Table of Contents

1 Introduction

1.1 What is Secure Information Courier?

Encrypted Email Submissions - Straight from your web site!

Advantages at a Glance...

- Allows your web site visitors to send you secure encrypted messages *with* attachments
- Visitors to your site need no software to use the secure facilities
- Customers are able to send credit card details or private information with confidence
- Allows you to remove insecure form submissions from your web site
- Easy to configure - the wizard guides you through

Secure Information Courier brings strong email encryption to your organization's web site. Visitors to your web site can send secure email to your organization and even convey digital documents securely using industry standard encryption. Secure Information Courier is easy to use and nothing is assumed about the skill level of visitors to your site or about software pre-installed on their computers.

To use Secure Information Courier, you simply deploy an ***ActiveX*** control in the "***contact us***" area of your web site. First time visitors accept the ActiveX control upon their first visit - it's signed with a trust certificate from Thawte, the leading internet trust authority. The ActiveX control contains ***Secure Information Courier*** and allows visitors to your web site to send secure email to your organization as well as securely relay documents to you. If you are an accountancy firm or law firm who for example might wish to receive financial statements or similar documents from clients and provide clients with a secure means of conveyance, then Secure Information Courier is for you.

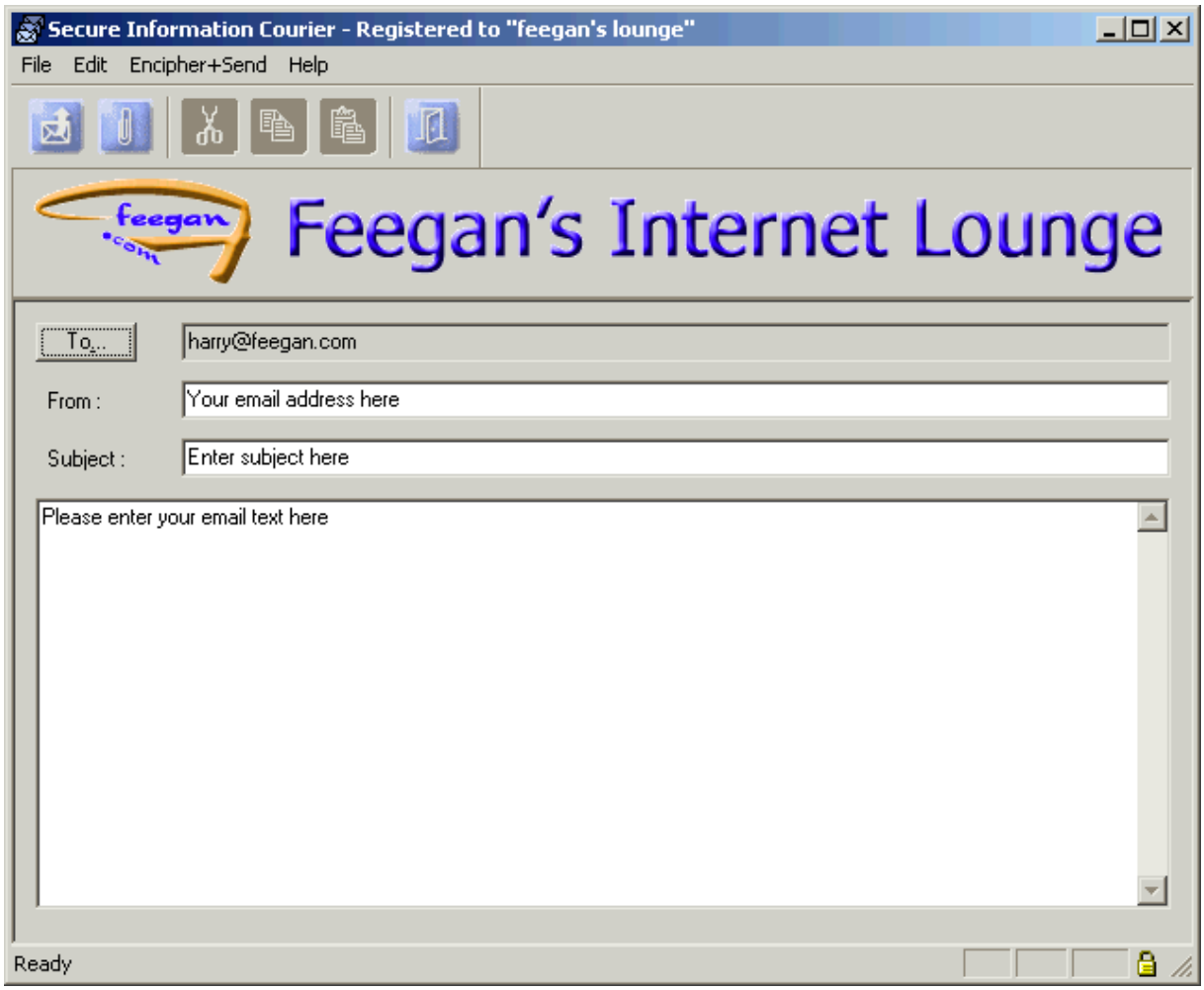
Features :

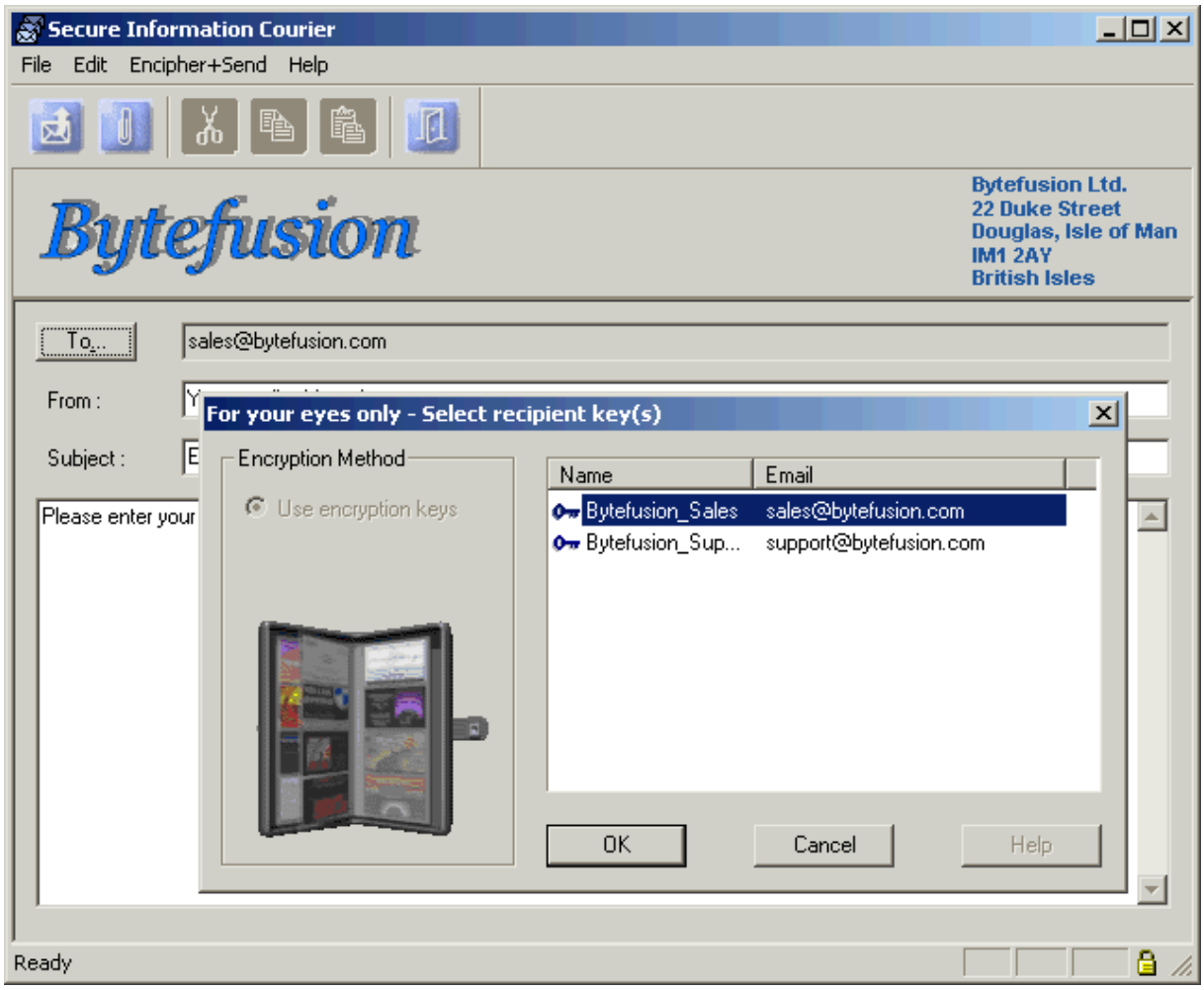
- Secure Information Courier is completely controlled by the web site owner and requires no intermediary services.
- No end user configuration is required. Web site visitors simply fill in a form, enter their message text, then hit encrypt and send...
- The Secure Information Courier user interface is "skin able". This means web site owners can customize the product with their own corporate logo and message prompts.
- Size: At approximately 400KB, Secure Information Courier only takes a few seconds to load.
- Trust: Secure Information Courier uses industry standard encryption technology. The core algorithm

