Description>,<Key>,<Key clue>,<E-mail>,<DES (Y/N)
   To export a subset of the keybook select the keys you want to export before selecting the **Export** operation.
   To export the entire keybook select a single key before selecting the **Export** operation.
   Note that you cant export a <u>Private or a Public key</u>.

To import keys into your keybooks
1. If you received a new keybook open it and use the clipboard for transferring the keys into your keybooks.
   Note that for copying a <u>Private or a Public key</u> you will have to use the Edit/Private-Public/Copy key to clipboard and Edit/Private-Public/Paste key from clipboard menu options rather than the normal Copy (CTRL-C) operation.
2. If you received a keybook export file use the File/Import menu option to import the keys into one of your keybooks.

Keybook Download

To open the keybooks download select the View/Download menu option or click the button.
If you are using keybooks which are stored on a remote computer you can use the download dialog to automatically copy the remote keybooks to your computer.
This will ensure that if you are disconnected from the network you will still have all the relevant keybooks and keys at your disposal.
After you specify which keybooks to download and where you will need to create connections   to them on your local drive.
For example, if your company keys are stored at H:\KEYBOOKS you can specify a download operation from H:\KEYBOOKS*.KBK to C:\PRIVSUIT\KEYBOOKS.
If you are using the keybooks MARKET.KBK and MANAGE.KBK you will have to specify the following connections: C:\PRIVSUIT\KEYBOOKS\MARKET.KBK and C:\PRIVSUIT\KEYBOOKS\MANAGE.KBK.
You can specify when the download operation will be performed in the keybook options screen.

See also:
Keybook Connections
Keybook Options

Keybook Wizard

The keybook wizard lets you create lists of keys automatically.
To activate the keybook wizard select a keybook and select Edit/Key wizard from the menu or click the right mouse button and select Key wizard.

You can create several types of key lists:
Keys for this keybook - The list will be automatically added to the current keybook
Keybook import file - Creates a text file that can be <u>imported</u> to a keybook
For printing - Creates a text file which is suitable for printing and storing in your wallet etc.
For PFileDOS - Creates a text file which can be used by <u>PFileDOS</u> program.

You then specify some the key list title and no. of key groups and keys in a group as well as the structure of each key record.

Click Create to create the key list. If a text file was created you will be asked whether you want to view it.

PrivaSuite SmartCard Support

PrivaSuite can use SmartCards for storing keybooks.
That keybook is managed by the Keybook Manager and is accessed by PrivaSuite applications as a regular keybook.

Two important differences between a regular keybook and a smartcard keybook are:
1. Before using the smartcard keybook and should be initialized and it's maximum size need to be determined.
2. Each key in the smartcard keybook can has it's own security level (Protected, Encrypted or both)

PrivaSuite currently supports the following smartcard readers:
A. Litronic Argus 210 serial
B. SCM SwapSmart PCMCIA
C. Schlumberger Reflex 20 PCMCIA
D. Schlumberger Reflex 60 serial

And the following cards:
A. Schlumberger Multiflex 3k/8k
B. Schlumberger Cryptoflex

See also:
Keybook SmartCard options
Initializing SmartCard keybook

SmartCard options

Enable SmartCard keybooks
> Check this option to activate PrivaSuite SmartCard support.

Access reader on startup
> Because accessing the SmartCard is a time consuming operation the SmartCard is not accessed when any of the PrivaSuite applications is started.
> Instead, when the user selects the SmartCard keybook for the first time the card is accessed and the keybook is retrieved.
> Check this option if you want the smartcard keybook to be retrieved upon application startup.

Reader Type and Port
> Select the type of your reader and, if applicable, it's COM port.
> Check PrivaSuite SmartCard support for the list of supported readers.

Card Type
> Select the type of your card you are using. It is recommended that you'll set this options on 'Auto Detect' unless automatic detection for your card fails.
> Check PrivaSuite SmartCard support for the list of supported cards.

See also:
Initializing SmartCard keybook

Initializing SmartCard Keybook

Before using the SmartCard for the first time it should be initialized.
During the initialization process you will be asked to state how much memory to allocate for the keybook on the card.
Be aware that the only way to change this value is to remove the keybook completely which will result in the loss of all the keys in it so choose this value carefully.

You will need to consider the following typical memory requirements for your keys.
Note: Key size varies depending on the length of the key (for symmetric keys), the keyclue, decription and E-mail address.

