Zarafa
Outlook sharing & Webaccess

www.zarafa.com

Zarafa S/MIME Webaccess Plugin User Manual

Client side configuration and usage.

Addresses

Zarafa
Schieweg 2
2627 AN Delft
The Netherlands

Zarafa S/MIME Webaccess plugin provides S/MIME functionality, for receiving and sending encrypted and / or sign messages using Zarafa Webaccess Interface.

Table of contents

1 Zarafa Webaccess

1.1 Introduction

The Zarafa S/MIME plugin enables the Webaccess users to send and received encrypted and / or signed messages based on the S/MIME protocol.

1.2 Features

- Support for Firefox browsers on Windows and Linux (other platforms maybe working)
- Receiving encrypted messages
- Verifying signed messages
- Sending encrypted messages

- Sending signed messages
- Sending encrypted and signed messages

1.3 Known limitations

- No support for multiple recipients of encrypted messages
- No support for verifying signatures of encrypted messages.
- Support for Mozilla Firefox only.

1.4 S/MIME Certificate providers

Free or commercial certificates are available from the following sources. Please note that most free certificates offered usually include some form of restricted usage.

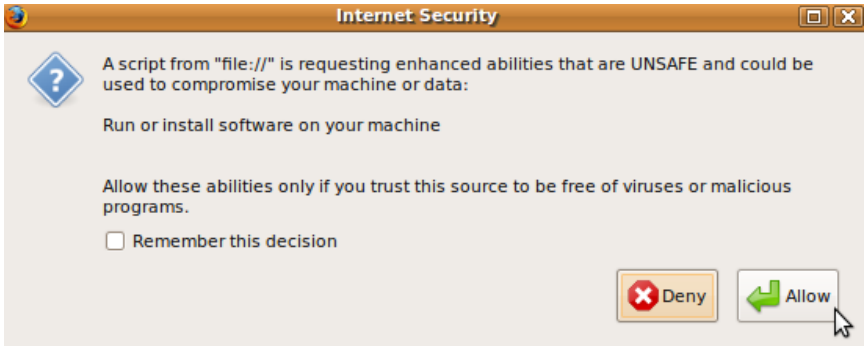
- InstantSSL / Comodo
- VeriSign
- GlobalSign
- Cacert (CAcert is NOT one of the trusted authorities built-in to FireFox and ThunderBird.)
- Secorio

1.5 Configuration

For the S/MIME plugin to work configuration of the Firefox Browser is needed. The webaccess plugin must be permitted to use Firefox XPCOM functions for encrypting, decrypting and signing of S/MIME messages. If your Zarafa Webaccess already has the zarafa-smime plugin installed you can configure your browser by visiting the following address

http://<ip-address>/webaccess/plugins/smime/userconf.php

You will be prompted to download the zarafaconf.html file which you should save in your local disk. After downloading, open the zarafaconf.html file with Firefox and permit the file to configure your web browser by clicking “Allow”. See screenshot 1



Screenshot 1

If the configuration is successful you will be presented with a file selection box which you can use to insert your personal certificate(s) to Firefox Certificate Manager. The certificates must be in PCKS-12 format.

Security Note: By configuring Firefox to permit access to the Zarafa Webaccess site to XPCOM

