MailAgent Pro 1.1

Table of Contents

Net.Dreams ELECTRONIC END-USER LICENSE AGREEMENT FOR ONE COMPUTER

NOTICE TO USER: THIS IS A CONTRACT. USE OF THIS SOFTWARE CERTIFIES THAT YOU HAVE READ THE LICENSE AGREEMENT AND ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

This Net.Dreams End User License Agreement accompanies a Net.Dreams software product ("Software") and related explanatory written materials ("Documentation"). The term "Software" shall also include any upgrades, modified versions, updates, additions, and copies of the Software licensed to you by Net.Dreams. This copy of the Software is licensed to you as the end user or your employer or another third party authorized to permit your use of the Software. "You" as used in the remainder of this License Agreement refers to the licensee. The "Permitted Number of Computers" as used in the remainder of this License Agreement is one (1) unless you have a written agreement which specifies otherwise.

Net.Dreams grants to you a nonexclusive license to use the Software and Documentation, provided that you agree to the following:

1. Use of the Software. You may install the Software in a single location on a hard disk or other storage device on a single computer. You may make one backup copy of the Software, provided your backup copy is not installed or used on any computer.

2. Copyright and Trademark Rights. The Software is ownned by Net.Dreams and its licensors. The structure, organization, and code of the Software are the valuable trade secrets of Net.Dreams and its licensors. The Software is also protected by United States Copyright Law and International Treaty provisions. You must treat the Software just as you would any other copyrighted material, such as a book. You may not copy the Software or the Documentation, except as set forth in the "Use of the Software" section. Any copies that you are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on or in the Software. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software. Trademarks shall be used in accordance with accepted trademark practice, including identification of trademark owner's name. Such use of any trademark does not give you any rights of ownership in that trademark. Except as stated above, this Agreement does not grant you any intellectual property rights in the Software.

3. Transfer. You may not rent, lease, sublicense or lend the Software. You may, however, transfer all your rights to use the Software to another person or legal entity provided that you transfer this Agreement, the Software, including all copies, updates and prior versions, and all Documentation to such person or entity and that you retain no copies, including copies stored on a computer.

4. Multiple Environment Software/Multiple Language Software/Dual Media Software/Multiple Copies. If the Software includes, or, in connection with the acquisition of the Software you receive, two or more operating environment versions of the Software (e.g. Macintosh® and Windows™), two or more language translation versions of the Software, the same Software on two or more media (e.g., diskettes and a CD-ROM), and/or you otherwise receive two or more copies of the Software, the total aggregate number of computers on which all versions of the

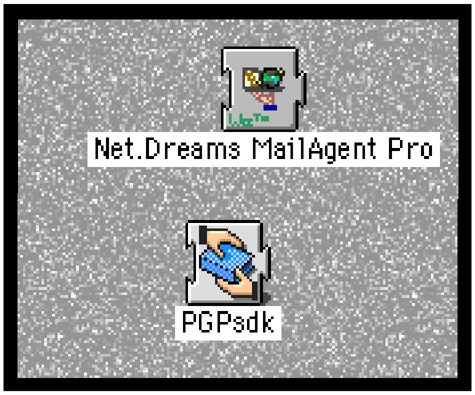
Software are used may not exceed the Permitted Number of Computers. You may make one back-up copy, in accordance with the terms of this Agreement, for each version of the Software you use. You may not rent, lease, sublicense, lend or transfer versions or copies of the Software you do not use, or Software contained on any unused media, except as part of the permanent transfer of all Software and Documentation as described above.

5. Limited Warranty. Net.Dreams warrants to you that the Software will perform substantially in accordance with the Documentation for the ninety (90) day period following your receipt of the Software. To make a warranty claim, you must return the Software to the location where you obtained it along with a copy of your sales receipt within such ninety (90) day period. If the Software does not perform substantially in accordance with the Documentation, the entire and exclusive liability and remedy shall be limited to either, at Net.Dreams' option, the replacement of the Software or the refund of the license fee you paid for the Software. Net.Dreams AND ITS LICENSORS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE OR DOCUMENTATION. THE FOREGOING STATES THE SOLE AND EXCLUSIVE REMEDIES FOR Net.Dreams' OR ITS LICENSORS' BREACH OF WARRANTY. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, Net.Dreams AND ITS LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL Net.Dreams OR ITS LICENSORS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR SPECIAL DAMAGES, INCLUDING ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN Net.Dreams REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY THIRD PARTY. Some states or jurisdictions do not allow the exclusion or limitation of incidental, consequential or special damages, or the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to you. To the extent permissible, any implied warranties are limited to ninety (90) days. This warranty gives you specific legal rights. You may have other rights which vary from state to state or jurisdiction to jurisdiction. For further warranty information, please contact Net.Dreams' Customer Support Department.

6. Governing Law and General Provisions. This Agreement will be governed by the laws in force in the State of California excluding the application of its conflicts of law rules. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms. You agree that the Software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations. This Agreement shall automatically terminate upon failure by you to comply with its terms. This Agreement may only be modified in writing signed by an authorized officer of Net.Dreams.

Net.Dreams, 6050 Commerce Blvd., Suite 208, Rohnert Park, California, USA.

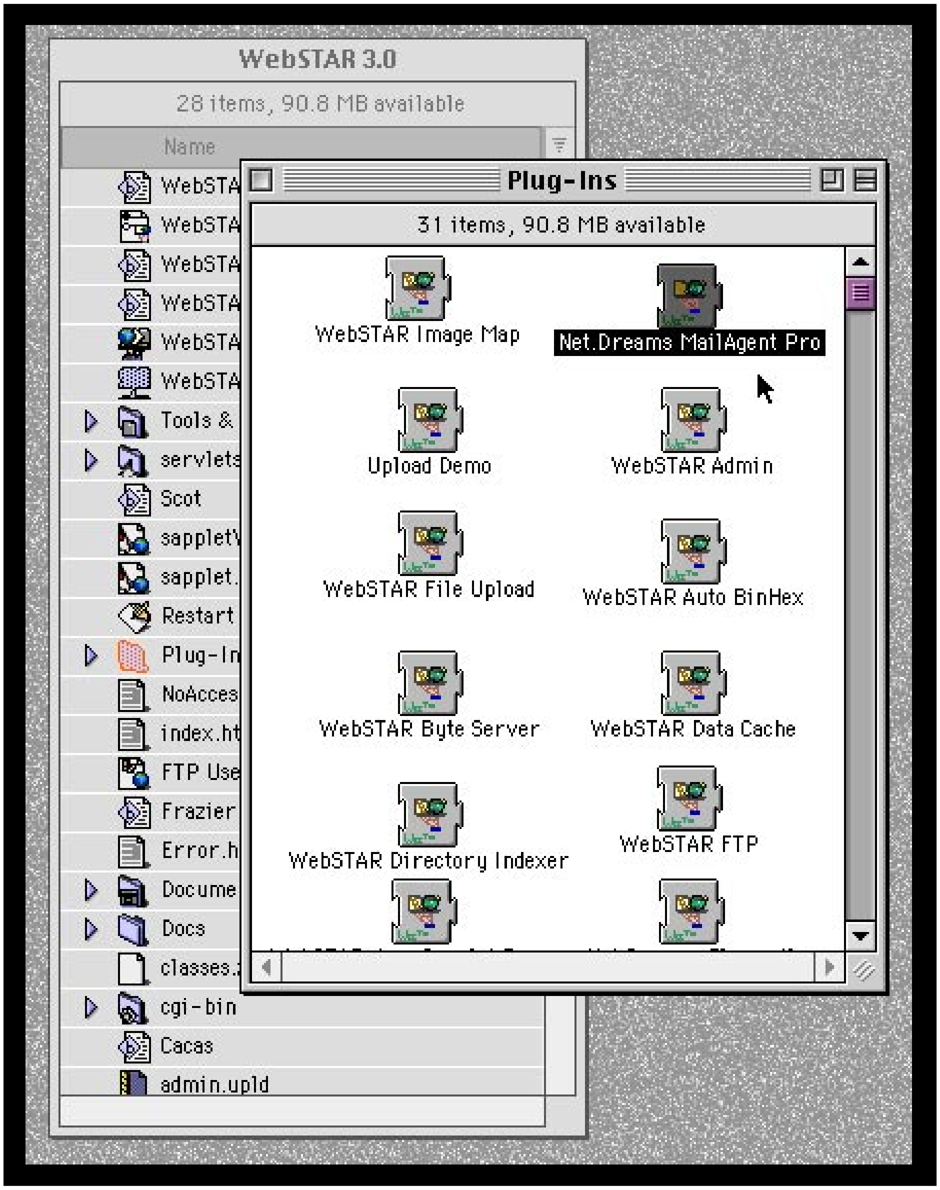
Installation Procedures



The installation procedure for Mail Agent is a simple, two part process;