Symmetric key
A typical symmetric key needs approx. 40 bytes.

Private/Public key

Key strength	Private	Public
512 bits	340 bytes	110 bytes
768 bits	490 bytes	150 bytes
1024 bits	630 bytes	180 bytes

If you do not plan to your your card for any other applications it is recommended you allocate 100 bytes less than the maximum amount available on the card, leaving some free space for additional applications that you might want to use in the future.

Otherwise, initialize the card after you have setup the other applications so that they will allocate their own space prior to the keybook setup process.

Note: Depending on the card type, you might have to submit a PIN/Transport key before initializing the keybook. If the card requires a PIN/Transport you will be asked for it. You can submit the PIN/Transport in either plain text or in hexadecimal digits.

Manufacturer's Name Plate

Manufacturer's name: **Aliroo Ltd.**

HQ

Address: Aliroo Ltd.
P.O.B. 178,
Kefar-Sava 44442, Israel

Tel. administration: (972) 9-7677732
Tel. technical support: (972) 9-7677732 (Ext 21)
E-Mail: support@aliroo.com
WEB: http://www.aliroo.com
Fax: (972) 9-7677739

Export license: 100-62482
U.S. export license: CCATS #43531

Patent pending.
PrivaSuite,PrivaSoft,PrivaMail,PrivaFile and PrivaSee are trademarks of Aliroo Ltd.

Technical support

For technical support contact your local distributor whose details appear in the **Distrib.wri** file found in the PrivaSuite BIN directory.

If additional technical assistance is required you can also contact <u>Aliroo</u> directly.

PrivaSuite in OS/2

PrivaSuite can run in a Windows3.1 window in OS/2 .

When in a Windows 3.1 OS/2 window PrivaSuite operates normally, including the Ctrl-C-C auto activation feature.
However, on some systems PrivaFile may cause an error when activated. To fix this, add the line OS2=1 to the [Path] section in the text file scramble.ini found in PrivaSuite BIN directory.

When running an OS/2 application you can still use PrivaMail for encrypting text through the clipboard.
To enable this you should change your OS/2 clipboard settings to Public so that native OS/2 applications and Windows 3.1 applications will be able to share data through the clipboard.
Look at Information / Windows programs in OS/2 on how to do that.
Note that the auto-activate feature will not work from a native OS/2 application.

Purchasing PrivaSuite

To purchase PrivaSuite activate the purchase application.
You can activate it either from the Tools & Docs icon in the PrivaSuite group or by selecting
Tools/Purchase in PrivaMail, PrivaFile or PrivaSuite.

Purchasing is done by contacting a PrivaSuite distributor by phone, fax or E-mail.
(The distributor contact details will appear in the Phone and Fax/E-mail screens).

After giving the distributor the relevant information (Your name, Credit card no. etc.) you will be given a
license no. to be entered in the screen.
This license no. is unique for the computer and is generated from the **Local ID** no. which is displayed on
the screen.

────────
See also
PrivaSuite FreeWare mode

PrivaSuite FreeWare Mode

When installing PrivaSuite for the first time on a computer PrivaSuite operates in **Demo mode**.
In this mode PrivaSuite offers you all of its features, but you get a limited amount of encryption attempts in PrivaMail, PrivaFile and PrivaSoft.
Once this limit has been reached the application switches to **FreeWare mode**.
In FreeWare mode each application disables some of its features relevant to encryption, but you can still encrypt and decrypt everything.
To benefit from all of PrivaSuite features after the applications switches to FreeWare mode youll need to purchase PrivaSuite.

Here is a list of the features not available when running in FreeWare mode:
General:
You wont be able to select a key from the keybook when encrypting (You will still be able to use the keybook for decryption)
Encryption will be done only with the 40 bit international mechanism. You wont be able to use DES encryption or Private/Public encryption or signing (You will still be able to decrypt messages encrypted using DES or Private/Public providing you have the DES or Private/Public modules).
PrivaSuite SmartCard support will be disabled.

PrivaMail specific:
You wont be able to encrypt text segments larger than 500 Bytes.
The encrypted text will lose its RTF attributes (**Bold**, *Italic* etc.)
You wont be able to re-encrypt an encrypted segment.

PrivaFile specific:
Files will not be compressed when encrypted.
Files larger than 150Kb will not be encrypted.

