PrivaMail 3.1™

for Windows* ™ *3.1 (or higher)

Quick Reference Guide

Made by Aliroo, Ltd. (972)9-7677732 E-mail:support@aliroo.com

- For a message from your PrivaSuite distributor please check the **DISTRIB.WRI** file in the bin directory.

Product License Agreement

The information contained in this documentation is subject to change without notice. Aliroo makes no warranties with respect to this documentation. Aliroo assumes no responsibility for errors within the documentation. No part of this book may be reproduced or transferred in any form or by any means without the written consent of Aliroo, Ltd.

Aliroo Ltd.
Product License Agreement

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS PRODUCT.

THE USE OF PRIVASUITE TO ENCRYPT OR DECRYPT TEXT FILES OR DOCUMENTS INDICATES THE USER'S ACCEPTANCE OF THESE TERMS AND CONDITIONS.

PRIVASUITE IS LICENSED FOR USE BY A SINGLE USER ON A SINGLE COMPUTER. THE USER MAY CREATE A COPY FOR BACKUP PURPOSES ONLY. THE USER MAY REPRODUCE AND SHARE WITH CORRESPONDENTS INTRODUCTION COPIES OF THE PRODUCT CREATED SOLELY BY USING THE DOWNLOADING PROCEDURE DESCRIBED IN THIS MANUAL.

DISCLAIMER OF LIABILITY

NOTWITHSTANDING ALIROO LTD.'S UTILIZATION OF HIGH QUALITY CONTROL MEASURES IN THE DEVELOPMENT AND PRODUCTION OF PRIVASUITE, ALIROO DOES NOT GUARANTEE THAT THE USE OF THE PRODUCT WILL BE ERROR-FREE. ACCORDINGLY, ALIROO LTD. SHALL NOT BE LIABLE FOR ANY DAMAGES, HOWEVER CAUSED, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS INFORMATION OR PROFITS, LOSS OF PRIVACY OR OTHER LOSSES ARISING FROM THE USE OR INABILITY TO USE PRIVASUITE.

Introduction.

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.

The PrivaMail encryption mechanism

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.

A version which will use 56 bit DES and Private/Public key mechanism is currently under development.

The encrypted text is limited to the 7 bit ASCII characters acceptable in Email correspondence. A clue for the key can be given to the recipient, to remind her/him of the correct key. The key / key-clue mechanism is common to the all three parts of PrivaSuite. See detailed explanation of the key / Key-clue mechanism in the PrivaSoft guide.

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

```
=>=>| [ Where we met ] @<%>@1K*J$OB#3!U$ lct!9#1$Wv !sF$I!w7$E
y1dB!dt$ql !yt$hN4i!s $je!5$I!yt $fnx#3$o#0 !akD$SL!7$ gmzzb!R$J5 aq#1!
P$iaF I!s$K!d#0! t$Ci!0$htD z7!c%|~|%
```

Starting PrivaMail

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, then OK, and then turn it on again, and then OK again.

Text encryption

Selecting text to be encrypted

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

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

Enter an encryption key and key-clue.

The encryption key can be any alphanumeric string 5-25 characters long.

You can also provide a key-clue to help the recipient recognize which key you have used. The key clue will be clearly displayed at the beginning of the encrypted segment.

Here are some handy Key / Key Clue combinations:

Key	Key Clue
def-gol-gud-bik	Key No. 23 in our list
Atlanta	City of 1996 Olympics
john lennon	Late beatle (4+6)

Using a key-book

For convenience, frequently used keys and key-clues can be stored in keybooks, and called upon when needed. Calling an entry from a keybook 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 of PrivaMail.

You can encrypt the contents of the keybook (see the Keybook Manager for further details).

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.

Saving the encrypted text to a file

You can save the text to a file (File/Save_as menu) from the main PrivaMail screen or from the viewer.

Sending an encrypted Email to a user who doesn’t have PrivaSuite

If you need to send an encrypted Email to a recipient who doesn’t have PrivaSuite, send along with it a small executable file named DECRYPT.EXE (in PRIVSUIT/BIN). Instruct the recipient to follow these instructions:

> Parts of this Email are encrypted for our privacy. If you do not have PrivaMail installed, copy the message to the clipboard and run the DECRYPT.EXE program attached to this Email. The PrivaMail Decryptor will display a clue to the key used in the encryption. Type the secret key and hit ‘Decrypt’. This decryptor will decrypt one encrypted segment at a time.

It is much more convenient to use the full PrivaSuite package for decryption and encryption of text. The recipient can download a copy from the PrivaSuite web site (http://www.aliroo.com) , or you can create a PrivaSuite setup diskette using your Tools/Download option and send him a diskette.

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

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.

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: 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.

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.

Text decryption

Selecting text to be decrypted

To decrypt text from your host application just copy it to the clipboard.
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 **%|~|%**.

```
|--------- Safety Margin --------|
Upon reception or retrieval of =>=>|[city where we met ] @<%>@1[$KFa^jM
#2^#4m)@K zZT?)<Z Ae6Kj[ 6CJZx)M jw@h#1B V#4i3Ql )DuRPAn #0g):`m1
(7uni3C [o^(9_[ )@L@:yJ cKZWvs J:PP@)7 #3m)>fKG Yqe#1a3 Ol=WIT
8ZR9DU #2)2GE^X HNLUG0 dyNM`; #2alcWT Jv)8Lu3 ]fZ)6PH n#4&aNS_
ZWJ)Jb L#1ss);%|~|% at the start.
                                             |- Safety Margin -|
```

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 keybooks, then PrivaMail 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.

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.

Viewing the decrypted text

The decrypted text is automatically placed in the clipboard, and can be viewed and used in several ways:

1. Pasted back into the host application, replacing the encrypted text. Note that if the selected area for decryption included some extra text - before and after the encrypted text - these text margins will return to their original place.
   You can specify to paste the decrypted text automatically into the calling application by selecting ‘Switch back & Paste’ in the ‘After decryption’ Options.
2. Pasted into an open document in another application.
3. Viewed in the PrivaMail viewer (click on the viewer icon). This is useful when the document containing the encrypted text is a "read only" document, and can not accept a "paste" operation. 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:

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 Tools/Options menu.