Installing MailAgent Pro

The Mail Agent plug in ("Net.Dreams Mail Agent") goes in your server software's "plug-ins" folder. Quit your server software, and drop the plug in into the folder. None of the other files need to go with it; MailAgent Pro will create all of the additional files it needs when you re-launch your server software(see graphic).



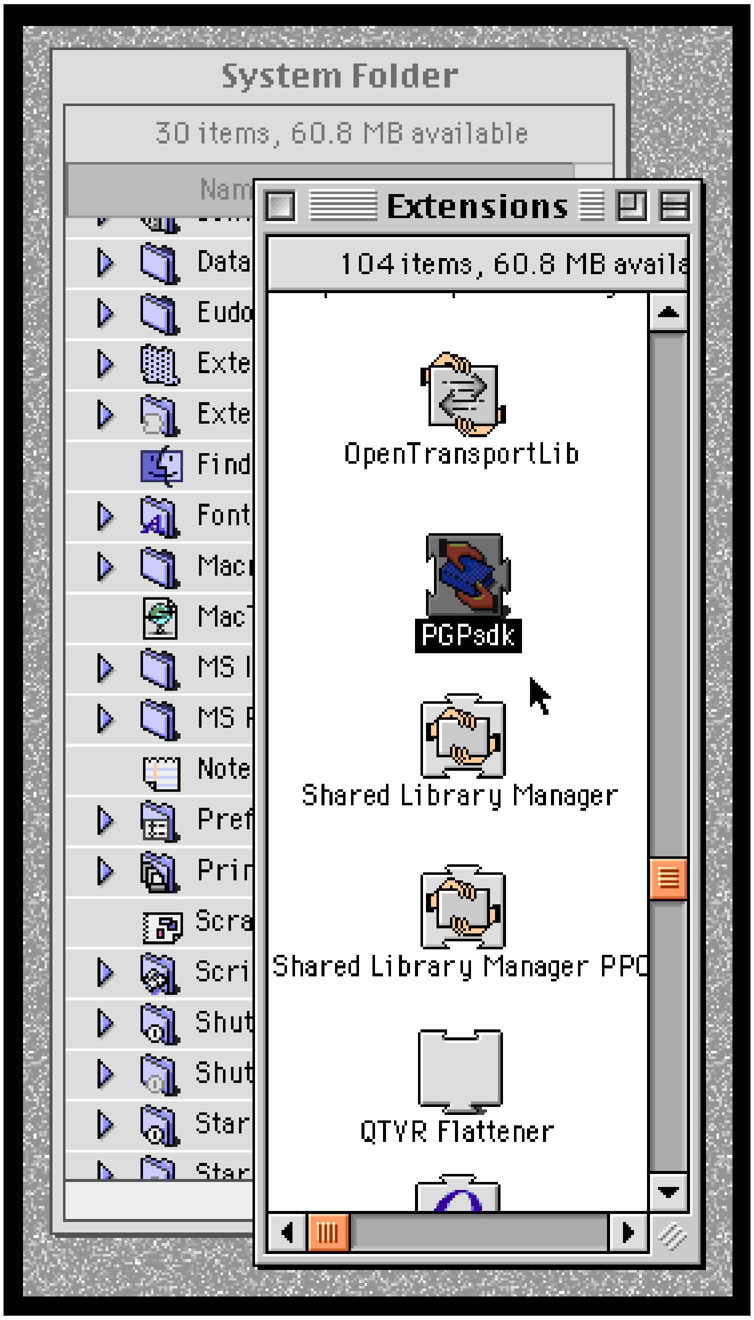
Installing the PGP Extension

The second file to install is called "PGPsdk," and it goes in the extension folder of your server machine's system folder. Drop it in the extension folder (see graphic).

Now re-launch your server software. That's all there is to it!

Upgrading from a previous version ofMailAgent

If you are already using a previous version of MaiAgent, you can keep all of your configurations while changing over to MailAgent Pro. In your plug-ins folder, there is a file named "Mail Agent.prefs" - rename it "MailAgent.prefs" (only the space between 'Mail' and 'Agent' needs to go!). Next to the newly re-named file,there should be a folder named "Mail Agent"—rename it "MailAgent Data" —then follow the instructions above.



Introduction to MailAgent Pro

MailAgent Pro is a general-purpose mail-sending utility for MacOS web servers that are compliant with the WebSTAR API 1.2 and higher. This includes WebSTAR 2 and higher, Quid Pro Quo, WebTen, and several other servers. You can use MailAgent Pro to send electronic mail from most dynamic web page tools like SSI, Lasso, Tango, and Flexmail. Although many of these tools have limited email capability already built in to them, MailAgent Pro provides important features and flexibility that they don't offer.

MailAgent Pro Features Include:

Encryption - messages can be encrypted with industry-standard PGP (Pretty Good Privacy). This means you can email sensitive information, such as credit card orders, from your secure server to people outside your network without worrying about unauthorized people gaining access to that information. Encryption feature is not available in MailAgent Lite

Attachments - you can send as many binary files as you like with each message. Your only restriction is the disk space required to save the message until it is sent. Attachment feature is not available in MailAgent Lite

Flexible Addressing - a message can be addressed to several people as the direct recipients (To), Carbon Copy recipients (Cc), and Blind Carbon Copy recipients (Bcc).

Message Recovery - messages are saved until they are sent. Messages that aren't properly formatted or suitable for transmission are filed where the server administrator can pick them up later. If the server goes down for any reason, unsent messages are read from disk and transmitted when the server is restarted.

Startup Notification - you can have MailAgent Pro notify you via email
whenever your server is launched.

Logging - MailAgent Pro messages are logged. There is also an "extended logging" option to record detailed information about each message.

Intelligent Header Parsing - you can include any header information you like in your messages. This means you can specify Sender and Reply-to addresses, content-type, language specifiers, and other advanced header options. If you use a header field that MailAgent Pro does not understand, it will simple leave the field alone.

Apple Events - you can activate MailAgent Pro from any application that can send AppleEvents.