PrivaSoft specific:
The head separator between the clear and encrypted parts is fixed at 2 inches.
Only a single page can be scrambled at a time.

Eudora plugin specific:
Automatic encryption using the **To:** field will be disabled

_____
See also
Purchase

PrivaSoft Help Index

PrivaSoft is a Windows application for encrypting and decrypting faxes.

General
How PrivaSoft encrypts faxes
PrivaSuite FreeWare mode
Purchase

Applications
PrivaSoft Scrambler - Scrambling fax documents
PrivaSoft Descrambler - Descrambling fax documents
PrivaSoft printer driver
PrivaSoft Feeder - Aquiring images from files or TWAIN scanner for scrambling/descrambling

How Do I…
Encrypt and send a fax
Receive and decrypt a fax

PrivaSoft Feeder

PrivaSoft Feeder is a separate application to be used together with the PrivaSoft Scrambler and Descrambler.

The feeder enables you to submit documents that are already in graphic file format to the scrambler or descrambler without using the host application.
The feeder can also scan a document directly to the scrambler or descrambler.

To use the feeder, click the PrivaSoft Feeder icon in the PrivaSoft program group. The PrivaSoft Feeder window will appear.

Open the file you want to scramble or descramble
From the **File** menu choose **Open** or click on the open button and select the file you want to scramble or descramble.

You may select the type of file you want to open (**BMP**, **DCX, PCR** or multiple **PCX**) from the **File** menu or from the selection box in the browse window.

Note the total number of pages in the document is displayed in the **Total pages in document** field.

You can view the document by clicking the View... button. This will open the viewer program which is the same as the viewer program in the Scrambler and Descrambler programs.

When you have made all the required selections, click the **Scramble** button to start the scrambling operation or the **Descramble** button to start the descrambling operation. The PrivaSoft Scrambler or Descrambler window will appear.

Scan Document
If your computer is equipped with a TWAIN compatible scanner the feeder can directly scan documents from the scanner. Select the scan paper size and the total number of pages to be scanned and select the **Scramble** button or the **Descramble** button to start the scanning operation.
If you are scanning a multi page document you will be prompt for feeding the next page into the scanner.
Once all the pages have been scanned the PrivaSoft Scrambler or Descrambler will be activated.

How the Feeder works

How the feeder works

Normally you would scramble or descramble a document starting from some host application (e.g. MS Word, Excel, WinFax etc.).

At times when the file is already available in graphic format, such as when you save a file from PrivaSoft or your Fax program you can use the PrivaSoft Feeder.

If you have a hard copy of the document you wish to scrambler/descramble and a TWAIN compatible scanner it is easier to use the feeder to scan the document and send it to the scrambler/descrambler than to do it in some other application.

If the input image is sent to the descrambler the feeder performs some operations on the image which enhances the quality of the descrambled image.

PCR File format
PCR is a proprietary multi-page graphic file format used by Aliroo LTD.
PCR files are 40% smaller on average than **PCX/DCX** files.
It is recommended to use this format when you wish to save a scrambled/descrambled document on disk.
You can use the PrivaSoft Feeder to view **PCR** files, save as as PCX or print them to the scrambler or descrambler.

PrivaSoft Printer Driver

The PrivaSoft Scrambler/Descrambler Printer Driver is a virtual driver used for transferring documents to the PrivaSoft Scrambler and Descrambler.

To scrambler a document simply print it to the PrivaSoft Scrambler printer driver, much like you print it to a regular printer driver.
After printing the PrivaSoft Scrambler main screen will come up.

To descrambler a document simply print it to the PrivaSoft Descrambler printer driver.
After printing the PrivaSoft Descrambler main screen will come up.

