ISEC Lab #2

Cifrado de Correo electrónico con GnuPG en Outlook

Vicente Aguilera Díaz
vaguilera<arroba>isecauditors.com

1 Introducción

En los últimos meses, la cantidad de virus, gusanos y demás variantes de códigos maliciosos que se distribuyen en cantidades ingentes por Internet ha aumentado de forma alarmante.

Algunos de estos están teniendo consecuencias muy graves para las empresas por el uso que emplean éstos de la "Ingeniería Social" en una de sus más simples formas: la falsificación del origen del correo electrónico con el que llega el virus. Esto está causando verdaderos problemas entre empresas incluso llegando a la rotura de relaciones comerciales, pérdida de clientes, daño en su imagen y hasta litigios entre empresas que se acusan de envíos de virus con consecuencias destructivas o con esas intenciones, y todo esto cuando realmente la empresa no fue origen de tal correo electrónico.

En este ISECLab pretendemos demostrar como con un mínimo esfuerzo podemos eliminar este efecto y muy al contrario generar confianza en todos aquellos que son destinatarios de correos electrónicos emitidos desde nuestra empresa. El cómo es muy sencillo, y el coste la mejor parte, es decir, cero.

Existen gran cantidad de productos software comerciales para el cifrado de correo electrónico, de muy altas prestaciones y funcionalidades, pero no todas las empresas pueden permitirse el uso de estos paquetes en todos sus puestos de trabajo, y desde hace un par de años, hasta los organismos públicos han descubierto como se reducen los costes en la empresa con el uso de un tipo de software por muchos desconocido, el de código abierto, llamado Open Source.

Con la antaño impensable introducción de herramientas Open Source en un escritorio de oficina basado en Windows, veremos como, además de incrementar la seguridad en el uso diario de nuestro correo electrónico de forma sencilla y con un coste nulo, reduciremos los problemas planteados anteriormente. La solución: emplear GnuPG (GNU Privacy Guard), versión opensource con licencia GPL del popular PGP (Pretty Good Privacy), creado en sus inicios por Philip Zimmermann a principios de los 90 y los plugins o "añadidos" para los clientes de correo del grande de Richmond, ya sea en su versión Express, mediante Windows Privacy Tools o WinPT (también Open Source) o estándar, mediante GnuPG-plugin de G-DATA Software AG (igualmente Open Source). Veremos como instalar ambos plugins, como generar nuestras claves, gestionar estas y usar la firma y cifrado de correos con los clientes de correo más usados actualmente, que no por ellos los más seguros, pero eso es parte de otro ISECLab.

2 Funcionamiento de GnuPG

Este artículo tampoco tiene como objetivo explicar en detalle cual es el funcionamiento del cifrado de clave pública, pero sí hay un concepto de este tipo de cifrado que debe entenderse para comprender cuál es la razón y uso de las claves de que disponemos en GnuPG.

Todo aquel que desea utilizar este sistema de cifrado debe disponer de un par de claves: una privada y un pública. Como su propio nombre indica, la clave privada únicamente es conocida por él y la clave pública deberá ser distribuida (por correo electrónico, en disquete o por cualquier otro medio) a todo aquel que queramos que pueda enviarnos correo cifrado.

El funcionamiento básico del cifrado es este: para que A envíe un correo cifrado a B, A cifrará el correo con la clave pública de B; cuando B reciba el correo, únicamente mediante su clave privada podrá descifrarlo.

Además, podemos firmar los correos asegurando que el origen es quién dice ser: para que A firme un correo enviado a B, A firmará el correo con su clave privada; cuando B reciba el correo, únicamente con la clave pública de A podrá comprobar la firma.

Tanto cifrado como firma pueden usarse por separado o ambos en un mismo correo, con lo que aseguramos su contenido (cifrándolo) y aseguramos que quién lea nuestro correo sabrá que lo enviamos nosotros (firmándolo).

Veamos como poner esto en marcha...

3 Instalación de GnuPG

La instalación de GnuPG no sería necesaria si tampoco tenemos mucho interés en estar usando la última versión de éste, dado que los plugins que instalaremos tanto para Outlook Express como Outlook instalan sus propias versiones del software de cifrado. En el caso que queramos poder tener GnuPG en ambos clientes de correo, es mejor realizar esta instalación para permitir que ambos usen las mismas versiones y de esta forma, incrementar mucho más la facilidad de actualización del software GnuPG que estemos utilizando. No debemos olvidar que todo el software debe actualizarse y ningún software está libre de errores o mejoras y por tanto exento de ser actualizado periódicamente.

GnuPG es desarrollado por la comunidad y su página web es www.gnupg.org. Desde esta página web podemos descargar la última versión disponible (en el momento de escribir este artículo la 1.2.5), documentación, acceder a grupos de noticias sobre su desarrollo, etc. En nuestro caso iremos a la zona de "Download" accesible desde el menú izquierdo de la página o directamente desde el link del número de la última versión en el texto "Version 1.0.0 has been released on September 7th, 1999. The current stable version is 1.2.5.". Desde aquí, nos descargaremos la versión "GnuPG 1.2.5 compiled for Microsoft Windows.".