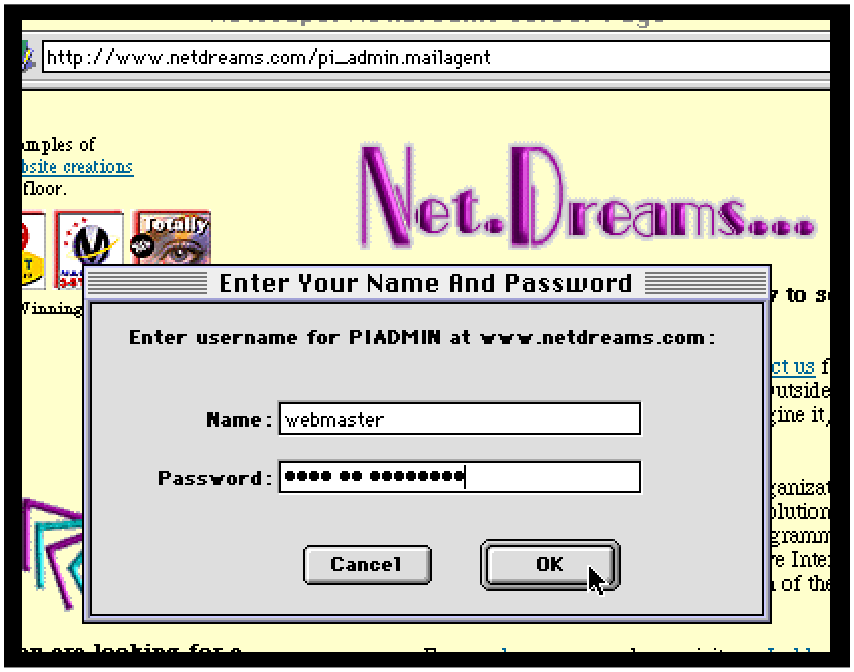
PIXO Support - will interoperate with PIXO dispatching plugins.

MailAgent Pro Administration

You must configure your mail server and enter your license key before MailAgent will work properly. To change the MailAgent Pro settings, use this URL:

<http://www.yourserver.dom/pi_admin.mailagent>

This URL will activate the administration pages of the plug-in. If you have restricted access to this realm (which is the default setting in WebSTAR) you will need to enter your system's administation username and password.



http://www.netdreams.com/pi_admin.mailagent

Enter Your Name And Password

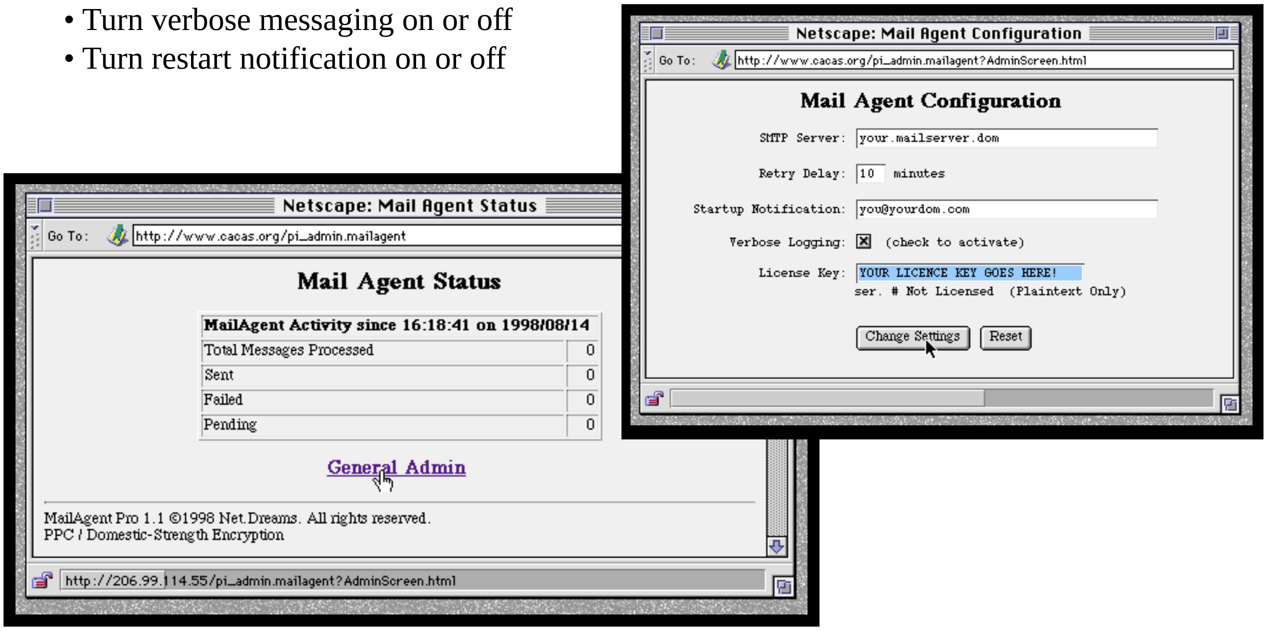
Enter username for PIADMIN at www.netdreams.com:

Name: webmaster

Password: •••• •• ••••••••

The MailAgent Pro administration pages allow you to do the following:

- Get traffic information since the last server restart
- Enter your license key, which you will have to do to use MailAgent Pro on a regular basis
- Set your mail server
- Turn verbose messaging on or off
- Turn restart notification on or off



Netscape: Mail Agent Configuration

Go To: http://www.cacas.org/pi_admin.mailagent?AdminScreen.html

Mail Agent Configuration

SMTP Server: your.mailserver.dom

Retry Delay: 10 minutes

Startup Notification: you@yourdom.com

Verbose Logging: ☒ (check to activate)

License Key: YOUR LICENCE KEY GOES HERE!

ser. # Not Licensed (Plaintext Only)

Netscape: Mail Agent Status

Go To: http://www.cacas.org/pi_admin.mailagent

Mail Agent Status

MailAgent Activity since 16:18:41 on 1998/08/14	
Total Messages Processed	0
Sent	0
Failed	0
Pending	0

MailAgent Pro 1.1 ©1998 Net.Dreams. All rights reserved.
PPC / Domestic-Strength Encryption

http://206.99.114.55/pi_admin.mailagent?AdminScreen.html

MailAgent Pro Basics

Message Format
WebSTAR SSI 3 Example
Flexmail Example

Message Format

MailAgent Pro is activated simply by giving it an email message. A message has two parts - the header and the body. A typical email message looks something like this.

```
 To: CJ Holmes <cjh@netdreams.com>
 From: Webmaster <webmaster@mydomain.org>
 Subject: An email message

 This is the body of the message.  Notice that there is a blank line
 between the end of the header and the beginning of the body of the
message.

 The message can be as long as you like - there is no hard limit on
 how long the message can be or how many people can receive it.
```

As you can see, there isn't much to it. In fact, if you use internet email regularly then you are already familiar with what email messages look like and how they are formatted.

The most important part is the header because this is where you tell MailAgent Pro who is to receive the message and what MailAgent Pro options you wish to use. We'll explain later exactly what is (and isn't) a valid header format, but to get started you need to know a few important points:

- Each line of the header begins with an entity name. This is a name like "From", "To", or "Subject". A header line should not begin with a space, a tab, or other nonalphabetic characters (including invisible characters generated by word processing software.)
- The entity name is followed by a colon and a space.
- There are no blank lines in the header.
- The first blank line in the message indicates the end of the header and the beginning of the body of the message.

WebSTAR SSI 3 Example

With WebSTAR SSI (version 3) MailAgent Pro adds its own tag to the SSI vocabulary. MailAgent Pro registers a tag that tells SSI to send email. Here is a short example:

Sample HTML Document with Custom SSI Tags

```
<html>
<head>
	<title>CJ's Mail Demo</title>
</head>
<body bgcolor=#f0f0f0>

<h2>Hello! This is a very short web page!</h2>

<mail>
To: you@your.address.dom (Your Name)
From: webmaster@theHouse.com (WebMaster)
Subject: A Visitor Stopped By

Visitor Number <!--#counter var="mail_counter"--> just stopped by.
They were using a <!--#echo var="http_user_agent"--> browser.

</mail>

</body>
</html>
```

Notice the custom tag inserted in the example above. When accessed by a browser, this file will cause MailAgent Pro to send a message to the address "you@your.address.dom". WebSTAR SSI 3 also has tags that allow you to insert form field contents into the text, which means you can include form data in the email message.

Flexmail Example

MailAgent Pro comes bundled with a product called Flexmail. Flexmail is a simple tool for taking the field data from an HTML form (such as an order form or survey form) and putting it into email, saving the data into an HTML file, or saving it into a simple data file.

Like SSI, Flexmail uses a <mail> tag to specify what part of the text is to be treated as email.