The driver has a setup screen where you can set the following properties:
Page size: A4, Letter or B4. Note that some applications (such as MS-Word) ignore this value and use the document page size when printing.
Orientation - Portait or Landscape
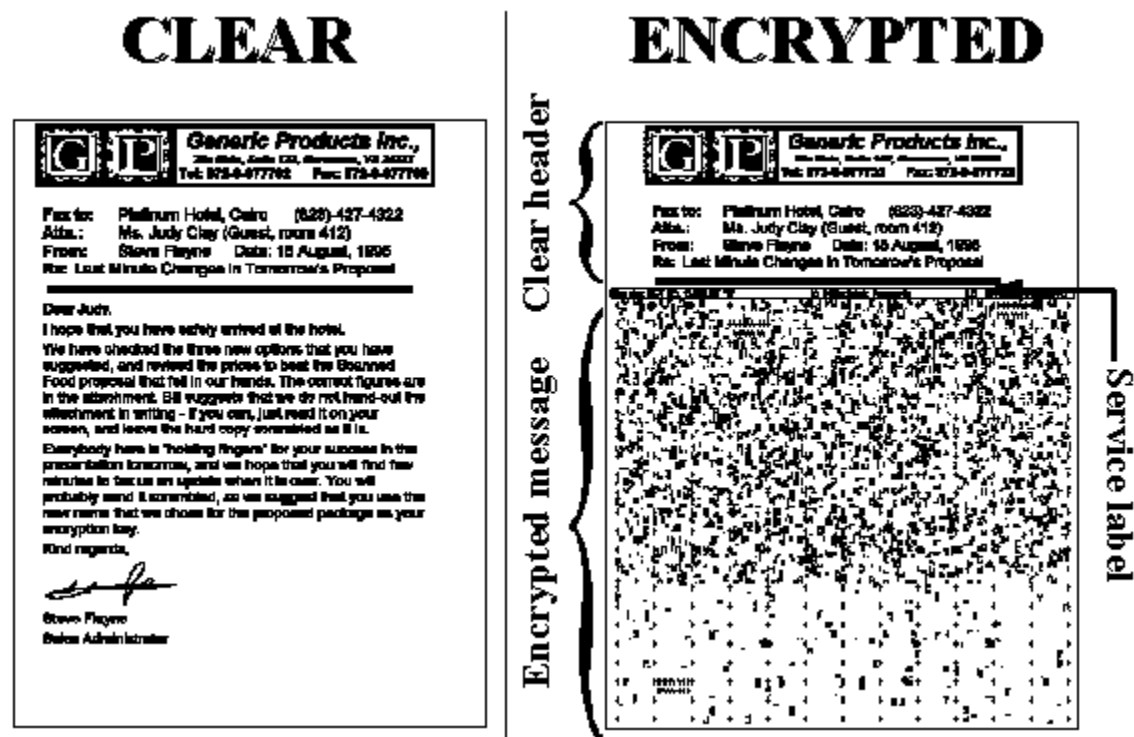**Resolution** - Normal (200* 100 DPI) or Fine (200 * 200 DPI)

How PrivaSoft encrypts faxes

PrivaSoft encrypts images by deviding the image into small tiles and rearranging them using a permutation calculated using the encryption key and key extension.

Since it is usually desirable to leave the top portion of the page whicih contains fax routing information clear the user can specify from where to encrypt the image. Between these two areas PrivaSoft adds a service label which contains the key clue and other information fields.

PrivaSoft needs to find the position of every such tiles when decrypting the image. Because during fax transmission lines may get lost and the page may be rotated and skewed PrivaSoft adds cross marks ✛ inside the scrambled area to help it syncronize on the tiles positions.
PrivaSoft also adds three areas of marks in the scrambled area that encodes data on the image (which page layout was used, version numbering etc.) .

Because these marks and serveice label occupy a portion of the output scrambled image it is possible that the combination of the original data on the image and the PrivaSoft data will not fit inside the page. In such cases PrivaSoft shrinks the original data so everything will fit inside the page.

When decrypting, PrivaSoft searches for its marks on the page and extrapolates the tiles positions from finding the embedded cross marks ✛. Using the same key and key extension PrivaSoft rearranges the tiles in the reverse order to reconstruct the original image.

It is important to understand that due to fax transmission, rotated or skewed images and differences between fax machines and fax printer drivers the reconstructed image will differ slightly from the original image.

See also
Set scrambling area

<u>Handling Tips</u>
<u>Service label</u>

PrivaSoft Scrambler

After you have printed a document to the <u>PrivaSoft Scrambler driver</u>, the PrivaSoft Scrambler main window will appear.

Supply an encryption key and key-clue.

The encryption key can be any alphanumeric string up to 25 characters. The key is case insensitive.
You may provide a <u>key-clue</u> to help the recipient recognize which key you have used.
You can store frequently used keys in the <u>keybook</u>.
Note: You cant encrypt using a key from the keybook or use the DES or Private/Public algorithms when PrivaSuite is running in <u>FreeWare mode</u>.