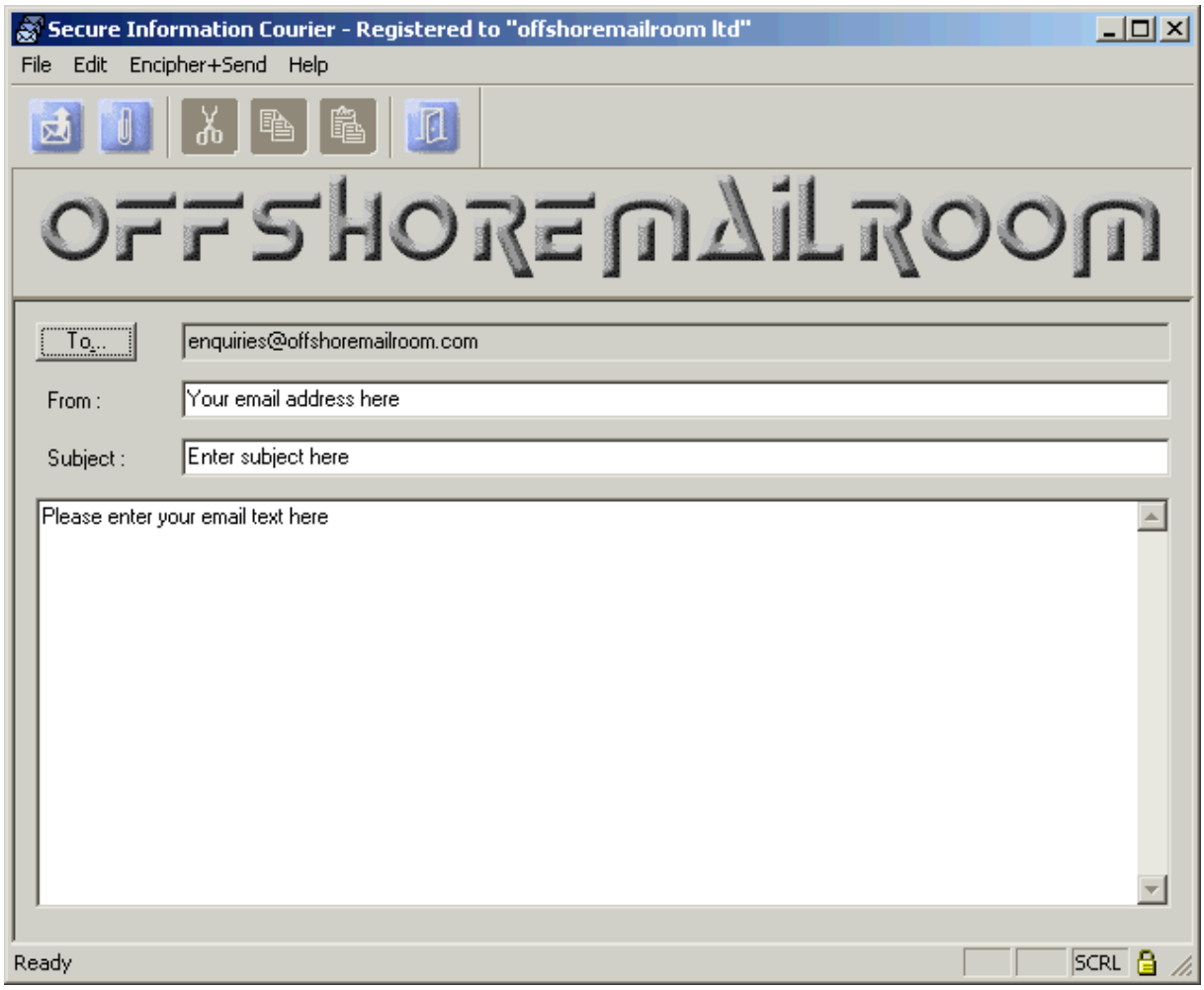
employed by the SecExMail message format is "Twofish". The algorithm is unencumbered by patents and has been subject to extensive peer review.
- Customers send email and documents securely and directly to your mail server. Mail is never stored on the servers of the customer's ISP.
- Compatible with SecExMail and Crypto Anywhere encryption software.

1.2 Secure Information Courier on the web

Depicted below are examples of Secure Information Courier on the web.



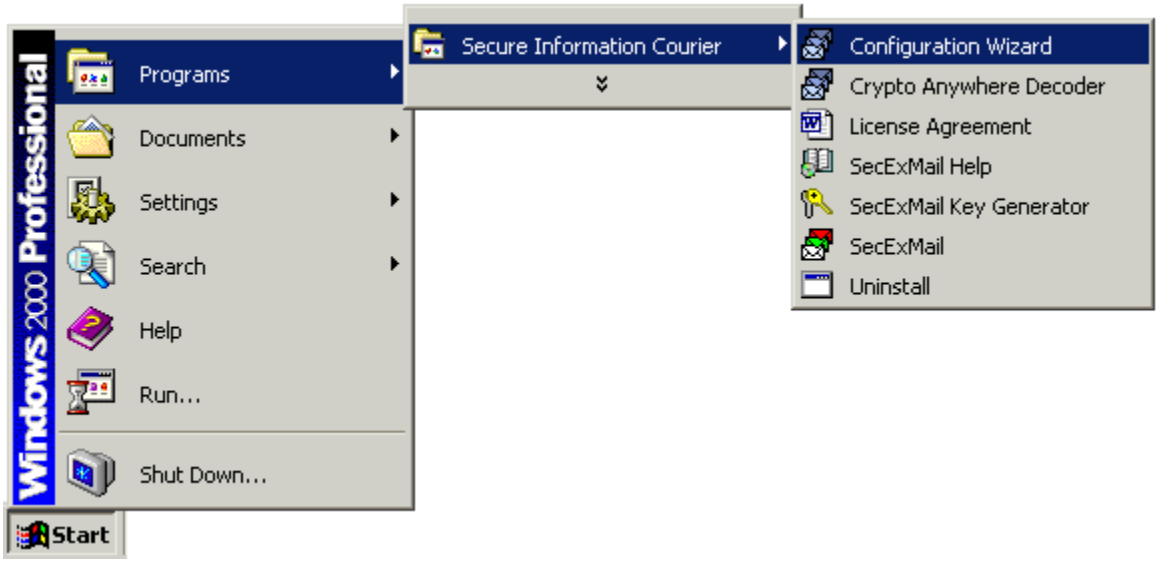




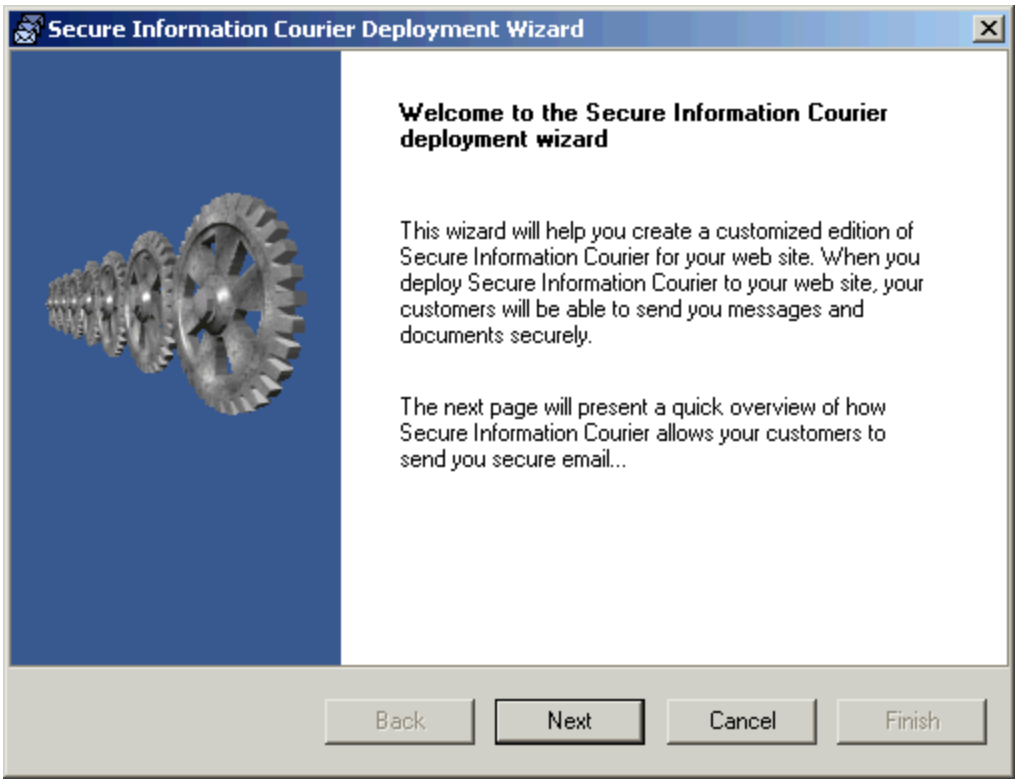
2 Customizing

2.1 Basic Configuration

Secure Information Courier can be customized with your own corporate logo and your own message prompts. You can define default message recipients and pre-load Secure Information Courier with your very own encryption keys, ensuring that only authorized recipients may decrypt and read email from your customers. Configuration is easy. Simply follow the steps outlined by the configuration wizard. To launch the configuration wizard, click Start, Programs, Secure Information Courier and select Configuration Wizard as shown in the illustration depicted below.



This will invoke the configuration wizard welcome screen.