Sample Flexmail Document

```
<mail>
To: webmaster@my.dom
From: %username% <%useraddress%>
Subject: A Registered User

 A user named %username% from %userstate%, %usercountry% registered
  at the web site.  They heard about the site address from %heardfrom%.
 </mail>

 <savedata registrants.txt>
username
useraddress
userstate
usercountry
heardfrom
</savedata>

<response>
<body bgcolor=#f0f0f0>
<h2>Thanks!</h2>
Thanks for registering at our web site.
</response>
```

As you can see, this example takes form input (the HTML input form is not shown here) and saves it into a text-and-tabs file. A copy of the data is sent to the webmaster of the site.

Attaching Files to Your Messages —MailAgent Pro version only.

In addition to text, you can also send binary data files through email. You tell Mail Agent to attach a file to a message by using X-Attach header. For example:

```
To: me@my.dom
 From: webmaster@my.dom
 Subject: Attachment
 X-Attach: "subfolder/afile.gif"; type="image/gif"

 You should receive an attached file with this message.
```

When attaching files through Flexmail, SSI, or PIXO, you may use a relative filename. That is, you can specify a filename or a "folder/filename" path. Mail Agent will look for the indicated folders and file within the same folder as the document currently being served by your web server.

You may also use a full path from the current site's root folder:

```
X-Attach: "/folder/afile.gif"; type="image/gif"
```

When attaching files through AppleEvents, the filename paths are always relative to your server's root folder.

Specifying a MIME Type

To display an email message, your recipient's software needs to know what kind of file it is reading. You can specify the MIME type of the enclosed file with the 'type' parameter. For a list of common file extensions and their MIME types, consult your web server's suffix mappings.

Sending Multiple Files

You can send as many files as you want at one time, and they can be as large as you like. Just keep in mind that large attachments will take longer to process and send, and will require more disk space to store until they are sent.

```
To: me@my.dom
From: webmaster@my.dom
Subject: Attachment
X-Attach: "subfolder/afile.gif"; type="image/gif"
X-Attach: "fileTwo.html"; type="text/html"
X-Attach: "fileThree.sit"; type="application/x-stuffit"
X-Attach: "fileFour.pdf"; type="application/pdf"
```

You should get four attached files with this message.

Headers

General info

An email message is divided into two parts: the header and the body. The two parts are separated by a blank line. The body of the message contains the actual message data. The header contains instructions on how the message is to be processed: to whom the message is addressed, how it should be displayed, the priority, etc. When sending email through Mail Agent, the header can also contain instructions on additional processing to do before the message is delivered.

Fields

A header is composed of fields. A field begins with a word, like "To" or "Subject", followed by a colon and one or more spaces, and then the field data. The following message has a header composed of three fields.

```
<mail>
To: CJ Holmes <cjh@netdreams.com>
From: Joe Bloe <joe@netdreams.com>
Subject: Hello

This is just a message to say hello.
</mail>
```

Folding a field

Sometimes a field won't fit on a single line. If your editing software won't "soft wrap" the text for you, or for some reason you want to use a "hard" return, then you must take care to "fold" the field properly. This means the second and subsequent lines of the field should begin with a space or tab character. Here are some examples of folded fields:

```
<mail>
To: CJ Holmes <cjh@netdreams.com>,
     John Doe <jd@netdreams.com>
From: claire@netdreams.com
Subject: This is a very long subject.  Normally, you shouldn't use
     a subject that is so long, but it is acceptable to do so.  I don't
     recommend that you do this.

This is the body of the message.
</mail>
```

Important Rules of Thumb

1. Each field name must start at the beginning of the line. Do not put spaces or tabs between the beginning of the line and the field name.
2. You must separate the header and body of the message with a blank line. You can not use a blank line in the header.
3. If you wish to spread a field across more than one line, you must fold it properly.

Important fields

From	This is a required field - the message can not be sent without it. It should contain exactly one address.

To	This field lists the direct recipients of the message. It is a required field, and must contain at least one address

Cc	A list of addresses that will receive a "Carbon Copy" of this message. By convention, Cc recipients are not expected to act directly on the message.

Bcc	A list of people who will receive a "Blind Carbon Copy". Mail Agent will attempt to deliver the message to the Bcc recipients, but will remove the Bcc field from the header. This is to prevent the other recipients from knowing that the Bcc recipients have a copy of the message.

Subject	The subject matter of the message

MaiAgent Pro specific fields

X-PGP	Instructs Mail Agent to encrypt the message before sending it. Read the section on "PGP Encryption" for more details.

X-Attach	Instructs Mail Agent to attach a binary file to the message. See the section on "Attachments" for details.

Other fields

Reply-to	Contains a single address. This is an instruction to the mail client to address replies to the indicated address instead of the From address. Most email clients honor this field.

Errors-to	Contains a single address. This is an instruction to mail servers to return the message to the indicated address if the message can't be delivered. Most email servers honor this field.

Content-Type An instruction to the mail client specifying the content type of the message body. This often comes in handy if you want to send HTML instead of plain text, for example. For plain text you can also specify the character set you used to create the message. Examples:

Content-Type: text/plain; charset="ISO-8859-2"
Content-Type: text/html

X-Priority Contains a number from 1 (highest) to 5 (lowest), with 3 the normal setting. Most clients will specially mark messages that have a set priority.

X-URL A URL associated with this message. Many email clients will display this field as a clickable link.

Address Formats

Addresses can be expressed in a few different formats. For example, pretend Emma Peel has an address at netdreams.com. All of these are valid ways to express his address:

To: Emma Peel <Emma@netdreams.com> (Preferred)
To: Emma@netdreams.com
To: Emma@netdreams.com (Emma Peel)
To: <Emma@netdreams.com> "Emma Peel"

The BEST way to express an email address is to place it within angle brackets.

To place multiple addresses into one field, simply separate them with commas. If you need to fold a To, Cc, or Bcc field try to do so between addresses and not in the middle of an address.

Using MailAgent Pro with AppleEvents

Event Specification

Any application on the same computer as your web server software can send email with MailAgent Pro. During the server startup, MailAgent Pro registers the following event with your server software:

Event Class	'WWWΩ'	(that last character is "Omega" or Option-Z)
Event ID	'Mail'	
'----'	The message to send, complete with headers.	(this is the direct object)

Lasso Example

(by Blueworld, www.blueworld.com)

This example illustrates the basics of using Lasso to send email with MailAgent Pro. The first example file is sendmail.html, which is a form that allows a user to compose a simple message.

```
<html>
    <head>
        <title>Compose Email</title>
    </head>
    <body bgcolor=#f0f0f0>
    <h2>Fill this out</h2>
<form action=sendmail.lasso method=post>
<pre>
Your email address:  <input type=text name="sender">
Destination address: <input type=text name="recipient">
Subject:             <input type=text name="subject">

Enter your message here:
<textarea name=body rows=15 cols=55 wrap=virtual></textarea>

<input type=submit value="Send"> <input type=reset value="Reset">
</pre>
</form>
    </body>
</html>
```

The second example file, sendmail.lasso file turns the form data into electronic mail.