Specify what to do after scrambling (Scramble and…)

You need to specify what you want to do with the scrambled image.
You can Fax or print it to any device, print the original image for filing or save the image to disk.
To speciy the output devices click on the **<u>Set Devices</u>** toolbar button. A dialog box where you can change the output devices as well as set their parameters will open.

Set scrambled area position

You can change the position of the separator which separates the clear header from the scrambled part by clicking the **<u>Set area</u>** toolbar button.

Scramble

To scramble press the **Scramble** toolbar button.
A progress window will come up showing you the status of the encryption process.
In this window you can select to cancel the operation or modify the View and confirm option.

View and confirm

If you have selected to view and confirm the scrambling result you will be presented with the scrambled image on screen for verification. Check that the unscrambled part of the image does not contain any sensitive information and that you have indeed used the correct key.
You can also modify the scrambled output destination by clicking the **Select destinations** button.
If you are satisfied with the result click the **OK** button, otherwise click the **Cancel** button.

Sending the output image

After scrambling (and, optionally, confirming) the scrambled image will be handled according to what you have specified.
Once this is done PrivaSoft Scrambler will terminate.

See also
<u>PrivaSuite FreeWare mode</u>
<u>Options</u>
<u>Set devices</u>
<u>Set scrambling area</u>
<u>Service label</u>

Service Label

The **service label** is printed automatically on each scrambled page between the header and the body of scrambled information.

```
Key clue : My favorite food                 0
```

```
By : Demo Version       1/1.   ©Aliroo   00000
```

The label contains the following fields:
Key clue - The keyclue of the scrambling key
Key extension - The key extension of the key (0 - 99)
By - User name
Page of page - This page number
Aliroo copyright notice
User serial number

Scramble Options

The Scramble Options window lets you configure various settings for the Scrambler's operation.
Open the Scramble Options window by clicking on the **Options...** button in the Scrambler window. When
you have made the selection, click the **OK** button to return to the Scrambler window.

General Options
Confirm on view
Use the View and confirm option when you want to make sure the document has been scrambled
properly before you send it to any of the output destinations.

You can override the current **'View and confirm'** selection during the scrambling process by clicking the
'View and confirm after completion' check box in the scrambling progress window.

When the scrambling process has ended, the scrambled document will appear in the viewer.

Click **OK** if you are satisfied with the scrambling results and wish to continue.
Click **Cancel** if the scrambled image is not to your liking and you wish to terminate the process.
Click **Set destinations** to change the Scrambler output destinations.

Generate key extensions
Select if you want to use the key extension mechanism.

Add Key structure to the Keyclue
If this option is enabled the key structure will be added to the keyclue. ex.: For the key BIG_BEN the
keyclue will be added with (3+3)
The key structure will not be added if no keyclue is specified.

Default entries
You can specify the default file name and file type for saving the scrambled image.
Save file format can be PCX, DCX, BMP or PCR.

See also
Alerts

Scrambling Alerts

PrivaSoft scrambler can alert if your document has not been <u>properly handled</u>.
The process includes several tests. You can activate or suppress any of these tests.
An alert report is generated, summarizing the outcome of the enabled tests.

These tests include:
PrivaSoft Scrambler set to 'Normal'
Warns if the the scrambler is in 'Normal' resolution mode.

Small font size
Warns if a font size smaller than 12 was used extensively in the document. A smaller font is not generally recommended for fax correspondence.

Serif font type
Warns if an unrecommended font type (such as MS-Serif) was used in the document.
Sans-Serif fonts are generally recommended for fax correspondence.

Header separator runs through data
Warns that the header separator is probably misplaced and is running through some data and not through a white line.

Page size is not consistent OR landscape orientation was used
Warns if output printer or fax device is set to landscape orientation or when its paper size does not match the paper size used for scrambling (Letter or A4).

Suppress all alerts
Suppress all alerts.

––––––––
See also
<u>Handling Tips</u>

Key extension
A key extension is a two digit number which is automatically added to the scrambling key.

This option is especially useful when you use the default key often and want to retain a high level of immunity against cracking of the key and in this way, increase the security of your document.

The key extension is displayed on the <u>Service Label</u> in the scrambled document.

When descrambling you will have to enter the key extension number in the key extension field.