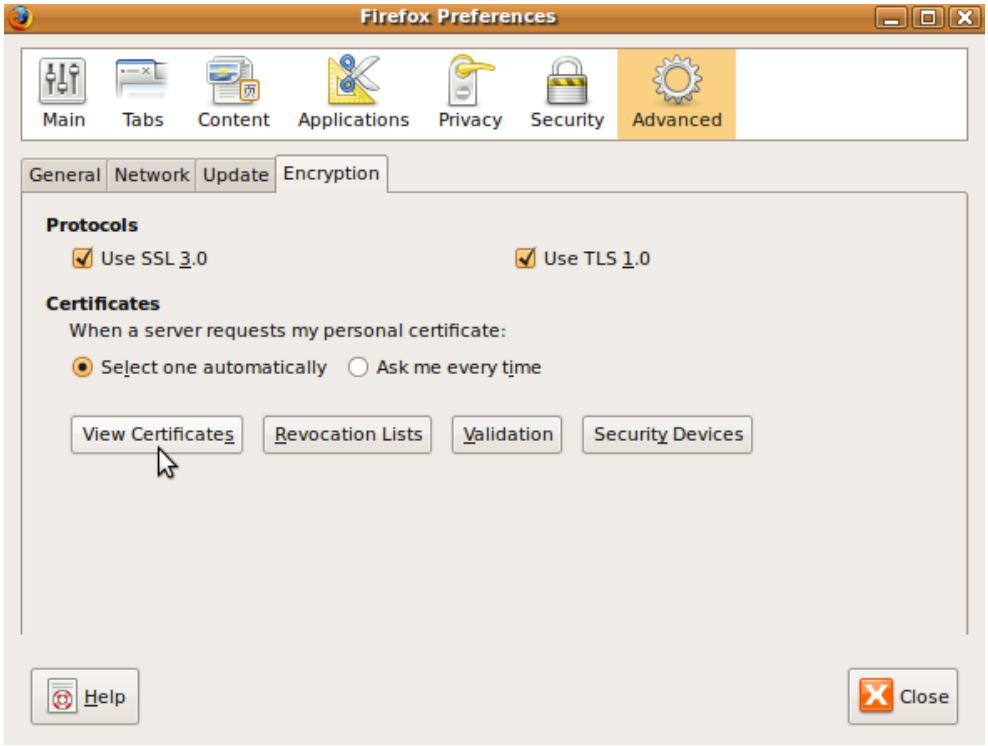
components, you permit your Zarafa Webaccess site to remotely access files in your computer and execute programs on your computer with more permissions compared to a typical web page. It is advised that the S/MIME Webaccess plugin is used with a trusted Webaccess server.

1.6 Certificate Management

The S/MIME Webaccess plugin uses Firefox build-in certificate manager to access the private and the public keys needed for sending and receiving S/MIME messages. To manage your certificates you can access Firefox Certificate manager:

- On Linux: Edit → Preferences → Advanced → Encryption → View Certificates
- On Windows: Tools → Options → Advanced → Encryption → View Certificates

See screenshot 2



Screenshot 2

You can import, delete, backup your personal certificates under the “Your Certificates” tab. Similarly you can manage public certificates under the “People” tab. For more information please visit Mozilla Firefox Knownledge Base http://support.mozilla.com/en-US/kb/Options+window+-+Advanced+panel?style_mode=inproduct#Certificates