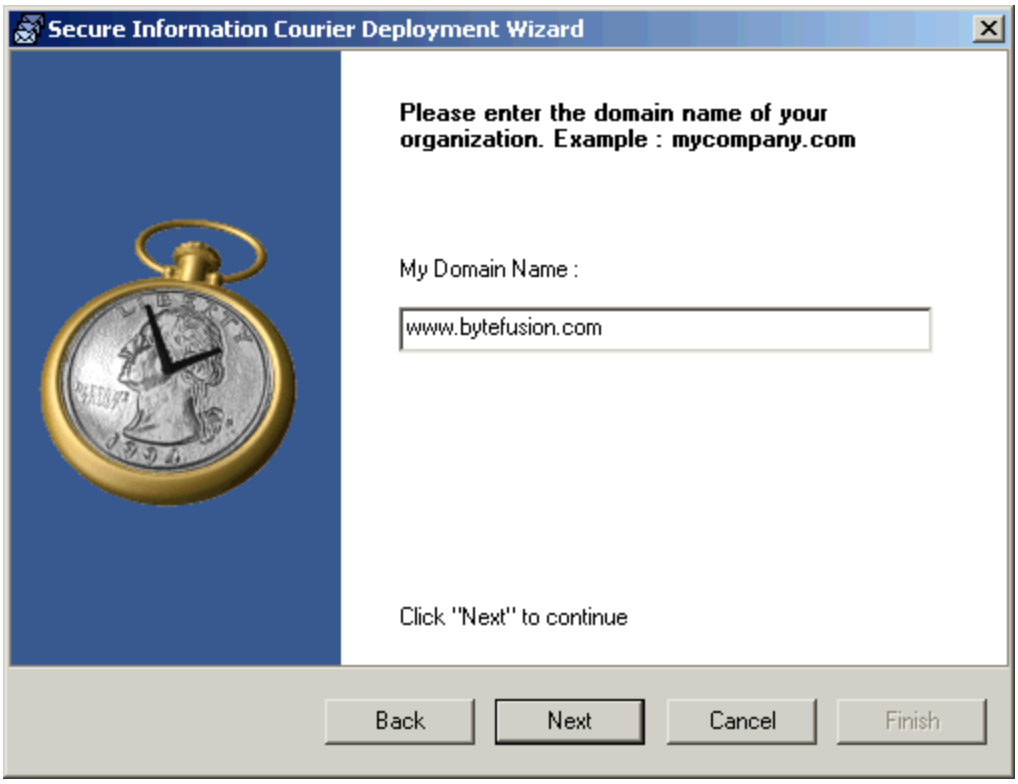
2.2 How Secure Information Courier works

Once Secure Information Courier (SIC) is deployed on your website, customers can download SIC and send email and documents securely and directly to your mail server. Mail is never stored on the servers of the customer's ISP. SIC is deployable as both a downloadable executable as well as an activex control which integrates with your website. Repeat visitors to your website who send secure email to

your organization on a regular basis, might wish to download the SIC executable while casual visitors to your website might find an integrated solution easier to use. The graphic depicted below illustrates the process.

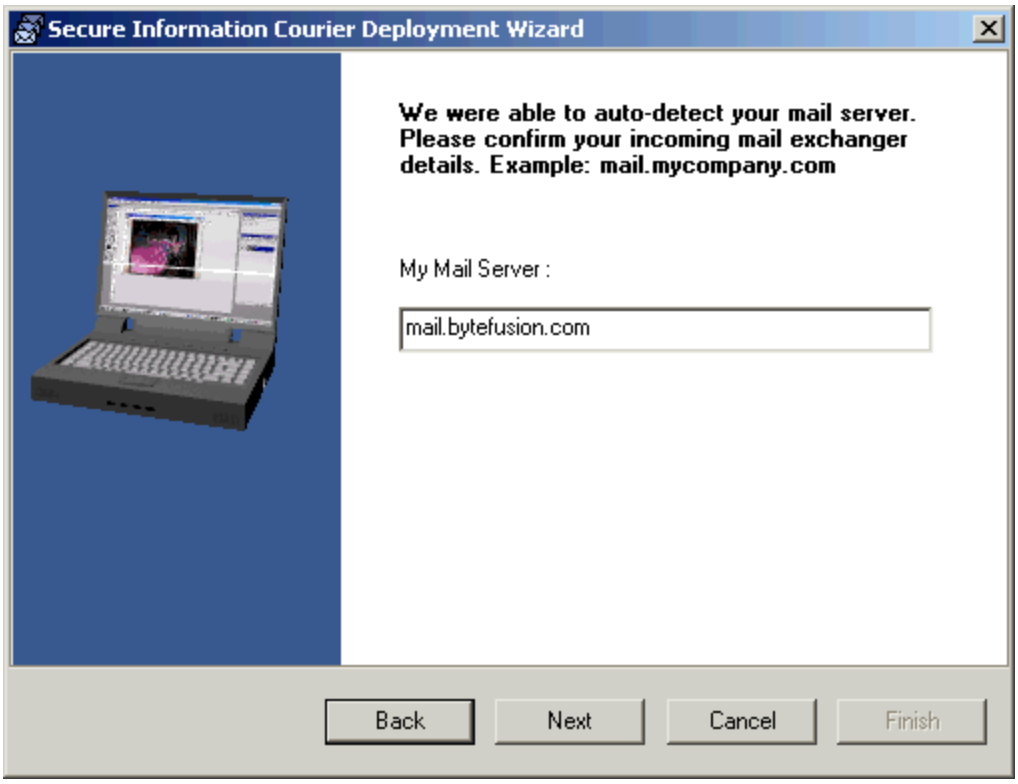
2.3 Domain Configuration

Firstly, you will need to provide the name of your organization's internet domain. This information will be used to auto-detect your organization's mail server(s). You may enter the name of your web site, e.g. *www.bytefusion.com*, or your domain name only, e.g. *bytefusion.com*.



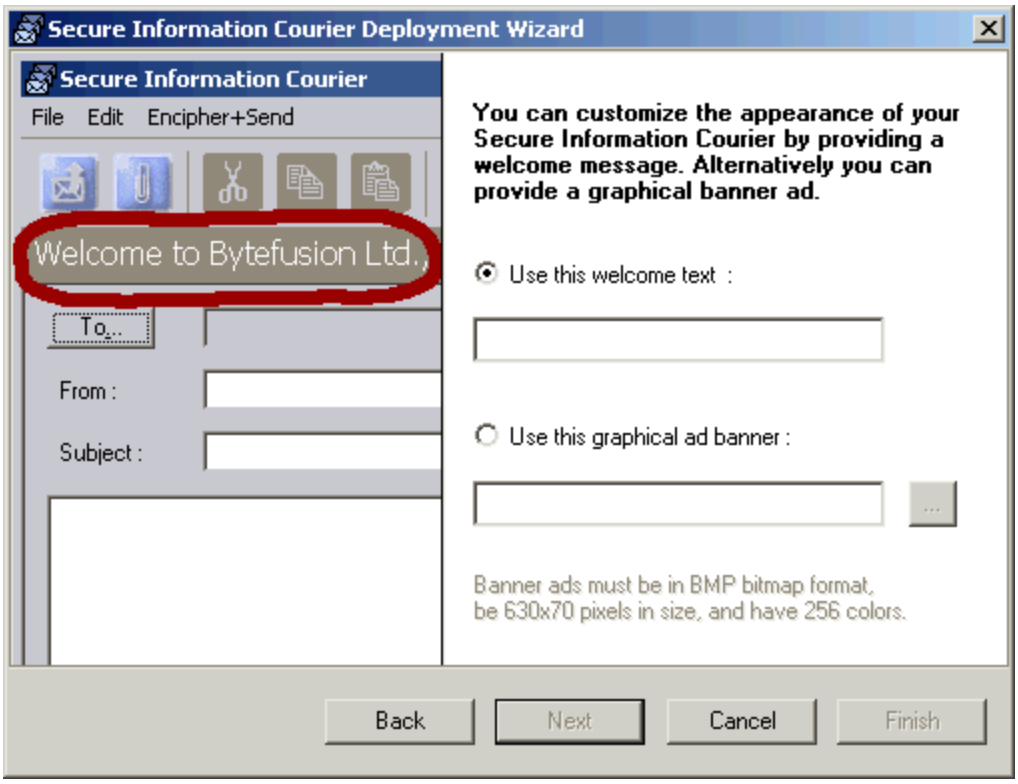
2.4 Confirm Incoming Mail Server

If the Secure Information Courier Wizard was able to auto-detect your incoming SMTP mail transfer agent, you will be prompted to confirm this setting. It is safe to accept the default. If auto-detection failed, kindly ask your system administrator to provide you with the IP address or DNS name of your incoming SMTP mail transfer agent and enter it in the "***My Mail Server***" field as indicated below.



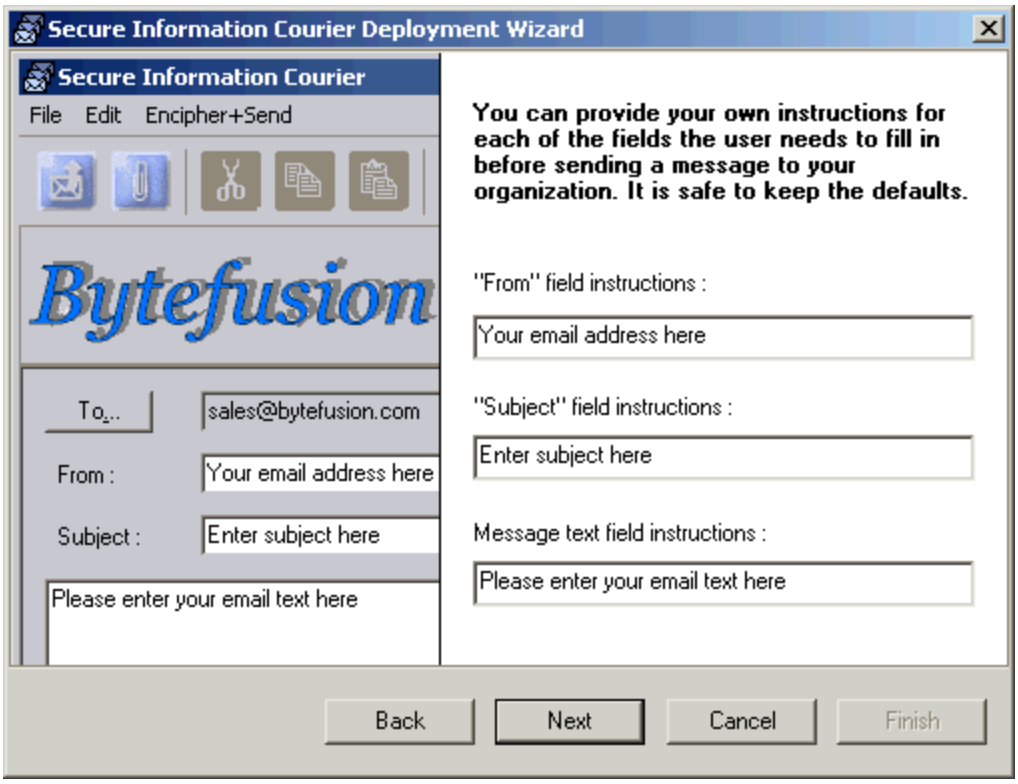
2.5 Graphical User Interface

You may customize the physical appearance of Secure Information Courier with your own welcome text or corporate logo. When providing your own corporate logo or banner ad, kindly note that the required file format is "***BMP***", ***630x70 pixels***, using a maximum of ***256 colors***.