Tips for obtaining better image quality after descrambling:

When scrambling:
Fax scrambled pages using 'Fine' (detail) mode.
Use a large font (12 and up)
Use a sans serif font (Arial, MS Sans Serif, CG-Omega etc.)
Make sure that the same paper size definition (A4, Letter etc.) is used throughout the scrambling chain - Host application, PrivaSoft Scrambler and destination device (Fax or Printer).
You can change the page size definition of PrivaSoft Scrambler in the 'Printer Setup' option usually found in the 'File' menu.
When sending the scrambled document avoid rotating the page when feeding it to the fax machine.

When descrambling:
Receive scrambled pages using 'Fine' (detail) mode.
Avoid page rotation when scanning the document. (e.g.: If using a fax machine for scanning avoid rotating the page when feeding it to the machine.)
Make sure that the same paper size definition (A4, Letter etc.) is used throughout the descrambling chain - Host application, PrivaSoft Descrambler and destination device (Fax or Printer).
You can change the page size definition of PrivaSoft Descrambler in the 'Printer Setup' option usually found in the 'File' menu.
For better automatic scale adjustments -
A. In your host application (typically a fax software) - save the incoming scrambled doucment.
B. Use PrivaSoft Feeder to open the saved file.
C. Send the file to the descrambler.

General Tips
Include the header separator in your word processor template.
Use the 'View and confirm' option to verify results.

_____

See also
Alerts

Device Setup

You can change the fax and printer drivers used for sending the output documents.

To change one of the drivers, click the **Devices** button in the main window. When the **Device Setup** window appears, select the required driver for the device you want to change.

Changing the fax driver
Select the fax driver you want PrivaSoft to use from the list of available printer drivers.

Changing the printer driver
Select the printer driver you want PrivaSoft to use from the list of available printer drivers.

You can configure the individual settings for each device by clicking the **Setup** button. The selected printer driver's options menu will be displayed. Consult the appropriate user's guide regarding the required settings for the specific printer driver.

Setting the scrambled area

Use the scrambled area dialog to specify the clear header and the scrambled part of the document.

To change the separator position
Position the mouse on the solid line between the Clear label and the Scrambled label.
Click the left mouse button, drag the mouse up or down and release the button.
You can also set the separator position by changing the Default position value in the Separator details group.
You can specify different separator locations for up to the first ten pages of the document.
The following pages (11 - …) will be scrambled using the separator position of the tenth page.
To set the separator position for the current page and for all consequent pages position the mouse over the ▼ arrow, click the mouse left button and drag the line to the desired position.

Note: When PrivaSuite is running in FreeWare mode, the separator is fixed at 2 inches.

Scramble from page
If your document starts with pages that should be left clear (such as a fax header page) you can specify which will be the first page to be scrambled.
The pages preceeding this page will be left clear.

Ignore separation mark
PrivaSoft can scan the input image for the $\perp$ character. If it encounters 20 such characters in a single line it places the separator line on that line. This feature enables you to created a document with different separator positions for every page.
However, since this operation involves heady processing it is recommended that if you dont use this feature check the Ignore separaion mark to speed up the encryption process.

Note: When PrivaSuite is running in FreeWare mode, this option is always enabled.

Maintain aspect ratio when shrinking page
Because PrivaSoft adds it own data to the scrambled image it is sometimes necessary to shrink the input image so that it would fit into the scrambled image.
Check this option if you want to maintain the aspect ratio of the document when shrinking it.

How to encrypt and send faxes

To encrypt and send a fax:
1. Compose the fax in any application (Word processor, Spreadsheet etc.)
2. Print the document to the **PrivaSoft Scrambler** printer driver. (Make sure that the page size of the document corresponds to the page size of the PrivaSoft Scrambler driver)
3. When the PrivaSoft Scrambler window appears, enter the key and the keyclue.
4. You can change the position of the separator which separates the clear header from the scrambled part by clicking the **Set area** toolbar button.
5. Select what to do with the scrambled image by clicking on any of the **Scramble and…** check boxes. To speciy the output devices click on the **Set Devices** toolbar button.
6. Click the **Scramble** toolbar button

How to decrypt faxes and images

To send the scrambled fax/image to the PrivaSoft Descrambler:
1. If you received the scrambled fax directly into your computer using a fax software, print the fax from the fax software to the **PrivaSoft Descrambler** printer driver.
2. If you have the scrambled image on paper on you have a scanner use the **PrivaSoft Feeder** to scan the image and send it to the PrivaSoft Descrambler.
3. If you have the scrambled image on paper on you have a fax modem, fax the paper from a regular fax machine to your computer and print the fax from the fax software to the **PrivaSoft Descrambler** printer driver.