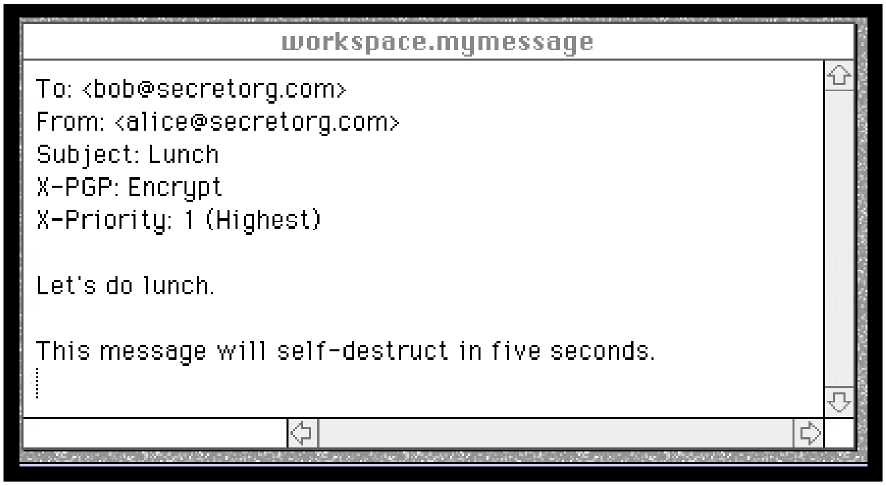
```
<html>
        <head>
                <title>Email Sent</title>
        </head>
        <body bgcolor=#f0f0f0>
        <h2>Your email is on its way</h2>

[event: class="WWWΩ", id="Mail", target="WWWΩ" wait_reply=false]
 '----':“To: [form_param:"recipient"]
From: [form_param:"sender"]
Errors-To: WebMaster <webmaster@my.dom>
Subject: [form_param:"subject"]

[form_param:"body"]
”
[/event]

        </body>
</html>
```

Some things worth noting about this example:

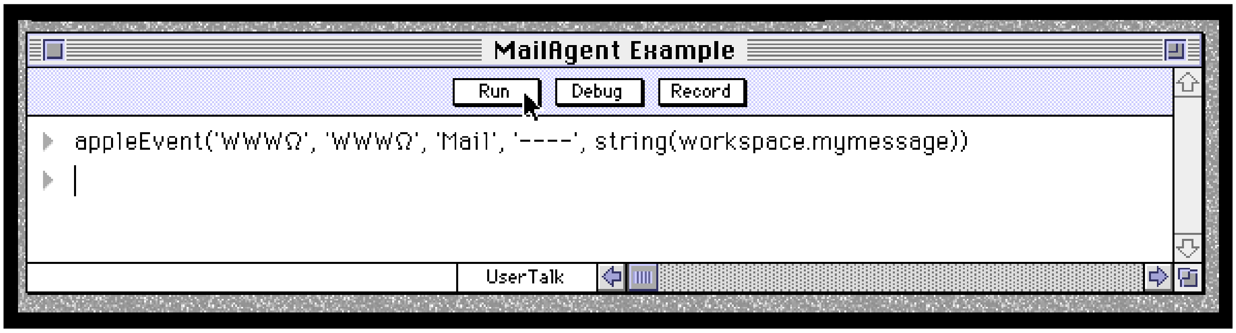
- The quotes around the message are "smart quotes" **(“ ”)**. To key on a Macintosh, use keystrokes **option** + **[** (for the open-quote) and **shift** + **option** + **[** (for the close quote). These characters are not apparent in HTML.
- You can include any headers you want in the message. You are not limited to just the headers that MailAgent Pro explicitly supports. The "Errors-To" header is especially helpful. If the mail server accepts a message from MailAgent Pro but can't deliver the message, the mail is usually forwarded to the error address.
- You can use any Lasso tags inside the message.

Frontier Example

Using MailAgent from Frontier is very simple. The message can any string value within the Frontier environment. Sending the message is just a matter of passing an AppleEvent to your Web server with the message. In this example, the message is a WP-Text item at "workspace.mymessage."



```
To: <bob@secretorg.com>
From: <alice@secretorg.com>
Subject: Lunch
X-PGP: Encrypt
X-Priority: 1 (Highest)

Let's do lunch.

This message will self-destruct in five seconds.
```



```
appleEvent('WWWΩ', 'WWWΩ', 'Mail', '----', string(workspace.mymessage))
```

History

1.1
980817
Added PGP and attachment support.

1.0.3
980807
Fixed compatability problems with Quid Pro Quo.

1.0.2
980703
Stopped registering a file type ('TEXT') and suffix ('ttxt') for MailAgent. Removed the CGI handler. This was a carry-over from our template plug-in.

Together, these two innocuous items caused some very unexpected behavior. The type and suffix were preempting the default definitions in the server's suffix table. When a file was requested whose extension did not appear in the suffix mapping table but whose creator/type codes matched the ones registered by Mail Agent, the request would be handed as a CGI to Mail Agent. The CGI-handling code would actually service the request but give a MIME type of text/plain. Hence, some HTML documents would be displayed as plain text.

980621
Name changes. The version without encryption or file attachment is now officially labeled "Net.Dreams MailAgent Lite". This is the version that will be included for free with Flexmail. "Net.Dreams MailAgent Pro" now includes PGP email encryption and attachments.

Failed message counting fix. Some failed messages were improperly counted as "pending". The MailAgent Pro status screen now reports the correct number of sent, failed, and pending messages.

980619
Fixed buffer-sizing errors under WebTEN. This bug caused the buffer size to be set to 0, thus causing MailAgent Pro to fall into an infinite loop when sending HTTP data.

Fixed shutdown under WebTEN. WebTEN does some funny stuff to pi-created threads during shutdown, so I had to change my shutdown proceedures to avoid causing an infinite loop.

1.0.1
980407
Fixed bug that caused MailAgent to fail to initialize on servers using W*API < 1.3. (eg: WebSTAR 2.1)

1.0
980401
Final Release in conjunction with Flexmail 2.1

Encrypting a message with MailAgent Pro

MailAgent Pro version only.

To encrypt a message with MailAgent Pro, there are a few things you need to do:

1. You must be running your server on a PowerPC Macintosh. Encryption is not yet available for 68K Macintoshes.
2. Make sure you have an encryption-enabled version of MailAgent Pro (1.1). If your version is encryption-enabled, the bottom of MailAgent Pro's "Admin Home" page contains the phrase "Domestic-Strength Encryption" or "Exportable Encryption".
3. You must have a license key that enables the encryption services. On the "General Configuration" administration page next to your key's serial number should be the phrase "Plaintext Only", "Domestic-Strength Encryption", or "Exportable Encryption".
4. You must place a PGP public keyring into your "MailAgent Data" folder. This keyring must contain the public keys of everyone to whom you want to send secure messages.
5. You must add the "X-PGP: Encrypt" header to the messages you wish to encrypt.

Example:

```
To: cjh@netdreams.com (CJ Holmes)
From: webmaster@my.dom
Subject: Encrypted Message
X-PGP: Encrypt

This message will be encrypted when it reaches you!
The "X-PGP" header will not appear in the final message.
```

Once you have accomplished steps one through five, it is very simple to encrypt any message that you send with MailAgent Pro. All you have to do is add the "X-PGP" header.

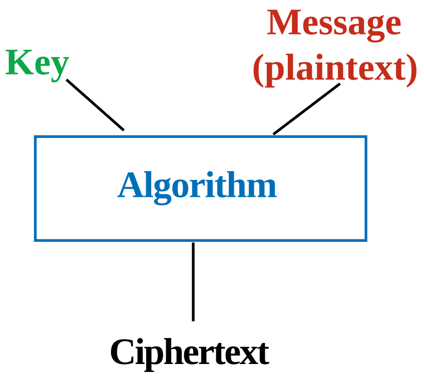
Cryptography Primer

This section is for users who are unfamiliar with with cryptography. If you are already familiar with public key cryptography, you do not need to read this section

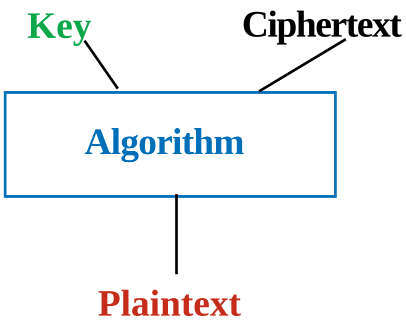
Symmetric Cryptography

Cryptography is the study of ways to conceal the content of messages. This is accomplished by processing the message in a manner which disguises or scrambles the content to prevent unauthorized people from deciphering it. This is called Encryption. When the authorized party receives the message, he or she processes the message to remove the disguise. This is called Decryption.