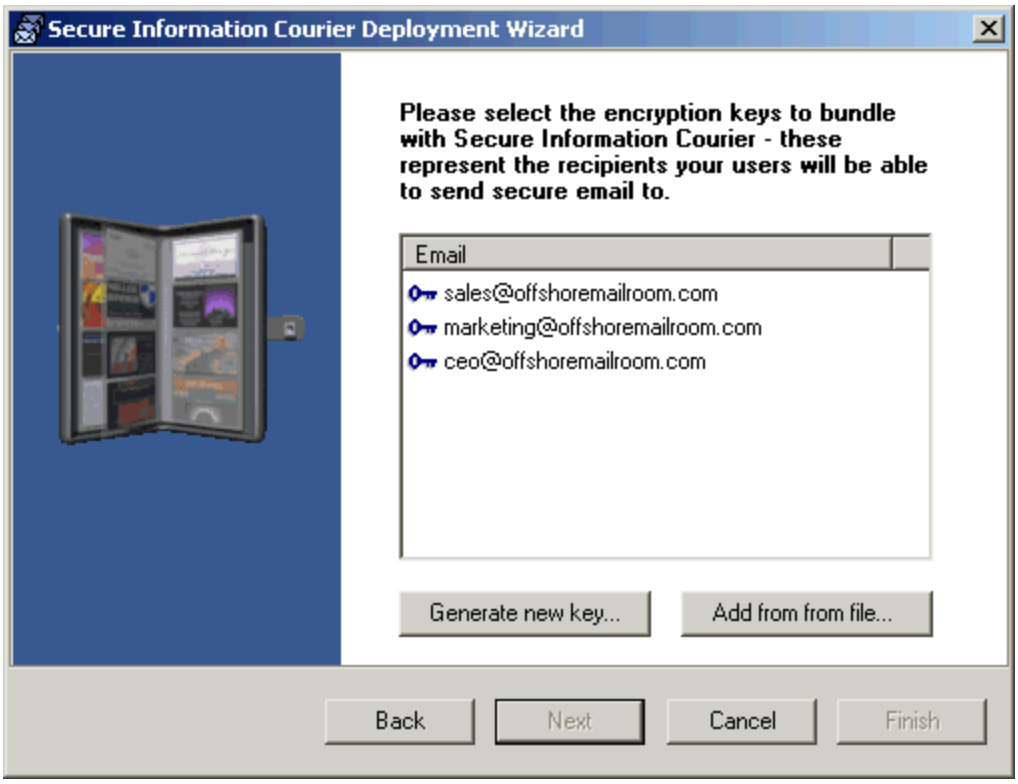
2.6 Message Prompts

You can provide your own instructions for each of the fields the user needs to fill in before sending a message to your organization. It is safe to keep the defaults.



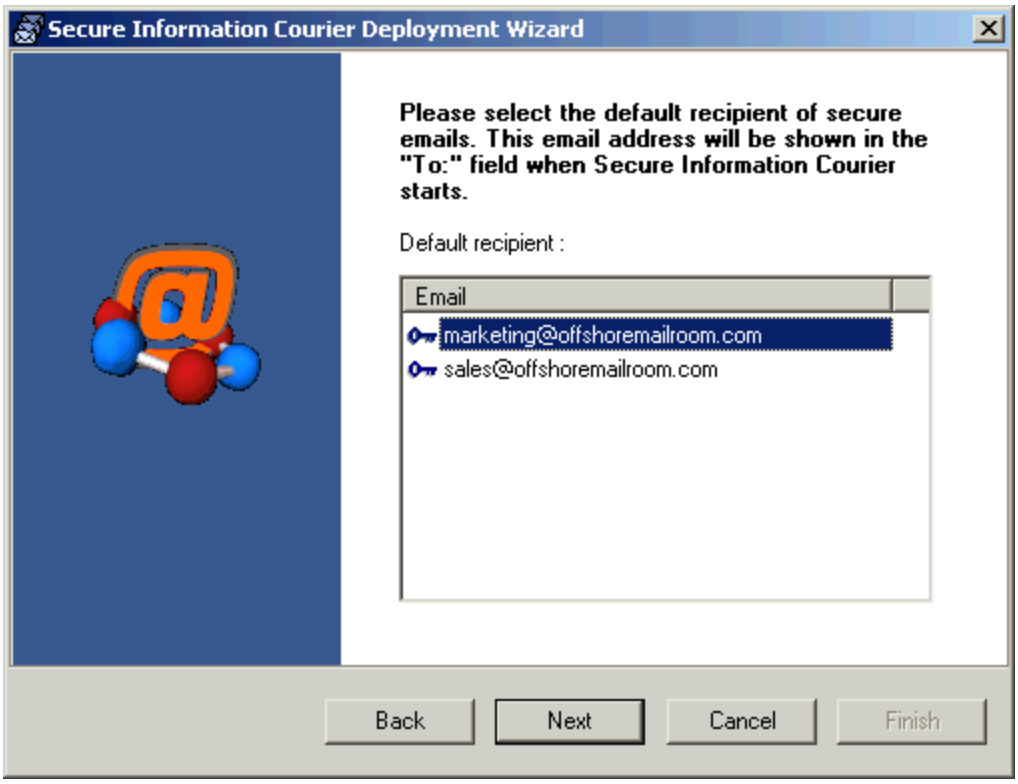
2.7 Encryption Key Selection

Secure Information Courier employs public key infrastructure (PKI) encryption keys. See also Secure Information Courier / SecExMail Keys. This technology ensures that only authorized recipients will be able to decrypt messages sent to your organization. If you have existing SecExMail keys, these will be auto-detected by the configuration wizard. If you have existing SecExMail or Crypto Anywhere keys on floppy or other removable medium, you may import these using the "***Add from file***" button. If you are new to SecExMail based encryption technology and require new encryption keys, please click "***Generate new key***" now and follow the steps outlined in the key generation wizard. Keys you generate here will be automatically available for decryption of messages in both Crypto Anywhere Decoder as well as SecExMail SOHO.



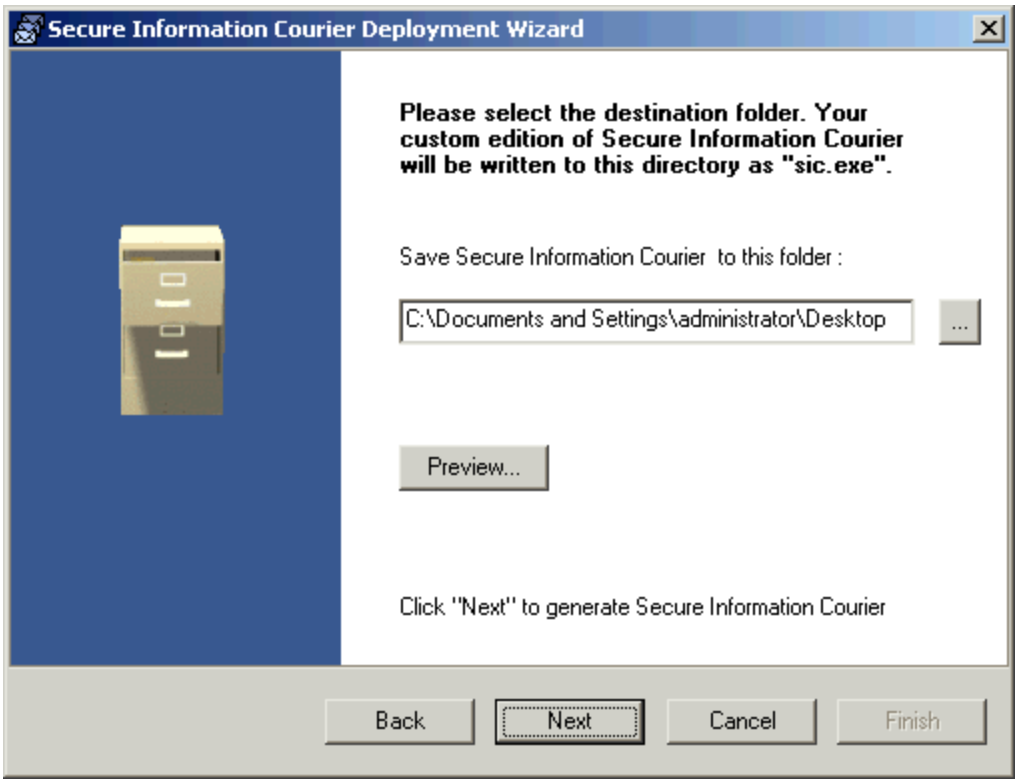
2.8 Default Message Recipient

Please select the default recipient of secure emails. This email address will be shown in the "***To:***" field when Secure Information Courier starts. Users will be able to override this selection with any one or multiple authorized recipients whom you have specified on the encryption key selection page.



2.9 Destination Folder

Please select the destination folder. Your custom edition of Secure Information Courier will be written to this directory as the file "sic.exe". Optionally, you may preview your custom edition of Secure Information Courier using the "***Preview***" button.