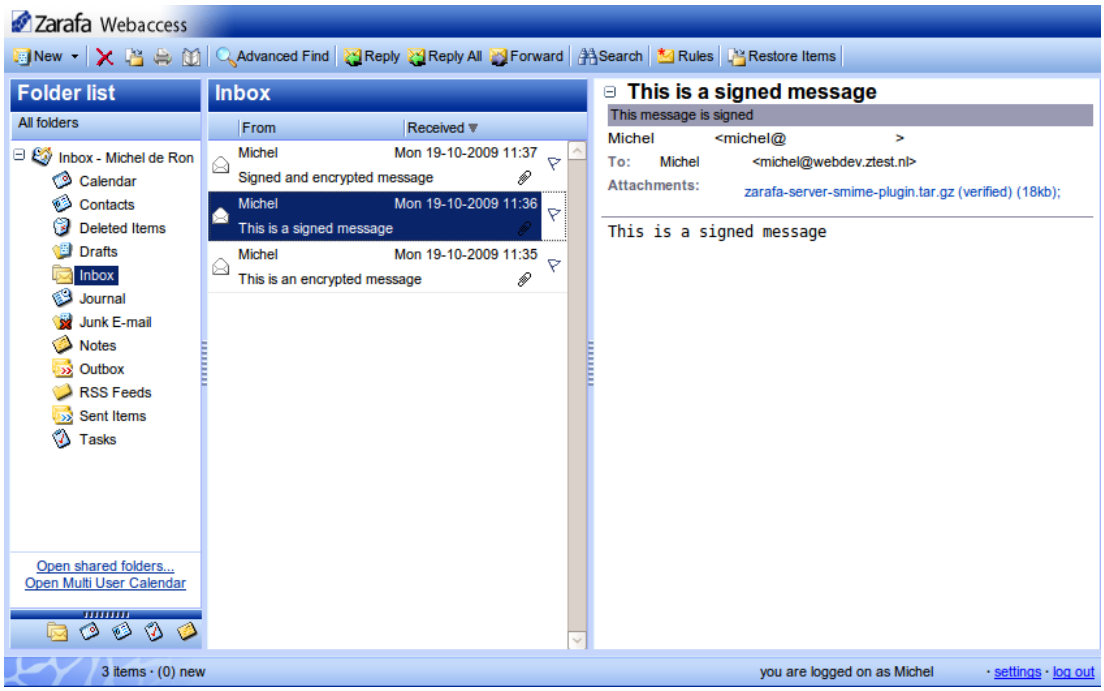
1.7 Receiving S/MIME Emails

1.7.1 Signed Emails

Signed S/MIME emails are automatically handled by the server to check if the signature is valid or not. A signature is valid when the contents of the message, namely the body and the attachments, have not been altered by any way by a person other than the signer of the email. When a message is verified as valid an extra information bar is displayed with the message “This message is signed”. For each verified signed attachment the text “verified” is displayed next to the filename. See screenshot 3

If the body of the email or the attachments have been altered the email is not considered valid and the

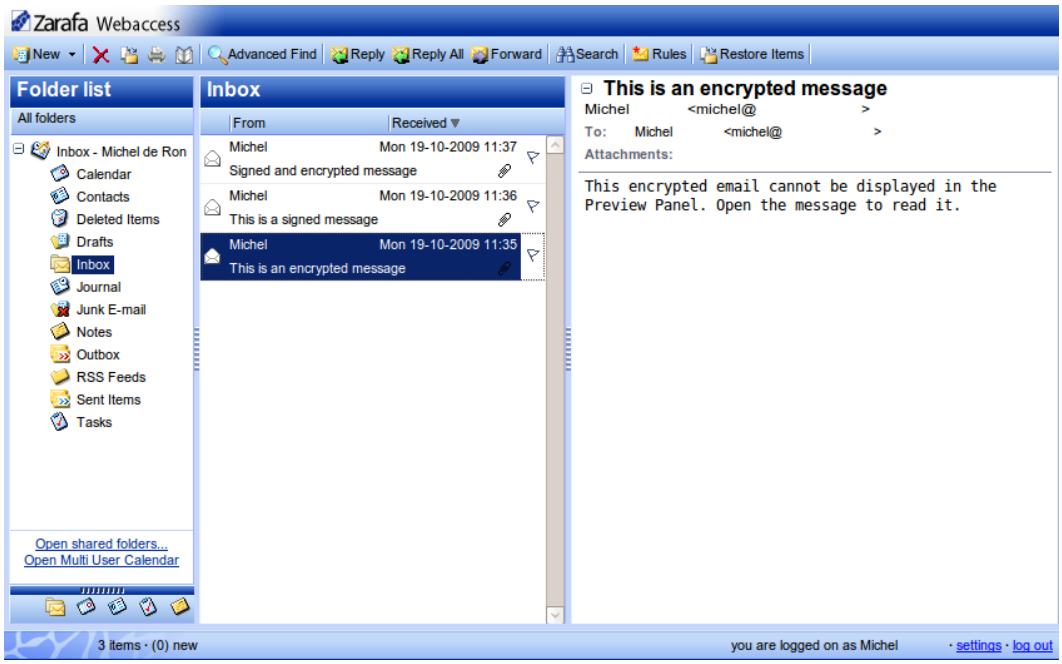
message “This message is signed but we cannot verify the signature. Maybe the contents of the message have been altered.” is displayed.