In symmetric cryptography, the encryption process combines the original message (the plaintext) with a secret (called the key) known only by the parties who wish to communicate. The result is a scrambled message that is difficult, if not impossible, for outsiders to understand.



To reverse the process, the recipient of the message uses the same process to combine the key with the ciphertext. The result is the original message.



The Problem with Symmetric Cryptography

There is a major problem with symmetric cryptography: Everyone who wants to communicate securely must share a secret with each person with whom they want to communicate. This has some important implications.

- You need to have a secure way to exchange keys. What if you need to send encrypted messages to your office in London, but you can't trust your telephone (it may be bugged) or the US mail? How do you send the key to your office in London without already having a secure way to send messages?

  Often, the answer is to put the key into a briefcase, handcuff the briefcase to a trusted courier, and put him on a plane to London. When he gets to London he gives the briefcase to your counterpart. This can be expensive, time consuming, and if the courier isn't so trustworthy it can be disastrous. If the courier is intercepted on his way to London or sells the keys to your competitors, all of your future communications could be compromised.

- If you need to communicate with lots of different people you can end up trying to keep track of hundreds, even thousands, of keys.

- It is very difficult to establish a secure channel to communicate with someone on a one-time basis.

Public-Key Cryptography

Public-key cryptography takes a very different approach to the problem of key management. Each individual has a special kind of key that is split into two parts - a public key and a private key. These keys have two important attributes:

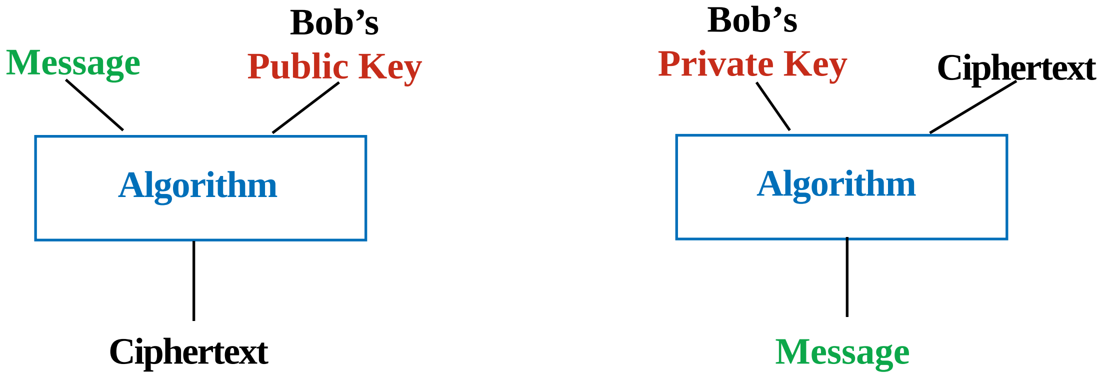
1. Whatever is encrypted with one key can only be decrypted with the other key.

2. The private key cannot be easily discerned just by knowing the public key.

Your private key is exactly that - private. You keep it safe and do not divulge it to anyone. Your public key can be distributed freely in email, public databases, and in any other way you choose.

Now when Alice wants to send a message to Bob, she can look up his public key in a database or simply ask him to email it to her. She can then encrypt a message with Bob's public key and email the message to him. When Bob gets the message, he decrypts it with his private key.

Alice uses
Bob’s Public Key
to send him a message.



The advantages of this system are:

1. You no longer need to establish a secure channel to exchange keys.
2. Key management is vastly simplified. Each person needs only one key pair.
3. It becomes practical to securely communicate with strangers.

Cryptographic Applications

Cryptography can do more than just protect you from eavesdropping. In fact, cryptography can supply security in four ways.

Authentication - It is possible for the receiver of a message to verify the sender of the message.
Integrity - The receiver can be certain that the message was not altered in transit.
Nonrepudiation - The sender can not claim that he or she did not send a message.
Confidentiality - protecting your communications from prying eyes. (This is the kind of security we've been talking about.)

PGP's authentication mechanism supplies some measure of integrity and nonrepudiation as a side-effect. PGP signatures are discussed in the next section.

PGP Basics

About PGP

Because you will be sending secure email from your server, you probably want to be able to decode and read it. For this you will need a utility that decodes PGP-encrypted email. Here are some links you will find useful:

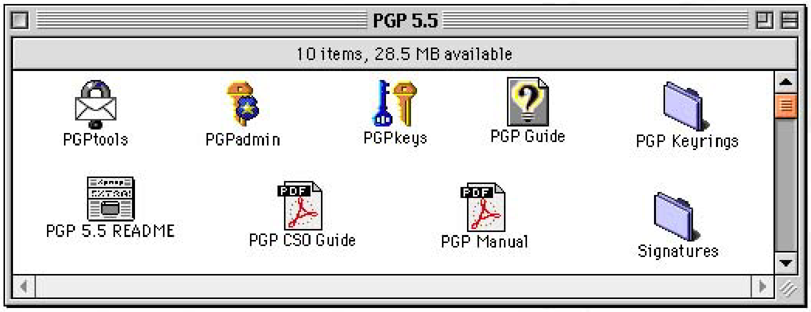
PGP Freeware Download
www.nai.com/products/security/pgpfreeware.asp
This software is for personal and evaluation use only. It is available for both Macintosh and Windows platforms.

PGP for email and files with RSA support
www.nai.com/products/security/pgp_business/pgp_busi.asp
This is the commercial-grade software, which we recommend if you are going to use PGP regularly in your business.

Network Associates home page
www.nai.com
If you do not already have a secure email tool of some kind, then we recommend you download PGP and install it on whatever computer you regularly use to pick up email. You do not need to install PGP onto your web server. On the MacOS, PGP integrates seamlessly with Eudora and many other Macintosh email applications.

We're going to take you through a very brief tour of PGP. We'll show you how to create your own public/private key pair, send encrypted email with Eudora, and use Eudora to read encrypted email.

PGP installs several components that are of interest to us:



PGP Keys application - You'll use this to create a key pair and to keep track of other peoples' public keys. You can also use PGP Keys to look up public keys in internet key databases.

PGP Contextual Menu - This is the little lock icon you see in the menu bar, just to the left of the Help menu. This icon will be present in many of your applications. You can use it to encrypt, decrypt, sign, and verify the contents of a document from any application that supports menu sharing.

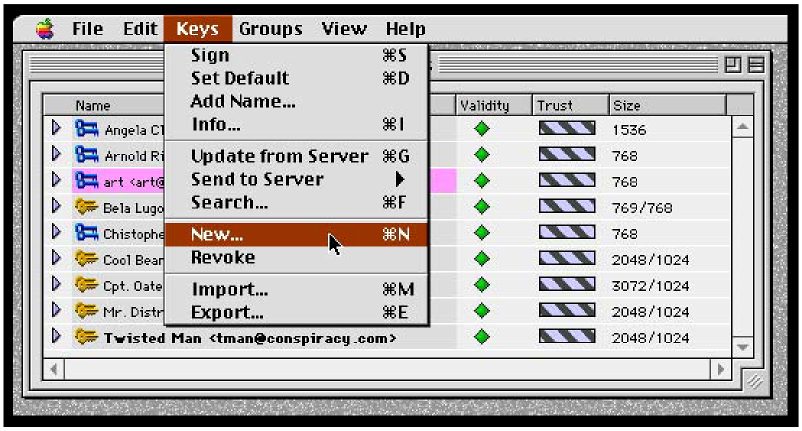
PGP Eudora Plugin - You can't see it here, but if you have Eudora, PGP will install an extension to it that makes it easy to encrypt, decrypt, sign, and verify documents.

PGP Manual - Because Network Associates doesn't support their freeware, you'll probably want to read the documentation sooner or later. For now, we can get by without it.

Creating Your Own Key Pair

Once you have installed PGP, you will want to create a public/private key pair. This will enable other people to send you secure messages, and will allow you to sign documents.