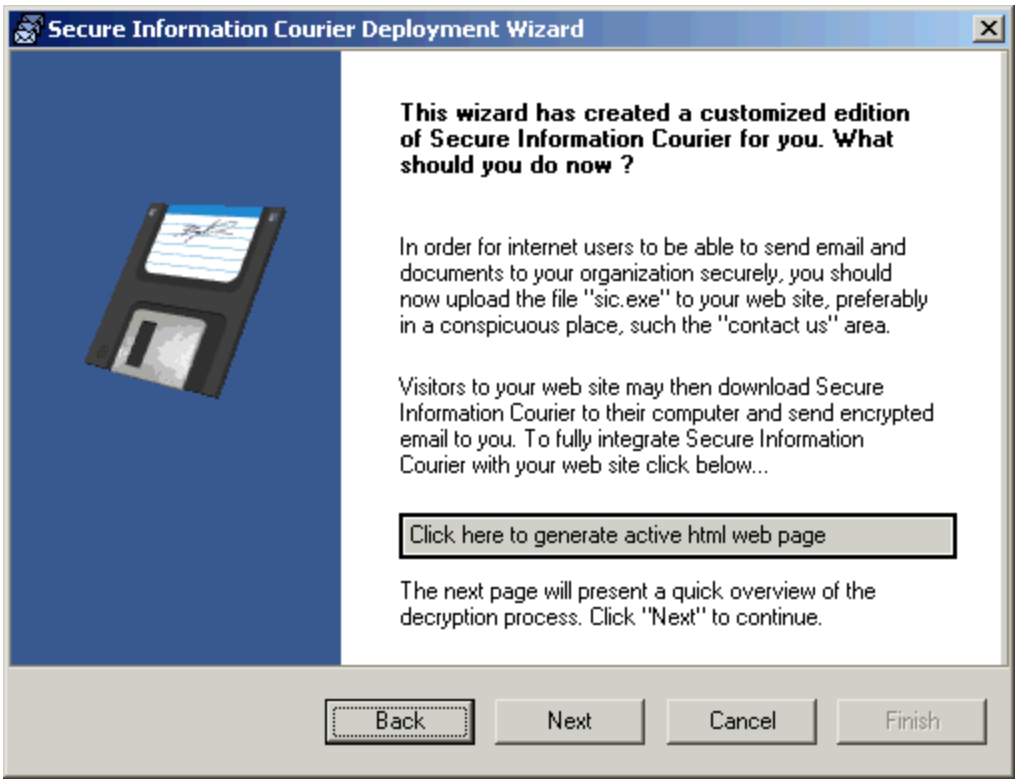


2.10 ActiveX HTML Page

This wizard will have created a customized edition of Secure Information Courier for you.

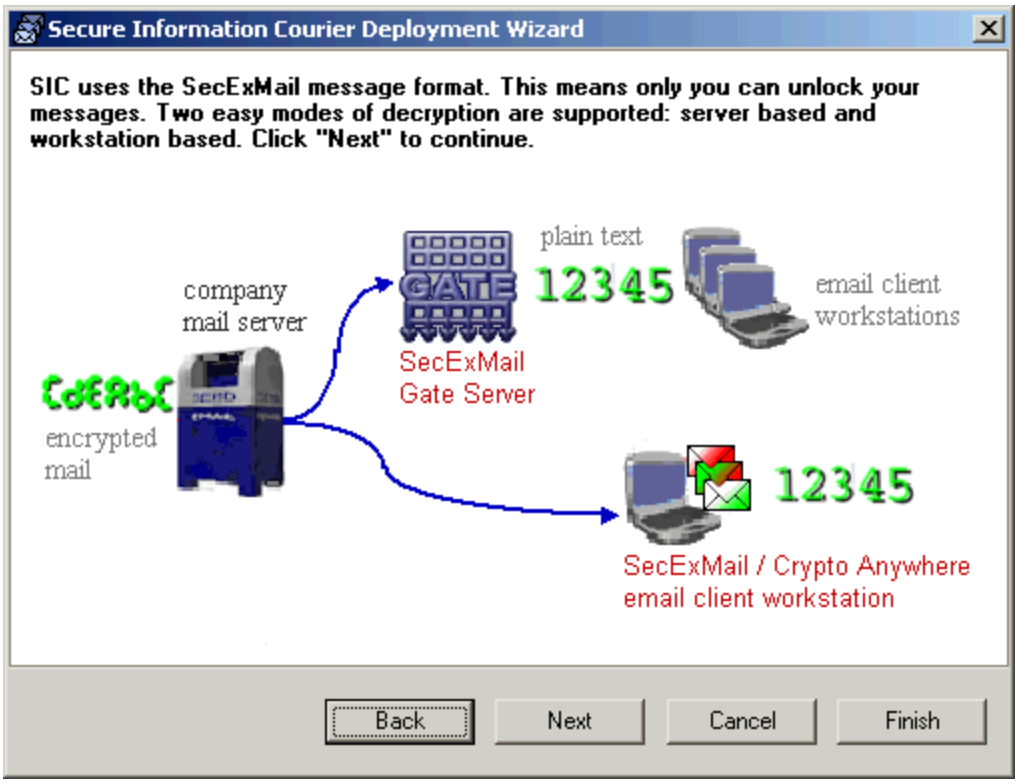
In order for internet users to be able to send email and documents to your organization securely, you should now upload the file "***sic.exe***" to your web site, preferably in a conspicuous place, such the "***contact us***" area.

Visitors to your web site may then download Secure Information Courier to their computer and send encrypted email to you. To fully integrate Secure Information Courier with your web site you might also whish to generate an accompanying HTML page and associated ActiveX control. To do this click the button labeled "***Click here to generate active html web page***".



2.11 Putting it all together

SIC uses the SecExMail message format. This means only you can unlock your messages. Two easy modes of decryption are supported: server based and workstation based.



2.12 Security Advice

Secure Information Courier is hosted on your website. If you have stringent security requirements, you might want to consider the use of a secure website using the HTTPS protocol also. The certificate mechanism used in HTTPS authenticates your website to visitors and gives visitors to your website the confidence that your web pages are not being misrepresented by a third party.

3 Decryption

3.1 Decryption Methods

Secure Information Courier ships with two workstation based decryption tools :

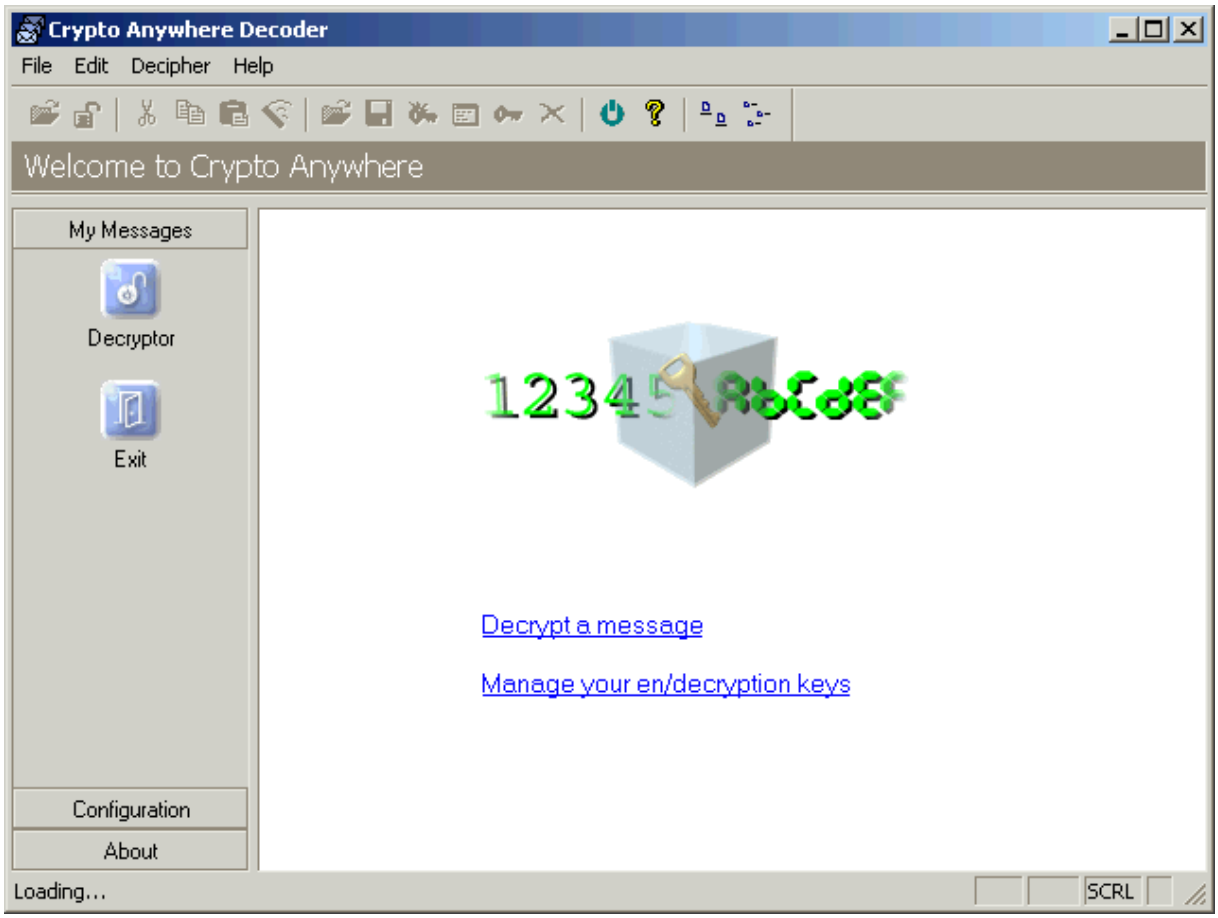
1) Crypto Anywhere Decoder. Decrypt messages in two easy steps by first copying them from your email client to the Windows clipboard and then pasting them into Crypto Anywhere Decoder.

2) SecExMail SOHO : Decrypt messages invisibly in the background. SecExMail will inter-operate with all SMTP/POP3 email client software.

Alternatively you may wish to consider centralized, server based decryption using the SecExMail Gate Server. Kindly visit our website at www.bytefusion.com for more information.

3.2 Crypto Anyhwhere Decoder

Crypto Anywhere Decoder allows you to easily decrypt messages in two easy steps by first copying them from your email client to the Windows clipboard and then pasting them into Crypto Anywhere Decoder. Visit Crypto Anywhere on our website at www.bytefusion.com for more information.