Screenshot 3

1.7.2 Encrypted Emails

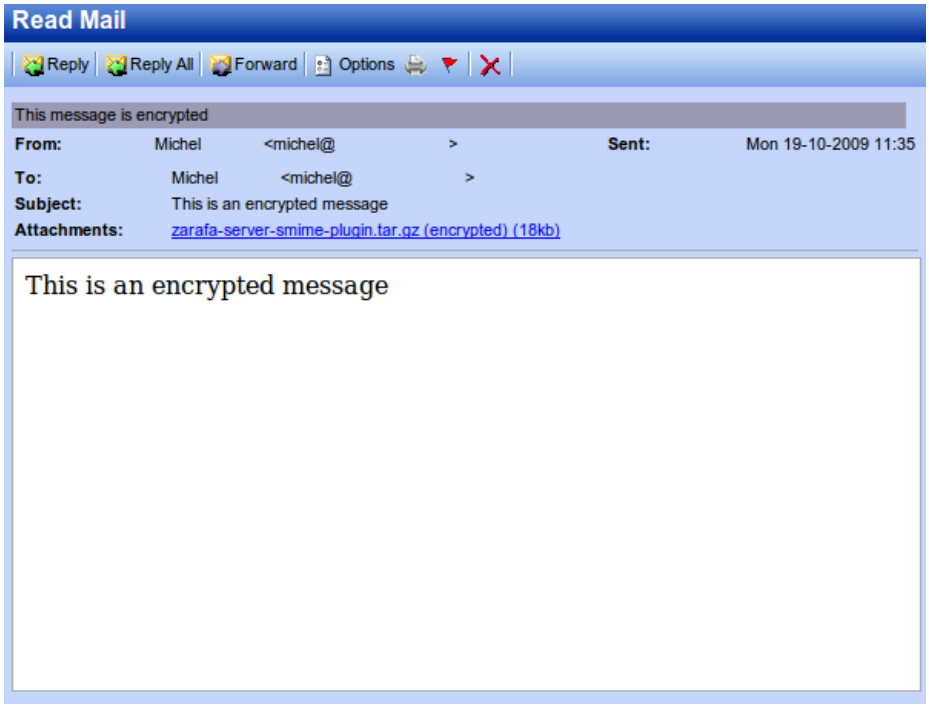
Encrypted emails are automatically downloaded to user's browser and decrypted using the private certificates in Firefox's Certificate Manager. For security reasons the encrypted emails are not displayed in Preview mode. Instead of the actual message the following text is displayed “This encrypted email cannot be displayed in the Preview Panel. Open the message to read it.”



Screenshot 4

Double clicking the message will open the message window and the browser will decrypt the message body and the attachments using one of your privates certificates stored in Firefox's Certificate Manager. The extra info bar “This message in encrypted” will be displayed. For each encrypted attachment the text “encrypted” is displayed next to the filename. See screenshot 5. The attachments are downloaded,

decrypted and saved to your computer by the time you open the message. The attachments get saved in user's temporary directory provided by the operating system and get instantly deleted from the filesystem when user closes the message window.



Screenshot 5

1.7.3 Encrypted and Signed Emails

Encrypted and signed emails are automatically downloaded to user's browser and decrypted using the private certificates in Firefox's Certificate Manager. Encrypted and signed emails are treated as encrypted emails, currently there is no support for verifying content body and attachments of encrypted messages. See paragraph 1.6.2 and screenshot 6.

Screenshot 6

1.8 Sending S/MIME Emails

The Zarafa S/MIME Webaccess plugin enables the user to send Encrypted and / or Signed emails using the S/MIME standard. When the S/MIME plugin is installed and enabled the “Create Email” window features two new buttons, “Encrypt” and “Sign”.

