This file describes the GPGOE functions and the integration in the Outlook Express mailer.

0.1 Requirements for GPGOE

First you need to have a working GnuPG installtion on the machine you plan to install GPGOE. If you don't have GPG in your machine, please visit http://www.gnupg.org and download the latest GPG version there. It comes with a graphical installer so there is no need to do this step manually.

You need at least Windows 2000/XP and at least Outlook Express 6.0 or higher. The plug-in will not work with earlier versions of Express.

0.1.1 Installation on Vista

Because of the nature of the plugin, it contains a lot of tricks for the Express integration, it cannot be guranteed, that it works on Vista in general or the Outlook Express version that comes with Vista. Feedback on the use with Vista is welcome but the adjustment, if possible at all will take a lot of time.

0.2 Installation of the Plug-in

It is always recommend to use the latest version of the plug-in. You can download it from http://wald.intevation.org/projects/gpgoe. Download the zip file with the binaries inside and unpack them in a folder. All files need to be in the same folder, so if you change the folder don't forget to move all files.

To activate the plug-in you need to start gpgoeinit.exe. You should now see a little (lock) icon in the taskbar which indicates that the plug-in is running. If you want to quit the program, double click on the (lock) icon and confirm the unload.

Now the plug-in is active.

0.3 Integration into Outlook Express

You have to enable the "Encrypt" and "Sign" items in the toolbar, in the "New Message" dialog to allow GPGOE to encrypt and/or sign the message.

There are no new icons for the plug-in and this means you can either use S/MIME or OpenPGP but never at the same time. If you want to use S/MIME again, just unload the plugin (quit gpgoeinit.exe).

It is very important to close Outlook Express before you unload the plug-in

0.4 How to use the plug-in

0.4.1 Encrypt a message

To encrypt a mail, you need to check the "Encrypt" toolbar button. If you click the "Send" button the plug-in will try to map each email address to a user-ID of an existing OpenPGP key. If no unresolved recipients were found, the mail is encrypted and stored in the outbox

folder. If one or more recipients couldn't be mapped to a key, the recipient dialog is shown to manually select the recipients.

0.4.2 Sign a message

To sign a message, you need to check the "Sign" toolbar button. If you click the "Send" button, GPG will figure out the default signing key and the plug-in openes a passphrase dialog to enter your passphrase for this key. If you entered it and the passphrase was correct, the plugin will sign the message and store it in the outbox.

0.4.3 Sign and Encrypt a message

To sign and encrypt a message, you have to check both toolbar buttons ("Sign" and "Encrypt"). The procedure is the same as in encrypt-only when one or more email addresses couldn't be mapped. Then the default key is used to sign the plaintext before it is encrypted with the selected recipients.

0.4.4 Decrypt and/or verify a message

If you received an OpenPGP message, you can just double-click the message to open it. The plug-in will figure out if it is encrypted or signed and will start the correct procedures. For decryption you need to enter your passphrase, otherwise the verify dialog is shown which contains information about the signature status. You can also use the "Next" and "Previous" toolbar buttons to jump to the next message or to go back to the previous. The plug-in will figure out the message status and will take the needed steps. If the message is neither signed nor encrypted, no action is performed.

0.4.5 Reply to an encrypted message

Newer versions of the plug-in provide a feature to decrypt the message before the text is used in the reply mail. As a result, the reply message will contain the plain text instead of the encrypted GPG armored message. This feature is automatically used whenever the user clicks on "Reply" or "Reply All" in the Outlook main window. But only in the case, the mail is actually encrypted. Optionally the plug-in will ask for a key passphrase.

0.5 Additional information and limitations of the GPGOE plug-in

- If you manually installed GPG and GPGoe, please make sure that you installed GPG at a standard place or create at least the gpgBinary registry entry. This is not needed if you use an automatic installer like GPG4WIN.
- Due to the fact the plug-in uses the clipboard for data transfer, the clipboard itself can be only of limited use to copy/paste messages into the mailer window or elsewhere. Newer versions of the plug-in save the original clipboard text before encryption/signing and the text is restored after the GPG operation ends.
- The current version of the plug-in will NOT encrypt any attachments which are attached to the message. You either need to encrypt them before or send them in cleartext. For the file encryption it is recommend to use GPGee or WinPT.

  The same needs to be done when an encrypted mail with encrypted attachments is in the inbox folder. You need GPGee or WinPT to decrypt the saved file.

- Even so the plug-in supports native line endings, which means you can properly exchange mails with Linux or Apple users, it is likely that there are problems with the charset. Newer versions of the plug-in try to handle UTF8 encoding correctly but even so it cannot be 100% assured that the receiver can handle the text in all cases.
- If you want to import keys or attach keys to a mail, you have to use an external key manager. WinPT is recommend in this case. It contains features to send public keys to mail recipients and also to export keys via the clipboard so you can easily paste the key into the text body of the message. The current version of the plug-in automatically uses WinPT for key import if the program is available and running.
- Currently signing can be only done with the default signing key. If you want to change the default signing key, you can use WinPT to select a different key and then GPGOE will use this one.
- GPGOE is NOT able to handle PGP/MIME (RFC3156) style messages. This means if you get such a message, the plug-in will not be able to automatically decrypt it. And due to the fact that the decrypted "attachment" will still contain a lot of control and coding information, you cannot simply decrypt it with WinPT/GPGee and use the output.