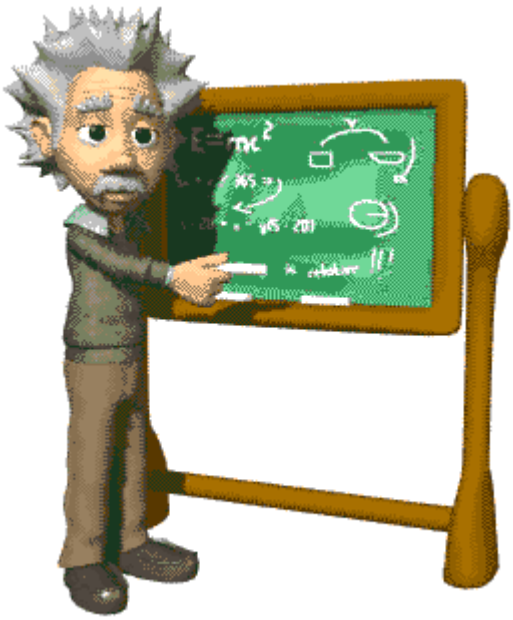
3.3 SecExMail SOHO

SecExMail SOHO allows you to decrypt messages invisibly in the background. SecExMail is compatible with all SMTP/POP3 compliant email client software. Please visit SecExMail on our website www.bytefusion.com for more information about SecExMail.

4 Technical

4.1 RSA Public Key Encryption

"c = me mod n" is the algorithm that turns the world of e-commerce. Introduced in 1978 by Rivest, Shamir and Adleman after whom the cipher is named, RSA is the worlds foremost public key encryption system. Contrary to the design of classic encryption algorithms where the same key is used to lock and unlock the information, public key encryption relies on "two key" algorithms. The sender encrypts the message with the recipients public key who, upon receipt of the message, is able to decipher the same with the private key counterpart. This development was revolutionary in the field of cryptography because parties wishing to establish secure communications no longer had to meet in "secret" to exchange confidential keying information.

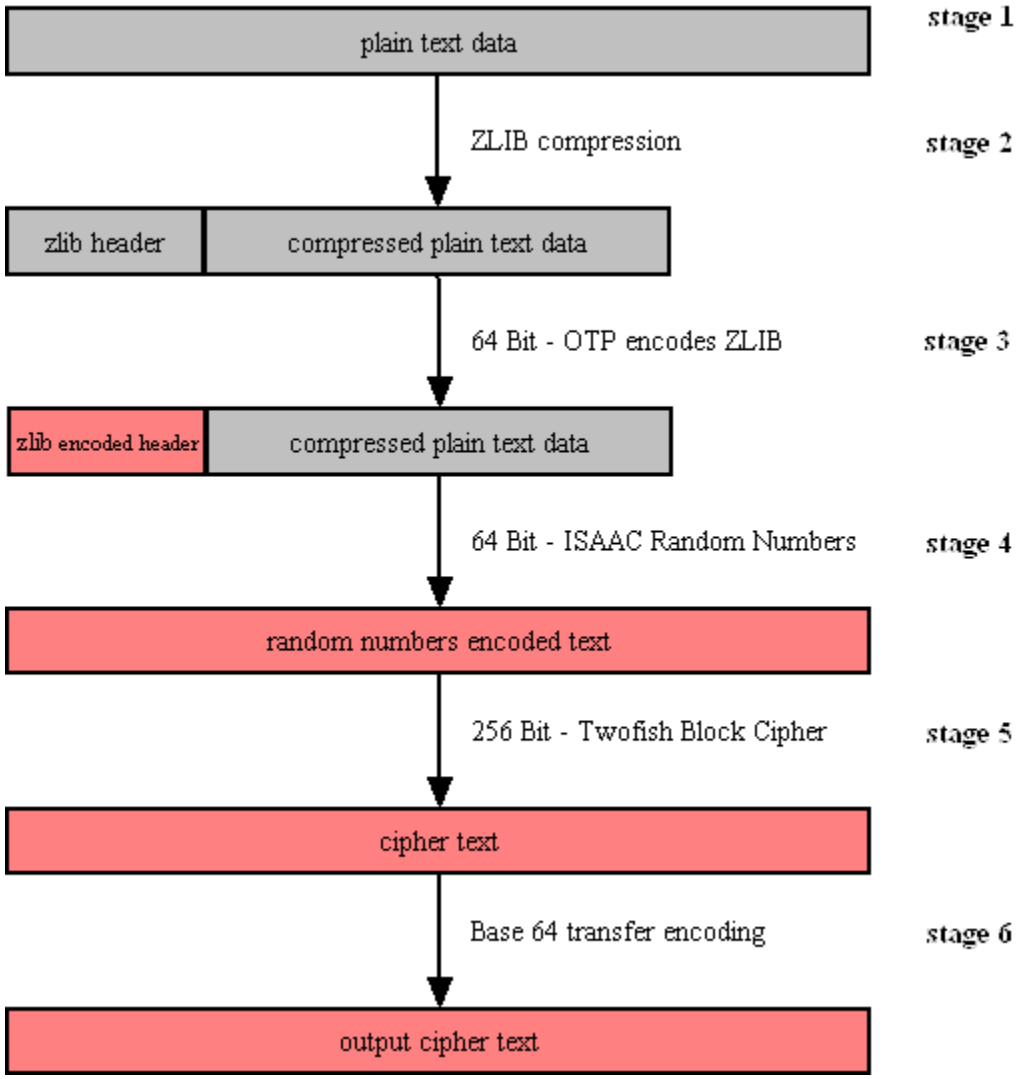


The SecExMail public key infrastructure uses industry standard RSA encryption as developed by the OpenSSL project.
See Acknowledgements.

4.2 Secure Information Courier / SecExMail Encryption

SecExMail encryption uses the Twofish block cipher in conjunction with the ISAAC random number generator and is optimized to operate on real-time email streams. It uses cryptographic primitives which are available to the general public and have been subject to extensive peer review. SecExMail encryption incorporates RSA public key encryption. Message encryption is performed via the Twofish block cipher and the ISAAC random number generator. SecExMail is warranted to be free from spy-ware, key escrow or key recovery features of any kind. The email encryption process is described in detail below. See diagram.

SecExMail Encryption



- **Stage 1**

  Email data is received in variable length data blocks. SecExMail parses SMTP header info, mail and data bodies.

- **Stage 2**

  Because email messages frequently contain known plain text, such as salutation and or tag lines, which gives rise to known plain text attacks on the encrypted message and in order to minimize overall message expansion, the plain text is first compressed using the ZLIB compression algorithm. The net effect of deflating large amounts of data, containing both tidbits of known plain text such as greeting or tag lines as well as unknown message text into a compressed data stream is that any known plain text is effectively obscured.

- **Stage 3**

  The ZLIB stream has a fixed header format which in itself might be exploited as known plain text by a savvy cryptanalyst. For this reason, the first 64 bits of the steam are encoded by way of a

One Time Pad, using standard XOR masking. This approach acknowledges that email messages will contain portions of known plain text and proactively manages this problem.

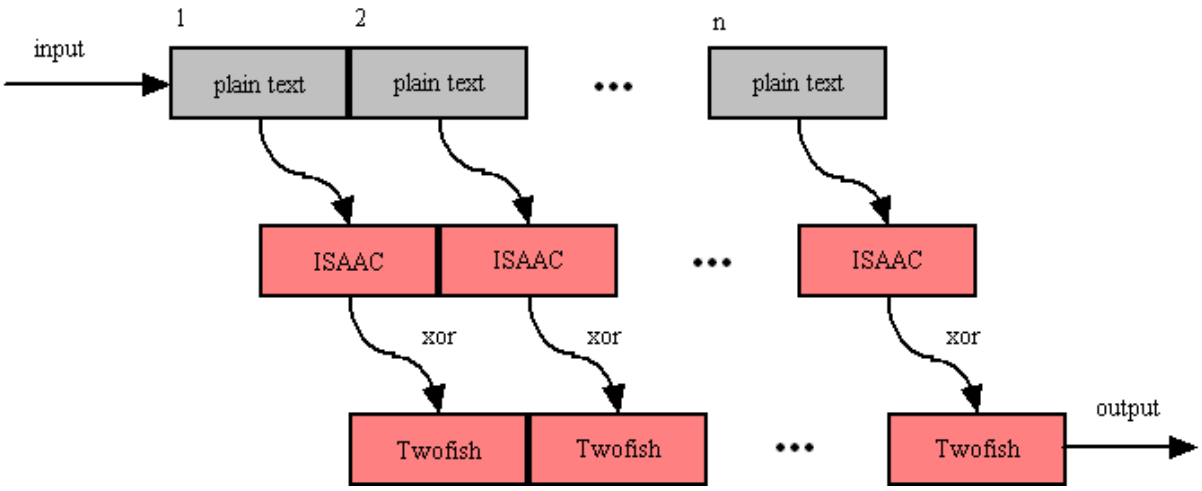
- **Stage 4**

  At this point the compressed data is XOR'ed using the 64 bit ISAAC random number stream.

- **Stage 5**

  The next step in the encryption process is to encrypt the random number encoded text using the 256 bit Twofish block cipher. Twofish is used in chained block mode. Instead of XOR'ing the previous block's cipher text into the plain text of the current block, the output from the ISAAC layer is "chained in". This chaining process is illustrated below.

Twofish Block Chaining



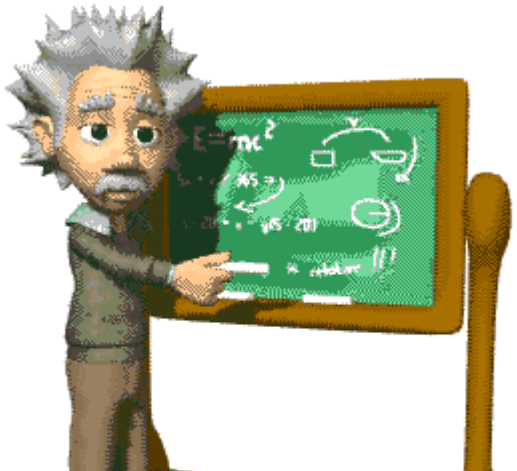
- **Stage 6**

The final step is to assemble the output in base64 transfer encoded format for transmission via mail transfer agents (MTA).