After the PrivaSoft Descrambler windows appears:
1. Select the descrambling key using the keyclue.
2. Select what to do with the scrambled image by clicking on any of the **Scramble and…** check boxes. To speciy the output devices click on the **Set Devices** toolbar button.
3. Click the **Descramble** toolbar button

PrivaSoft Descrambler

After you have printed a document to the <u>PrivaSoft Descrambler driver</u>, the PrivaSoft Descrambler main window will appear.

Supply a decryption key
The <u>Service label</u> is automatically detected and displayed in the descrambler window at the beginning of the descrambling process.
Use the scroll bar to view the <u>Key Clue</u> and <u>Key extension</u> that appear on the service label.
If the scrambled pages are too distorted, or if you printed a regular (non-scrambled) document to the descrambler, the message "Could not find Key clue area" will be displayed instead of the service label.

Use the keyclue to determine which key was used for scrambling and enter the same key for descrambling.
You can store frequently used keys in the <u>keybook</u>.

Specify what to do after descrambling (Descramble and…)
You need to specify what you want to do with the descrambled image.
You can Fax or print it to any device, print the original scrambled image for filing or save the image to disk.
To speciy the output devices click on the **<u>Set Devices</u>** toolbar button. A dialog box where you can change the output devices as well as set their parameters will open.

Descramble
To descramble press the **Descramble** toolbar button.
A progress window will come up showing you the status of the decryption process.
In this window you can select to cancel the operation or modify the View and confirm option.

View and confirm
If you have selected to view and confirm the descrambling result you will be presented with the descrambled image on screen for verification.
You can also modify the descrambled output destination by clicking the **Select destinations** button.
If you are satisfied with the result click the **OK** button, otherwise click the **Cancel** button.

Sending the output image
After descrambling (and, optionally, confirming) the descrambled image will be handled according to what you have specified.
Once this is done PrivaSoft Descrambler will terminate.

See also
<u>Options</u>
<u>Range</u>
<u>Set devices</u>
<u>Service label</u>

Descramble Options

The Descramble Options window lets you configure various settings for the Descrambler's operation. Open the Descramble Options window by clicking on the **Options...** button in the Descrambler window. When you have made the selection, click the **OK** button to return to the Descrambler window.

General Options
Confirm on view
Use the View and confirm option when you want to make sure the document has been descrambled properly before you send it to any of the output destinations.

You can override the current **'View and confirm'** selection during the descrambling process by clicking the **'View and confirm after completion'** check box in the descrambling progress window.

When the descrambling process has ended, the descrambled document will appear in the viewer.

Click **OK** if you are satisfied with the descrambling results and wish to continue.
Click **Cancel** if the descrambled image is not to your liking and you wish to terminate the process.
Click **Set destinations** to change the Descrambler output destinations.

Nose removal
Select the **Noise removal** option when you want to clean up small lines and dots that may appear as a result of the fax transmission process.

Default entries
You can specify the default file name and file type for saving the descrambled image.
Save file format can be PCX, DCX, BMP or PCR.

See also
Alerts

Range

Use the **Range** setting to descramble only some of the pages from a multiple page document. Select **Range...** from the **Document** menu in the descrambler window.

The **Descramble range** dialog box will appear.

In the dialog box, select **All** to descramble all pages of the document. This is the default setting. To descramble only a range of pages, select **Pages** and enter the index number of the first and last page you wish to descramble. Note that the index numbers of the scrambled pages appear in the Service label.

Descrambling Alerts

PrivaSoft descrambler can alert if your document has not been <u>properly handled</u>.
The process includes several tests. You can activate or suppress any of these tests.
An alert report is generated, summarizing the outcome of the enabled tests.

These tests include:
Excessive image rotation
Warns if the image is rotated more than desired under normal circumstances.

Excessive image scaling
Warns if the image was scaled more than desired under normal circumstances.

Distortion or damaged image
Warns if the image is distorted

Page size is not consistent or landscape orientation was used
Warns if the output printer device is set to landscape orientation or its paper size does not match the paper size used for scrambling (Letter or A4).

Suppress all alerts
Suppress all alerts.