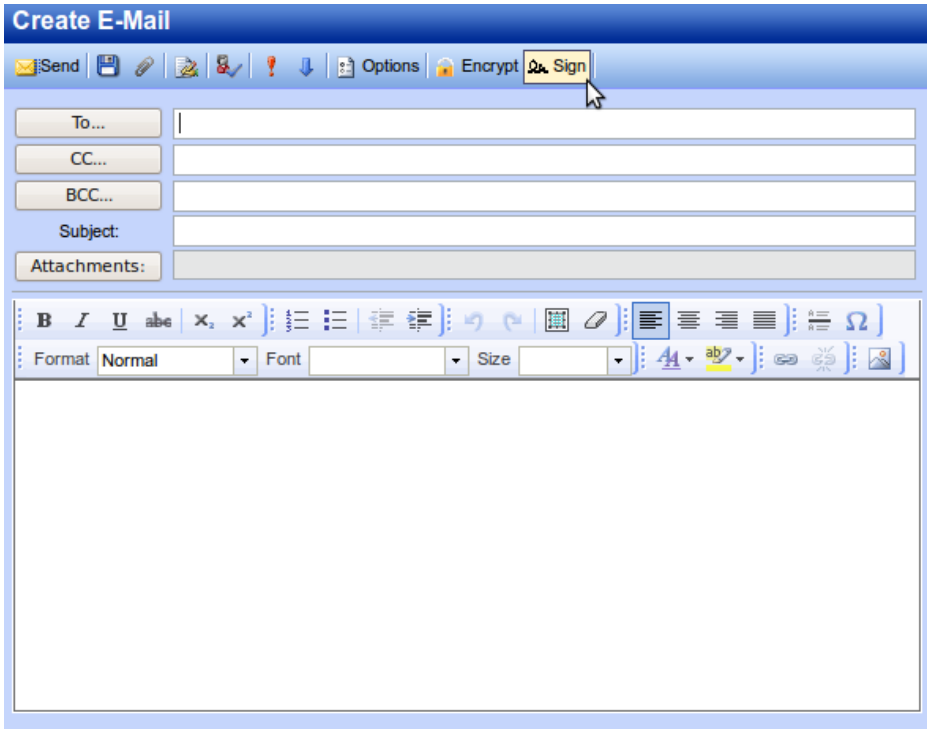
1.8.1 Signed Emails

To send a signed email the “Sign” button must be checked. See screenshot 7

When the “Send” button is clicked the message body and the attachments (if available) will be enclosed in a virtual envelop and you will be asked to select a certificate to sign this message. Selecting a Signing Certificate, filling in the correct Firefox Master Password (if applicable) and clicking “OK” will sign and send the message. See screenshot 8.

Note that signing generates high CPU usage and may cause temporary browser freezing for messages, of combined body and attachments of 2Mb or more.

If there are no certificates for signing the message “You don't have certificates for signing” will be displayed and the sending procedure will be canceled. The user should either install the private certificates in Firefox's Certificate Manager (see paragraph 1.5) or uncheck the “Sign” button.



Screenshot 7

Screenshot 8

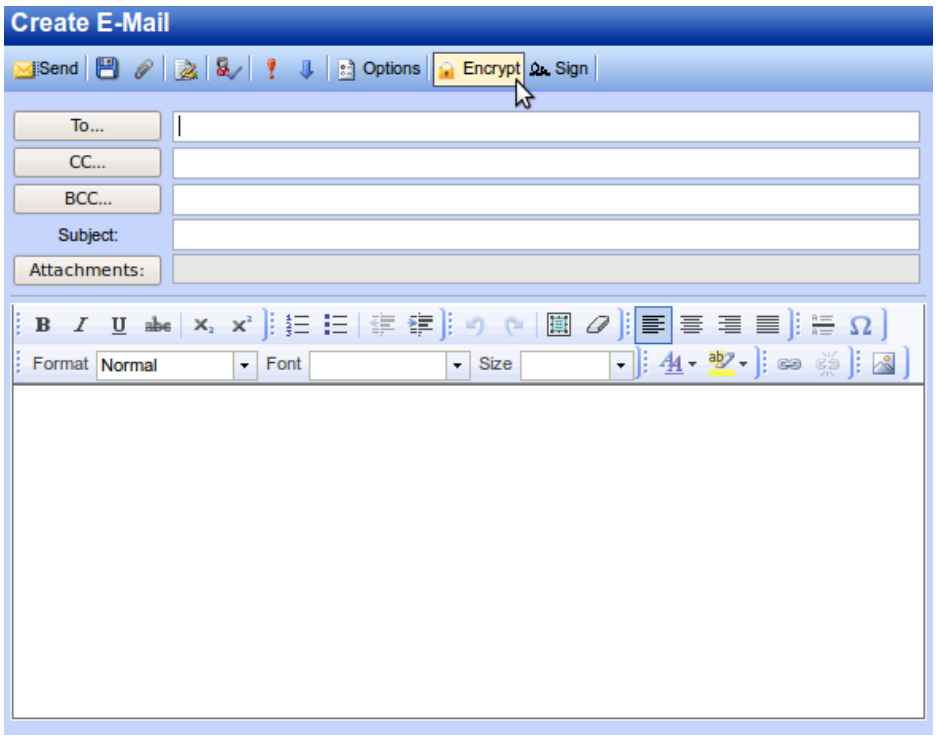
1.8.2 Encrypted Emails

To send an encrypted email the “Encrypt” button must be checked. See screenshot 9.

When the “Send” button is clicked the message body and the attachments (if available) will be enclosed in a virtual envelop, which will get encrypted using the recipient's public certificate.

The plugin will look for the recipient's certificate is Firefox Certificate Manager, using the email address of the recipient. If no certificate's for the recipient is found the following message will be displayed “Error: Certificate for email 'michel@' not found! Try installing the certificate using firefox's certificate manager or uncheck 'encrypt' button” and the sending procedure will be canceled.”. The user should either install the public certificate in Firefox's Certificate Manager (see paragraph 1.5) or uncheck the “Encrypt” button.