4.3 ISAAC Random Number Generator

ISAAC (Indirection, Shift, Accumulate, Add, and Count) is a cryptographically secure pseudo random number generator. With an average cycle length of 2 to the 8295th power its output is uniformly distributed and unpredictable. ISAAC has been developed by Bob Jenkins and placed into the public domain in 1996. See Acknowledgements for legal information on ISAAC.

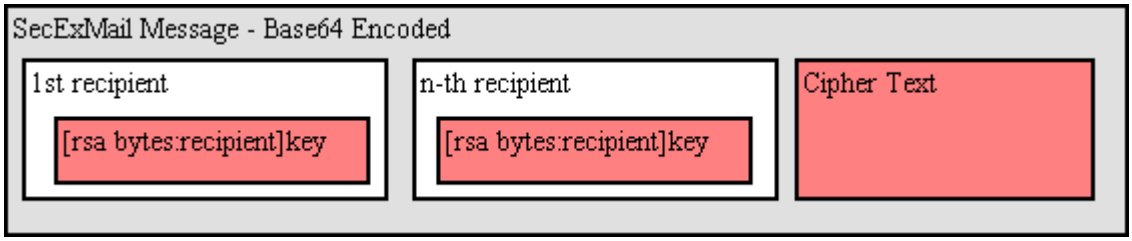
ISAAC is at the heart of SecExMail's entropy collection system.



4.4 SecExMail Message Format

SecExMail messages are transferred in base64 encoded format. Messages may be encrypted to multiple recipients. The internal message layout is defined as follows :

[<rsa bytes>:<recipient>]key[<rsa bytes>:<recipient>]key...cipher text



- **RSA Bytes**

  This is the size of the recipient's RSA key in bytes. Therefore a 2048 bit RSA key would be listed as having a size of 256 bytes. RSA This parameter is defined for RSA key sizes of 2048, 4096, and 8192 bits.

- **Recipient**

  This is the email address of the recipient to whom the message is encoded.

- **Key**

  This is the SecExMail session key material, encrypted with the RSA public key of the recipient. The SecExMail session key is used to encrypt the message body of the email message and is comprised
  of a 64 bit One Time Pad key, a 64 bit ISAAC random number generator key, and a 256 bit Twofish key.

- **Cipher Text**

  This is the message body encrypted using SecExMail Encryption.

A typical SecExMail message is depicted below :

```
--Begin SecEx 1.1--
WzI1NjpjaHJpc0BvZmZzaG9yZW1haWxyb29tLmNvbV0dJyyJnwwCm0659zpBY/asERA3FRG99
OYRhm5f+rwohYORt8Wp3rmwI2Nguhk38KvH5pg8ZRTXXWiEHYMakQPPXpJepJFZeXTcNMTi/d
p0Rc5HCTui5okW/00Gv8Sp328Ldh3DlgQcGW7oYt9qxG/cJ/PaVxxDM3I4cnsCyLjfX+I0JY6
h+emWt4U/N6u+K0tPL4ua2OfGhGoBXo+6KK042bXGpk/Pj6WEOQMc+VrsOx6ZcTgpqS3WCcUc
2/JDy9zHqlkPLohXcT4G2Hiwp/1JhviaQtoKA2NYYimuY5ZjNUGPMs0h6AKS3/qZsHhK1LtcA
WpLnuoFbQleekuJngBCC1RIlIlI4lfFgMkxoUkZrtXg6E217Q6GMMhNJ4EU3D2c1BgauDYAQG
Rpz0p8efm/WAZoXai6KVElMEiK7tv98s8wu9LpUxN44QYj2eNRVI+GPfkBoKvr6eK5/TU4cHN
Dg9VxCGj4n8KDvfYsPRpBSNzLL+Ta4iz7toQ/MGdPCQa
--End SecEx Mail--
```

4.5 One-Time Pads

A one-time pad is a block of random data used to encrypt a block of equal length plain text data. Encryption is usually by way of XOR'ing the one-time pad with the message text. This process may be thought of as a 100% noise source used to mask the message. The one-time pad is secure if it is comprised of random data and is never reused. Because of this, one-time pads have limited application in modern ciphers, but are commonly acknowledged as the holy grail of cryptography.

SecExMail uses one-time pads to encrypt the ZLIB compression header in SecExMail messages.

4.6 Secure Information Courier / SecExMail Keys

SecExMail employs public key encryption. Messages are encrypted to one or more recipients using their **public keys**. Only the intended recipient can, upon receipt of the message, recover the plain text using his/her **private key**. Public key encryption differs from classical encryption because the recipient of a message does not use the same key for decryption as the sender used for encryption.

In cryptography the fictional characters "Alice" and "Bob" are often used for illustration purposes. Consider the following scenario : Alice lives in New York and Bob lives in Los Angeles. Alice wants Bob to be able to send her confidential mail. She goes to her local hardware store and purchases a dozen or so combination padlocks, sets the unlocking code on each padlock, confuses the dials again, and sends the open padlocks to Bob in Los Angeles.

Bob is now in possession of Alice's padlocks, but not the unlocking codes. When Bob wants to send Alice a confidential letter, he places the letter inside a steel box and locks it with one of Alice's padlocks. Once the padlock is snapped shut, even he himself cannot re-open the box since he is not in possession of the combination which will release the lock. Only Alice will be able to open the box and therefore read the letter once she has received Bob's parcel in the mail.

Public key encryption works much in the same manner. The **public key** may be thought of as an open, electronic padlock. You can send this electronic padlock to all your friends. Your friends may then use that padlock to secure their emails to you in an electronic box. This electronic box is the encrypted email. Upon receipt of the encrypted email, you dial the secret combination which is your **private key**

and retrieve the original message.

SecExMail does all this for you.

5 About

5.1 About Secure Information Courier

Secure Information Courier
Version 1.2

5.2 About Bytefusion Ltd.

Bytefusion Ltd.
22 Duke Street
Douglas, IOM
IM1 2AY
British Isles

Inquiries: sales@bytefusion.com

5.3 System Requirements

- **System Administrator Workstation Disk Space:** 7.5 MB of free disk space.
- **Operating System Compatibility:**

  Administrator Workstation - Configuration Wizard: Windows NT, 2000, XP
  Secure Information Courier Web Executable : Windows 95/98/Me + Windows NT/2000/XP
  Secure Information Courier ActiveX Control : Microsoft Internet Explorer 4.0 +

- **Web Site Hosting :** Any HTTP compliant web server, such as Apache or Microsoft IIS
- **Web Site Space :** 441KB (activex control). 888K (sic.exe).

5.4 License - Retail

Secure Information Courier

READ THE FOLLOWING LICENSE IN IT'S ENTIRETY BEFORE USING THIS SOFTWARE:

DEFINITIONS. LICENSEE shall mean you as an individual user. LICENSOR shall mean Bytefusion Ltd. SOFTWARE shall mean Secure Information Courier, also referred to as SIC.

This End User License Agreement (hereafter referred to as "EULA") is a legal agreement between LICENSEE AND LICENSOR governing the use of SOFTWARE. By using SOFTWARE you agree to be bound by all of the terms of this EULA. SOFTWARE is protected by international copyright laws and treaty provisions. LICENSOR retains all intellectual property rights to SOFTWARE.

GRANT OF LICENSE. SOFTWARE is licensed, not sold. LICENSOR hereby grants LICENSEE the right to install and use on a single computer one copy of the SOFTWARE for each license purchased. A license for SOFTWARE may not be shared or used concurrently on more than one computer. You may not rent or lease SOFTWARE. You may not reverse engineer, decompile, or disassemble SOFTWARE.
SOFTWARE contains components which are designed to be put on LICENSEE website for the purpose of allowing customers of LICENSEE to communicate securely with LICENSEE. This Agreement includes those elements and LICENSEE agrees that these elements shall contain a license number linking LICENSEE to the published elements. LICENSEE further agrees not to modify these elements in any way so as to attempt to hide license numbers.

WARRANTY. This SOFTWARE is supplied "as is." To the maximum extend permitted by applicable law, LICENSOR, distributors and suppliers disclaim all warranties, expressed or implied, including without limitation the warranties of merchantability and of fitness for any purpose. To the maximum extend permitted by applicable law, in no event shall LICENSOR, distributor or suppliers be liable for damages of any kind, direct, indirect, special, incidental, or consequential, which may result from the use of SOFTWARE or the inability to use SOFTWARE.

REVOCATION. Without prejudice to any other rights, LICENSEE's right to use SOFTWARE is automatically terminated if LICENSEE fails to comply with the terms and conditions of this EULA. In such event, LICENSEE must destroy all copies of SOFTWARE and all of its component parts.

ENTIRETY. This EULA supersedes any prior agreement or understanding, whether written or oral, between LICENSOR and LICENSEE.

SEVERABILITY. You agree that if any term or condition of this EULA is declared invalid, it shall not affect the remaining terms or conditions which shall remain binding.

LICENSOR may update this license from time to time and you agree to be bound by the terms of any subsequent updates.

UNCLEAR ELEMENTS OF AGREEMENT
If LICENSEE is in any way unclear about or does not understand the terms of this Agreement or believes there to be different interpretations of any clause of this Agreement, they must contact LICENSOR immediately. LICENSOR maintains the right to clarify the intended meaning of any clause or element of this Agreement and the new text or clause shall become a binding element of this Agreement.

GOVERNING LAW. This EULA is governed by the laws of the Isle of Man. You hereto irrevocably attorn to the jurisdiction of the courts of the Isle of Man.

SPECIAL CONDITIONS ON USE OF SOFTWARE.