To begin, double-click on the PGP Keys application. You will probably be asked if you want to create a new keyring. Because you don't have any keys yet, go ahead an allow PGP Keys to create the keyrings. Once it has launched, select **Keys...New** from the menu.
The "Key Generation Wizard" will walk you through the process of creating your own key pair. Just follow the directions and you'll be fine. Here are some suggestions that you might find helpful.



Name	Validity	Trust	Size
Angela C1	◆	▨	1536
Arnold Ri	◆	▨	768
art <art@	◆	▨	768
Bela Lugo	◆	▨	769/768
Chistophe	◆	▨	768
Cool Bear	◆	▨	2048/1024
Cpt. Oate	◆	▨	3072/1024
Mr. Distr	◆	▨	2048/1024
Twisted Man <tman@conspiracy.com>	◆	▨	2048/1024

Email Address - You should enter the email address you use for picking up email.

Key size - The default key size is fine for most applications. Larger keys are much harder to break, but take longer for the computer to use. If you plan to change your private key every six months or so, you can select a smaller key size.

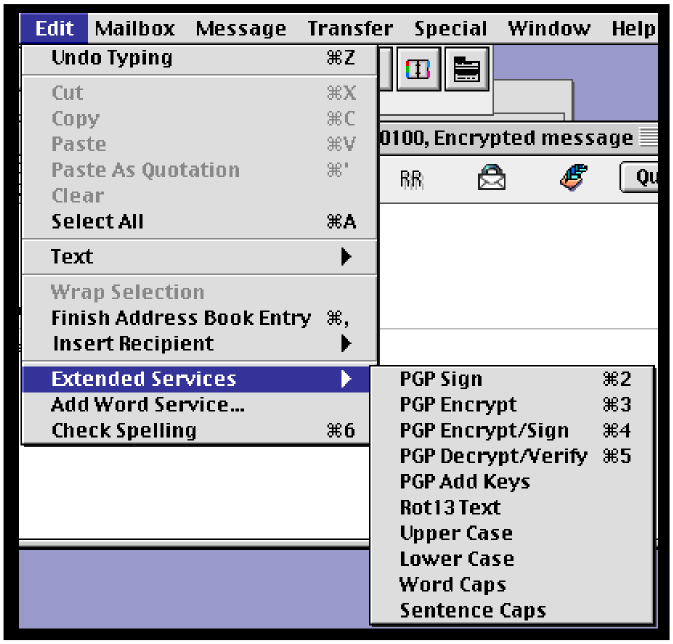
Expiration - We highly recommend using an expiration date of one year, and then generating new keys every year. Setting an expiration date will prevent people from using old versions of your public key.

Password - The password is used to protect your private key - without the password nobody can use your private key. You will need to enter your password whenever you sign or decrypt a message. You can use a whole phrase as a password. Make sure it is something you will remember— if you lose your password there is no way to get it back—you've effectively lost your private key.

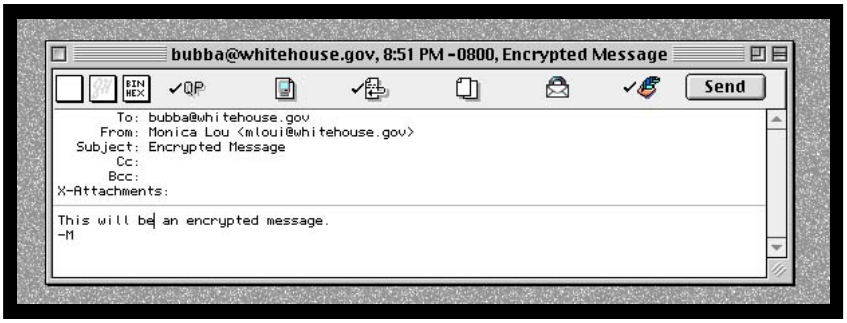
Send key to server - If you are just experimenting, don't bother sending your public key to the server. If you plan to use your key regularly, you should publish your public key on a key server. This allows people to find your public key easily.

Sending Encrypted Email with Eudora

Once you have completed composing a message, you can select PGP Encrypt from Eudora's Edit Extended Services menu. PGP will ask you to select the public keys of the people for whom you want to encrypt the message, and drag them into the small window. When you click the OK button, your email will be instantly turned into gibberish.



You can also select PGP Sign or PGP Encrypt/Sign from the Word Services menu. When you do this, PGP will ask you for your password, and then sign the message using your private key.



```
           To: bubba@whitehouse.gov
         From: Monica Lou <mloui@whitehouse.gov>
      Subject: Encrypted Message
           Cc:
          Bcc:
X-Attachments:

This will be an encrypted message.
-M
```

People who receive this message from you can use your public key to verify that you sent the message. Both of these operations can be performed automatically by selecting either the "locked envelope" icon (for encryption) or "quill" icon (for signing) on the message window. The next time Eudora sends your queued messages it will perform all of the encryption and signing necessary. It will also look up the public keys to use for you from your public keyring. If you are signing more than one message, you will only need to enter your password once.

Receiving Encrypted Email with Eudora

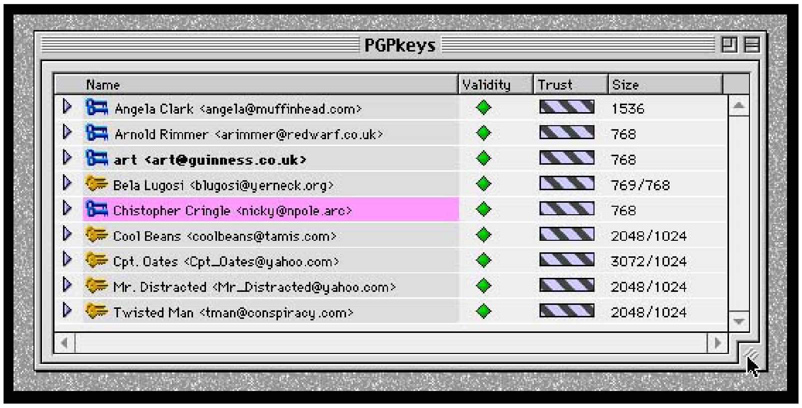
If you receive a message that is encrypted using your public key, you can decrypt it easily by select **PGP Decrypt/Verify** from the **Edit...Extended Services** menu. You will be asked for the password to your private key, and then the message will be decrypted.

About Keyrings

What is a keyring?
Managing keys
MailAgent Pro and your public keyring

What is a keyring?

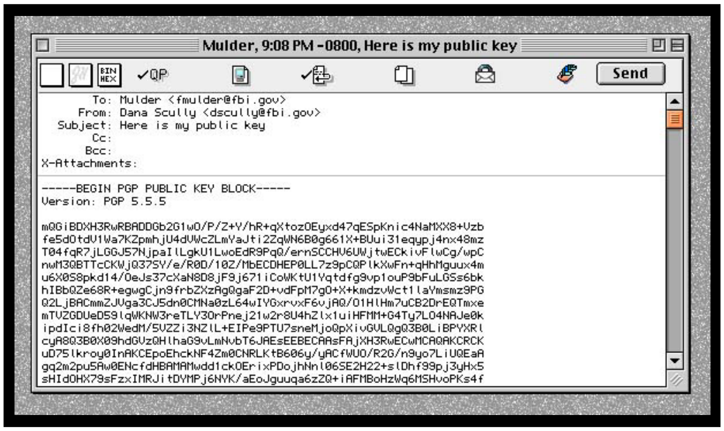
PGP keys are actually very large numbers. Printed in decimal, some of them would be dozens of digits long. Because it would be impractical to remember so many large numbers, these keys are stored in a database called a keyring. You have two keyrings: one for the public keys of you and your friends, and another keyring for your private keys. When you open up the PGPKeys application both of these keyrings appear in the same window as if they were a single file.