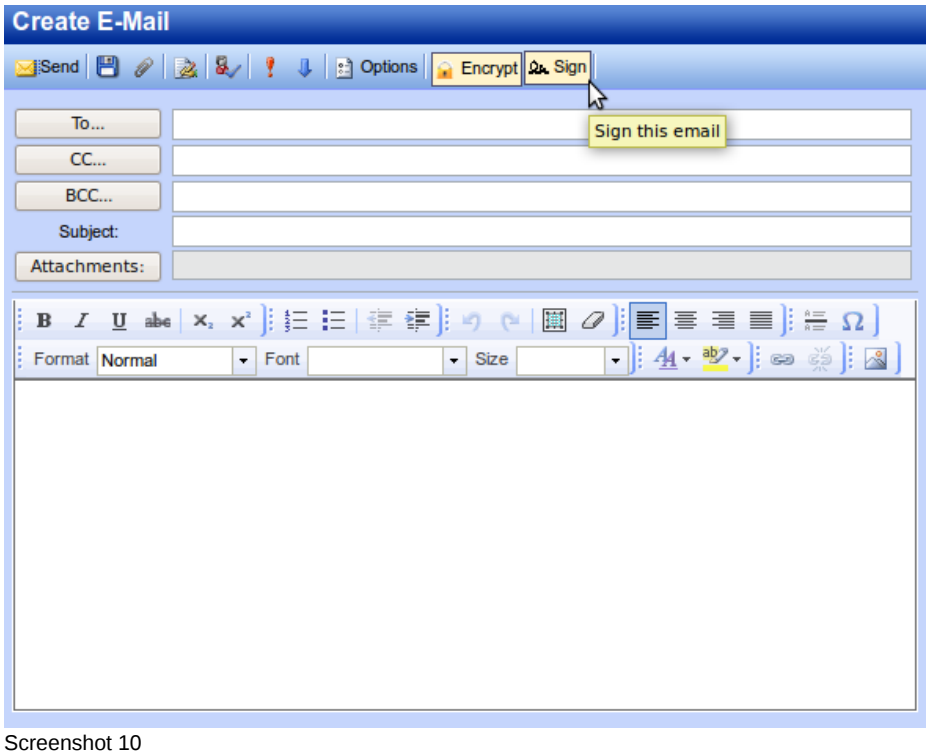
Note that currently there is no support for multiple recipient's when sending encrypted messages.



Screenshot 9

1.8.3 Encrypted and Signed Emails

To send a signed encrypted message both buttons “Encrypt” and “Sign” should be checked. The message's body and the attachments (if available) will be first signed as described in paragraph 1.7.1 and then encrypted as described in paragraph 1.7.2. See screenshot 10.



Screenshot 10

1.8.4 General sending notes

When sending encrypted and / or signed messages the attachments are combined with the message body in one encrypted and / or signed attachment. Note that the size of this attachments must be equal or less than the maximum size of attachments permitted in your webaccess installation.

Moreover note that when sending encrypted and / or signed messages the attachments and the message body are uploaded to the server after the sending button has been pressed. The user may notice more time is needed for the “Create email” window to close depending on the internet connection used.

If the user selects attachments and then clicks on any of the encrypt or sign buttons, the attachments must be selected again. Note that by first selecting attachments and then clicking encrypt, the attachments will be uploaded and store to your webaccess server unencrypted. Deciding if the message will be encrypted and / or signed before uploading any attachments is the suggested way of the plugin usage. Similarly if you choose to encrypt and / or sign, select attachments and then decided to not encrypt or sign the attachments must be selected again.

1.9 Known issues

1.9.1 Known issues with signed messages

Sending a signed e-mail from Zarafa webaccess to Zarafa webaccess works but the resulting e-mail in the sent-items folder will state that the signature could not be verified.

1.9.2 Known issues with encrypted messages

Encrypted e-mail messages from Zarafa webaccess to Zarafa webaccess will work but the senders public key will need to be installed manually.

1.9.3 Known issues with signed and encrypted messages

Sending a signed and encrypted e-mail from Zarafa webaccess to Zarafa webaccess works but the resulting e-mail in the sent-items folder will state that the signature could not be verified.

1.9.4 Known issues when replying to signed e-mail

When sending a reply to a signed e-mail the certificate of the original message is used to sign the reply.