SOFTWARE CONTAINS STRONG ENCRYPTION, THE USE OF WHICH MAY BE RESTRICTED IN CERTAIN JURISDICTIONS. USE OF SOFTWARE IS HEREBY RESTRICTED, IN ADDITION TO THE RESTRICTIONS STIPULATED IN THIS EULA, TO INCLUDE RESTRICTIONS APPLICABLE IN THE JURISDICTION OF LICENSEE. SENDING ENCRYPTED MAIL OR MAKING AN ENCRYPTED EMAIL SERVICE AVAILABLE MIGHT CONSTITUTE EXPORT IN SOME JURISDICTIONS. LICENSEE IS RESPONSIBLE FOR ENSURING COMPLIANCE WITH ALL APPLICABLE LAWS. FURTHERMORE, LICENSEE IS SPECIFICALLY PROHIBITED FROM USING SOFTWARE FOR THE PURPOSES OF COMMUNICATING CHILD PORNOGRAPHY OR ORGANIZING CRIMINAL ACTS OR COMMUNICATING WITH KNOWN CRIMINALS OR CRIMINAL ORGANIZATIONS. IN ADDITION TO THE ABOVE RESTRICTIONS, PERSONS WHO RESIDE IN ANY COUNTRY WHICH IS LISTED OR BECOMES LISTED AS EMBARGOED BY THE UNITED NATIONS WITH REGARD TO EXPORT OF ENCRYPTION SOFTWARE, ARE HEREBY NOT LICENSED TO USE SOFTWARE. TRANSPORT, ELECTRONIC OR OTHERWISE, OF SOFTWARE TO SUCH COUNTRIES IS EXPRESSLY FORBIDDEN AND MAY CONSTITUTE A CRIME IN SOME JURISDICTIONS.

5.5 License - Evaluation

Secure Information Courier
Evaluation Edition

READ THE FOLLOWING LICENSE IN IT'S ENTIRETY BEFORE USING THIS SOFTWARE:

DEFINITIONS. LICENSEE shall mean you as an individual user. LICENSOR shall mean Bytefusion Ltd. SOFTWARE shall mean Secure Information Courier, also referred to as SIC.

This End User License Agreement (hereafter referred to as "EULA") is a legal agreement between LICENSEE AND LICENSOR governing the use of SOFTWARE. By using SOFTWARE you agree to be bound by all of the terms of this EULA. SOFTWARE is protected by international copyright laws and

treaty provisions. LICENSOR retains all intellectual property rights to SOFTWARE.

GRANT OF LICENSE. SOFTWARE is licensed, not sold. LICENSOR hereby grants LICENSEE the right to install and use SOFTWARE exclusively for the purpose of evaluation of SOFTWARE. All other uses require the purchase of a license. You may not rent or lease SOFTWARE. You may not reverse engineer, decompile, or disassemble SOFTWARE.
SOFTWARE contains components which are designed to be put on LICENSEE website for the purpose of allowing customers of LICENSEE to communicate securely with LICENSEE. This evaluation edition of SOFTWARE specifically excludes the right to place any component of SOFTWARE on a publicly accessible site. For the purpose of this Agreement, a publicly accessible site is any site that can be accessed by persons other than LICENSEE or employees of LICENSEE located at the same physical address sharing the same post code.

WARRANTY. This SOFTWARE is supplied "as is." To the maximum extend permitted by applicable law, LICENSOR, distributors and suppliers disclaim all warranties, expressed or implied, including without limitation the warranties of merchantability and of fitness for any purpose. To the maximum extend permitted by applicable law, in no event shall LICENSOR, distributor or suppliers be liable for damages of any kind, direct, indirect, special, incidental, or consequential, which may result from the use of SOFTWARE or the inability to use SOFTWARE.

REVOCATION. Without prejudice to any other rights, LICENSEE's right to use SOFTWARE is automatically terminated if LICENSEE fails to comply with the terms and conditions of this EULA. In such event, LICENSEE must destroy all copies of SOFTWARE and all of its component parts.

ENTIRETY. This EULA supersedes any prior agreement or understanding, whether written or oral, between LICENSOR and LICENSEE.

SEVERABILITY. You agree that if any term or condition of this EULA is declared invalid, it shall not affect the remaining terms or conditions which shall remain binding.

LICENSOR may update this license from time to time and you agree to be bound by the terms of any subsequent updates.

UNCLEAR ELEMENTS OF AGREEMENT
If LICENSEE is in any way unclear about or does not understand the terms of this Agreement or believes there to be different interpretations of any clause of this Agreement, they must contact LICENSOR immediately. LICENSOR maintains the right to clarify the intended meaning of any clause or element of this Agreement and the new text or clause shall become a binding element of this Agreement.

GOVERNING LAW. This EULA is governed by the laws of the Isle of Man. You hereto irrevocably attorn to the jurisdiction of the courts of the Isle of Man.

SPECIAL CONDITIONS ON USE OF SOFTWARE.

SOFTWARE CONTAINS STRONG ENCRYPTION, THE USE OF WHICH MAY BE RESTRICTED IN CERTAIN JURISDICTIONS. USE OF SOFTWARE IS HEREBY RESTRICTED, IN ADDITION TO THE RESTRICTIONS STIPULATED IN THIS EULA, TO INCLUDE RESTRICTIONS APPLICABLE IN THE JURISDICTION OF LICENSEE. SENDING ENCRYPTED MAIL OR MAKING AN ENCRYPTED EMAIL SERVICE AVAILABLE MIGHT CONSTITUTE EXPORT IN SOME JURISDICTIONS. LICENSEE IS RESPONSIBLE FOR ENSURING COMPLIANCE WITH ALL APPLICABLE LAWS. FURTHERMORE, LICENSEE IS SPECIFICALLY PROHIBITED FROM USING SOFTWARE FOR THE PURPOSES OF COMMUNICATING CHILD PORNOGRAPHY OR ORGANIZING CRIMINAL ACTS OR COMMUNICATING WITH KNOWN CRIMINALS OR CRIMINAL ORGANIZATIONS. IN ADDITION TO THE ABOVE RESTRICTIONS, PERSONS WHO RESIDE IN ANY COUNTRY WHICH IS LISTED OR BECOMES LISTED AS EMBARGOED BY THE UNITED NATIONS WITH REGARD TO EXPORT OF

ENCRYPTION SOFTWARE, ARE HEREBY NOT LICENSED TO USE SOFTWARE. TRANSPORT, ELECTRONIC OR OTHERWISE, OF SOFTWARE TO SUCH COUNTRIES IS EXPRESSLY FORBIDDEN AND MAY CONSTITUTE A CRIME IN SOME JURISDICTIONS.

5.6 Acknowledgements

- **ISAAC Random Number Generator**

  At the time of writing, the ISAAC home page can be found at http://burtleburtle.net/bob/rand/isaacafa.html.
  ISAAC has been placed into the public domain by its author, Bob Jenkins in 1996.

  My random number generator, ISAAC.
  (c) Bob Jenkins, March 1996, Public Domain
  You may use this code in any way you wish, and it is free. No warrantee.

- **RSA Public Key Encryption**

  The RSA algorithm was patented until September 2000 when RSA® Security Inc. released the algorithm into the public domain. *"BEDFORD, Mass., September 6, 2000 -- RSA® Security Inc. (NASDAQ: RSAS) today announced it has released the RSA public key encryption algorithm into the public domain, allowing anyone to create products that incorporate their own implementation of the algorithm."* At the time of writing a copy of this statement can be found at http://www.rsasecurity.com/news/pr/000906-1.html

- **Twofish Block Cipher**

  The Twofish block cipher by Counterpane Labs was developed and analyzed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson. Twofish was one of the five Advanced Encryption Standard finalists. At the time of writing the Twofish homepage can be found at http://www.counterpane.com/twofish.html. The cipher has been made available to the general public by the following statement on http://www.counterpane.com/about-twofish.html :

  " Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses. Everyone is welcome to download Twofish and use it in their application. There are no rules about use, although I would appreciate being notified of any commercial applications using the algorithm so that I can list them on this website. "

- **Info-ZIP Library**

  This is version 2003-May-08 of the Info-ZIP copyright and license. The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

  Copyright (c) 1990-2003 Info-ZIP. All rights reserved.

  For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

  Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P.

Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

- **ZLIB Compression Library**

ZLIB is a lossless data-compression library written by Jean-loup Gailly and Mark Adler. ZLIB is made
available as free, unpatented software to the general public at http://www.gzip.org/zlib/. The license conditions are set forth at http://www.gzip.org/zlib/zlib_license.html and reproduced below :

```
" Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty.  In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
   claim that you wrote the original software. If you use this software
   in a product, an acknowledgment in the product documentation would be
   appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not
be
   misrepresented as being the original software.
3. This notice may not be removed or altered from any source
```

```
distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu "
```

- **RIPEMD-160**

  The RIPE message digest was written by Antoon Bosselaers for Katholieke Universiteit Leuven, Department of Electrical Engineering ESAT/COSIC, Belgium. License conditions ask us to quote the following :

```
" RIPEMD-160 software written by Antoon Bosselaers,
available at http://www.esat.kuleuven.ac.be/~cosicart/ps/AB-9601/ "
```

- **Viking Art - SecExMail Logo**

  Katja Bengtsson of Brisbane, Australia (katja@offshoremailroom.com)

- **OpenSSL Project**

  SecExMail contains cryptographic software from the OpenSSL project at www.openssl.org which is licensed under a "*BSD-style*" open source licenses. These licenses asks us to state the following :

```
"This product includes software developed by the OpenSSL Project for use
in the OpenSSL Toolkit. (http://www.openssl.org/)"

"This product includes cryptographic software written by  Eric Young
(eay@cryptsoft.com). This product includes software written by Tim Hudson
(tjh@cryptsoft.com)."
```

  SecExMail is an independent, derived work and no endorsement of SecExMail by the OpenSSL project is implied. The full text of the OpenSSL license and the original SSLeay License is reproduced below.

```
OpenSSL License

================================================================
Copyright (c) 1998-2001 The OpenSSL Project.  All rights reserved.

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

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.

3. All advertising materials mentioning features or use of this
   software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project
   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
   endorse or promote products derived from this software without
```

prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

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

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

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The licence and distribution terms for any publicly available version or
derivative of this code cannot be changed.  i.e. this code cannot simply
be
copied and put under another distribution licence
[including the GNU Public Licence.]
```

- **SecExMail Encryption**

  Chris Kohlhepp and Mark Robertson, Bytefusion Ltd.