Name	Validity	Trust	Size
Angela Clark <angela@muffinhead.com>	◆	▨	1536
Arnold Rimmer <arimmer@redwarf.co.uk>	◆	▨	768
art <art@guinness.co.uk>	◆	▨	768
Bela Lugosi <blugosi@yerneck.org>	◆	▨	769/768
Chistopher Cringle <nicky@npole.arc>	◆	▨	768
Cool Beans <coolbeans@tamis.com>	◆	▨	2048/1024
Cpt. Oates <Cpt_Oates@yahoo.com>	◆	▨	3072/1024
Mr. Distracted <Mr_Distracted@yahoo.com>	◆	▨	2048/1024
Twisted Man <tman@conspiracy.com>	◆	▨	2048/1024

Managing Keys

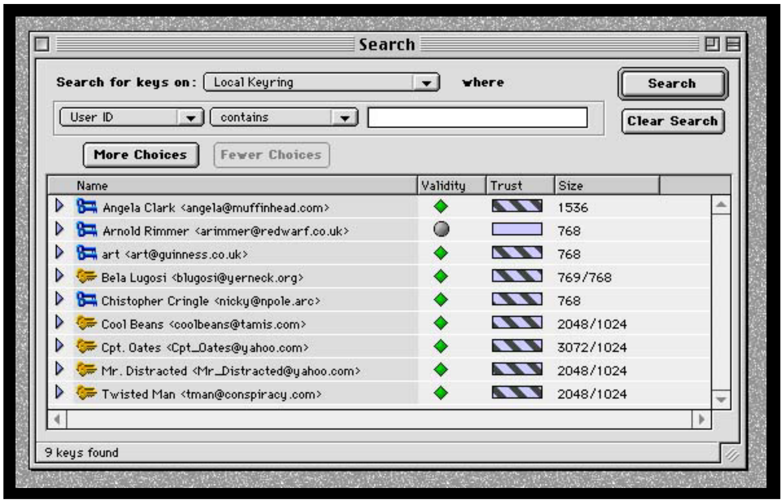
Like you would expect, you can select one or more keys and then delete them with a keystroke. You can also copy and paste your key into email messages. Simply select your key from the PGPKeys application, copy them, and then paste your key into any text window. What you should see will look like this:



```
          To: Mulder <fmulder@fbi.gov>
        From: Dana Scully <dscully@fbi.gov>
     Subject: Here is my public key
          Cc:
         Bcc:
X-Attachments:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 5.5.5

mQGiBDXH3RwRBADDGb2G1wO/P/Z+Y/hR+qXtozOEyxd47qESpKnic4NaMXX8+Vzb
fe5dOtdV1Wa7KZpmhjU4dVWcZLmYaJti2ZqWN6B0g661X+BUui31eqypj4nx48mz
T04fqR7jLGGJ57NjpaIlLgkU1LwoEdR9PqQ/ernSCCHV6UWjtwECkivFlwCg/wpC
nwM3QBTTcCKWjQ37SY/e/R0D/10Z/MbECDHEP0LL7z9pCQPlkXwFn+qHhMguux4m
u6X0S8pkd14/OeJs37cXaN8D8jF9j671iCoWKtU1Yqtdfg9vp1ouP9bFuLGSs6bk
hIBbQZe68R+egwgCjn9frbZXzAgQgaF2D+vdFpM7gO+X+kmdzvWct1laYmsmz9PG
Q2LjBACmmZJVga3CJ5dn0CMNa0zL64wIYGxrvxF6vjAQ/O1HlHm7uCB2DrEQTmxe
mTVZGDUeD59lqWKNW3reTLY3OrPnej21w2r8U4hZlx1uiHFMM+G4Ty7LO4NAJe0k
ipdIci8fh02WedM/5VZZi3NZlL+EIPe9PTU7sneMjoQpXivGVLQgQ3B0LiBPYXRl
cyA8Q3B0X09hdGVzQHlhaG9vLmNvbT6JAEsEEBECAAsFAjXH3RwECwMCAQAKCRCK
uD75lkroy0InAKCEpoEhckNF4Zm0CNRLKtB606y/yACfWUO/R2G/n9yo7LiUQEaA
gq2m2pu5Aw0ENcfdHBAMAMwdd1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5
sHIdOHX79sFzxIMRJitDYMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4f
```

This is very handy when you want to send someone your public key in an email message. The same trick also works in reverse. When someone sends you a public key in email you can copy it and then paste it right into your keyring. PGPKeys automatically converts the key data from text into the correct format.

You can also look up keys from internet servers. From the PGP Keys application use the **Keys | Search...** menu item. You can search for keys on your local disk or on internet key servers. As you can see from this screen shot, I am looking for people named "Thornton" who registered their keys on a public PGP key server.



Search for keys on: Local Keyring where

User ID contains

Name	Validity	Trust	Size
Angela Clark <angela@muffinhead.com>	◆	▨	1536
Arnold Rimmer <arimmer@redwarf.co.uk>	●	□	768
art <art@guinness.co.uk>	◆	▨	768
Bela Lugosi <blugosi@yerneck.org>	◆	▨	769/768
Chistopher Cringle <nicky@npole.arc>	◆	▨	768
Cool Beans <coolbeans@tamis.com>	◆	▨	2048/1024
Cpt. Oates <Cpt_Oates@yahoo.com>	◆	▨	3072/1024
Mr. Distracted <Mr_Distracted@yahoo.com>	◆	▨	2048/1024
Twisted Man <tman@conspiracy.com>	◆	▨	2048/1024

9 keys found

This can take several minutes, depending on what kind of search you ask for. When you get a list of matching keys, you may add one or more of them to your keyring. Just select the keys you want to add and then drag them to your keyring window.

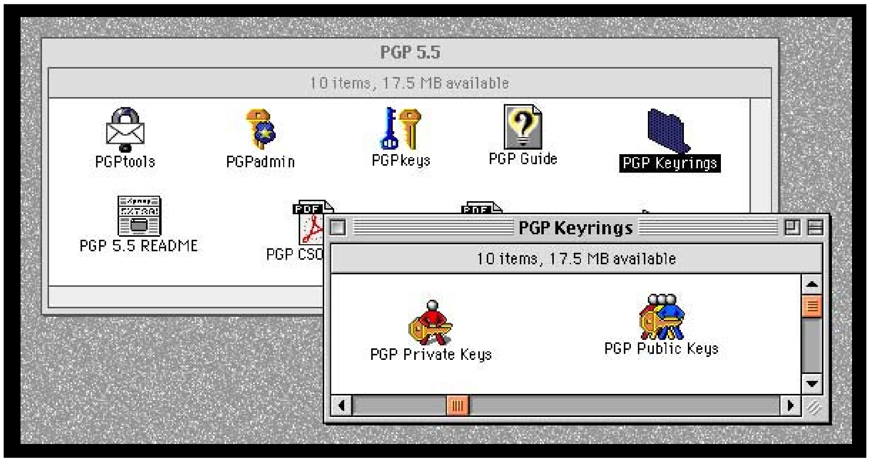
MailAgent Pro and your public keyring

MailAgent Pro needs a copy of your public key ring so it can encrypt messages properly. Each person who will be receiving encrypted messages from your server must have a key in that keyring, and their email address must be included as part of the key information.

1. Quit your server software.
2. Copy your public keyring to the folder, “MailAgent Data”, located in your server software’s plug-ins folder.
3. Launch your server software.

Note:

You must not have more than one public key for each email address in the keyring. If MailAgent Pro finds more than one key for the same email address, it may fail to encrypt that message.



The End.

MailAgent Pro 1.1 Documentation compiled for your convenience and reading pleasure by:

Royal Jelly:
CJ Holmes, President, Founder, Owner, Devloper, Designer, and so forth.

Worker Bees:
Barbara Moore, PDF Mistress
Scot Frazier, Creative Solutions
Kim Grant, Still More Creative Work-Arounds

note: ©1998 Net.Dreams, Inc. “When in doubt, make it Quit!”