_____

See also
<u>Handling Tips</u>

PrivaMail Plugin for Eudora

PrivaSuite has a plugin for Eudora E-mail software that enables easy text encryption and decryption.
To use the plugin you need to have Eudora Version 3.0.1 or higher.
Download the Eudora plugin from Aliroos web page and copy it to the Eudora PLUGINS directory.

Plugin encryption features
Plugin decryption features
Plugin options

Eudora Plugin Encryption Features

The plugin can encrypt a message in two ways:

On Demand
Encrypts the text immediately, replacing the clear text with the encrypted text
To encrypt a message place the cursor inside the message text.
If you want to encrypt a selection from the message select it, otherwise the entire message will be encrypted.
Select the **PrivaMail encrypt/decrypt** plugin from the Edit/Message plug-ins menu option.
If the message contains a PrivaMail encrypted segment the plugin will behave as if you requested to decrypt the message.

If the **Encrypt automatically using recepient name** option is selected the plugin will try to encrypt the text automatically using the **To:** address as reference. If there is a key record in a keybook which E-mail entry correspondes to the **To:** address it will be selected as the encryption key.

Note: This feature is disabled when PrivaSuite is running in FreeWare mode.

If the plugin cant encrypt the message automatically the plugin dialog will appear and will ask you to provide the key for encryption.

After encryption the encrypted text will replace the original text of the message.

On Transmission
Encrypts the entire text message (including the signature) when it is sent to your mail server.

If the **Encrypt automatically using recepient name** option is selected the plugin will try to encrypt the text automatically using the **To:** address as reference. If there is a key record in a keybook which E-mail entry correspondes to the **To:** address it will be selected as the encryption key.

Note: This feature is disabled when PrivaSuite is running in FreeWare mode.

If the plugin cant encrypt the message automatically the plugin dialog will appear and will ask you to provide the key for encryption.

Note that your copy of the outgoing message will not be encrypted.

See also:
Managing keys in the keybook
Plugin options

Eudora Plugin Decryption Features

To decrypt a message select the **PrivaMail encrypt/decrypt** plugin from the Edit/Message plug-ins menu option.

If the message does not contain a PrivaMail encrypted segment the plugin will behave as if you requested to <u>encrypt</u> the message.

If the **<u>Try to decrypt automatically using keyclue</u>** option is selected the plugin will try to decrypt the text automatically.

If the plugin cant decrypt the message automatically the plugin dialog will appear and will ask you to provide the key for decryption.

After decryption the decrypted text will replace the original (encrypted) text of the message.
When you will close the message Eudora will ask you whether you want to save the changes; Select Yes if you want the message to be kept with the decrypted text.

See also:
<u>Managing keys in the keybook</u>
<u>Plugin options</u>

Eudora Plugin Options

To access the plugin options, Select the Special/Message plug-ins settings menu option.
When the plug-ins dialog appears, select the PrivaSuite plugin and click Settings….

Encrypt on send - This sets options relevant to the On Transmission Action
Encrypt every outgoing message by default
Select this option if you want that every message you compose will be encrypted when it transmitted to your mail server.
You will still be able to set that a specific message will not be encrypted by clicking on the Plugin selection

 button of the message.

Dont encrypt if message already contains an encrypted segment
If you encrypt a segment in the message and the PrivaMail Encrypt On Transmission action is selected this options determines whether in such case the message will indeed be encrypted when it is transmitted to your mail server.

Encrypt/Decrypt on demand - This sets options relevant to the On Request Action
Encrypt automatically using recepient name
If the **To**: field contains an E-mail address that can be matched agains a key record in a keybook then that key will be used for encrypting the text and the encrypted text will automatically replace the clear text.
Note: This feature is disabled when PrivaSuite is running in FreeWare mode.

Try to decrypt automatically using keyclue
If the encrypted text keyclue can be matched agains a key record in a keybook then that key will be used for deencrypting the text and the deencrypted text will automatically replace the encrypted text.

Notify after automatic encryption/decryption
If automatic encryption or decryption was used a message box will appear after the encrypt/decrypt operation.

Add [and **] around decrypted text**
Since after decryption you have no way of knowing whether a specific text in a message was once encrypted you instruct the plugin to add the [** and **] text around the decrypted text.

Add decryption detail after decrypted text
This option will add the decryption detail (User name and date/time of decryption) after the decrypted text.