Para instalarlo, simplemente debemos descomprimirlo en el directorio que queramos y seguir una simple indicación. Por defecto, el directorio donde debe descomprimirse es "c:\\GnuPG", pero si eso de ir instalando software en el directorio raíz no nos gusta, podemos dejarlo, por ejemplo en "c:\\Archivos de Programa\\GnuPG". Si lo hemos descomprimido en el directorio por defecto, deberemos localizar el fichero "gnupg-w32.reg" y pulsar dos veces sobre él, se nos informará si queremos introducir la información en el registro (debemos aceptar) y se nos informará de que la actualización no ha tenido problemas (de nuevo aceptar). Si todo no fuesen buenas noticias hasta ahora es probable que sea producido por que no tengamos suficientes permisos en nuestra máquina para instalar software (o en este caso, modificar el registro de Windows). Si hemos optado por la opción de instalar GnuPG en una carpeta de nuestra elección, deberemos editar el archivo "gnupg-w32.reg" antes de ejecutarlo, y modificar las líneas:

```
"HomeDir"="C:\\GnuPG"
"gpgProgram"="C:\\GnuPG\\gpg.exe"
"MODir"="C:\\GnuPG\\Locale"
```

sustituyendo el directorio "C:\\GnuPG" en ambos casos, por aquel donde hayamos descomprimido el zip de GnuPG que nos bajamos de la web. Es imprescindible que entre directorio y directorio recordemos que la barra "\" debe escribirse dos veces (como aparece entre "C:" y "GnuPG"). Hecho esto, lo ejecutamos como en el caso anterior.

Sea cual sea el lugar escogido, ahora ya tenemos GnuPG instalado en nuestra máquina. Ahora sólo falta facilitar el acceso de nuestro cliente de correo Microsoft a éste, cosa que haremos con los plugins para cada uno de ellos.

4 Instalación y Configuración de WinPT

Para entender que es WinPT que mejor que leerlo de la propia ayuda de la página web del proyecto:

"Hasta Enero del 2003, WinPT era Windows Privacy Tray. Timo Schulz, el autor original del popular Windows Privacy Tray, accedió a ceder el acrónimo a un nuevo proyecto llamado WinPT por el nombre windows Privacy Tools, e integrar la hasta entonces utilidad Tray en este paquete.

Windows Privacy Tools (WinPT) es una colección de herramientas en múltiples lenguajes para el cifrado y firma digital de datos. WinPT está basado en GnuPG, que a su vez es compatible con software OpenPGP (como PGP) y de libre distribución para uso comercial y personal bajo licencia GPL.

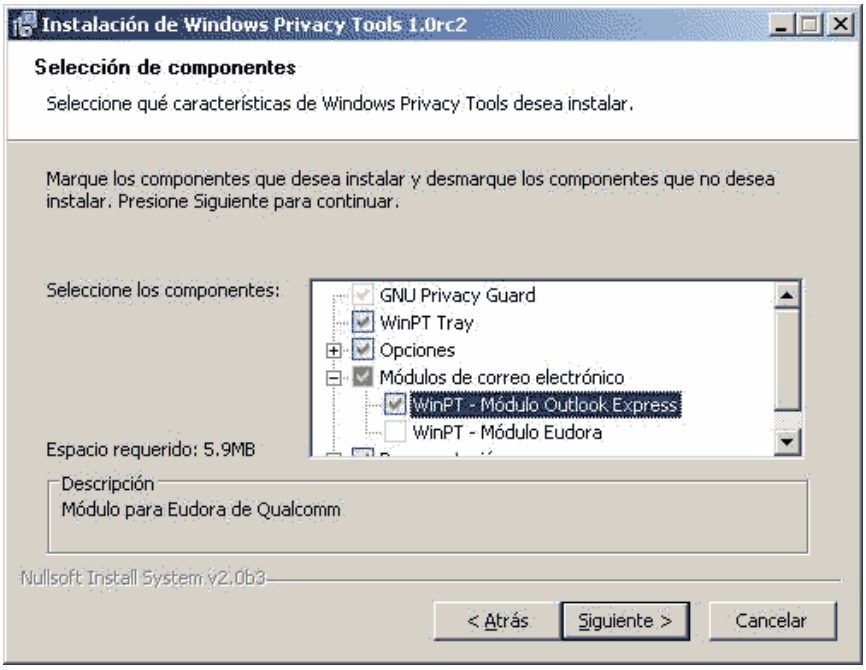
WinPT Tray es un "Frontend" que permite acceder al motor de cifrado Gnu Privacy Guard (GnuPG). WinPT Tray es una aplicación Windows® que [una vez instalada] incorpora un icono en nuestro System Tray [junto el reloj de la barra de tareas de Windows]. WinPT Tray no contiene rutinas de cifrado, por lo que puede exportarse libremente a cualquier país del mundo.

WinPT Tray puede usarse como un plug-in universal para cualquier programa de correo porque permite cortar y pegar desde cualquiera de estas aplicaciones, y cifrar datos que se encuentran en el portapapeles de Windows [aunque con los diferentes plugins que veremos evitaremos estos cortar/pegar muy molestos cuando realmente usemos el cifrado de forma habitual]. También incorpora un navegador de ficheros para el cifrado [o descifrado] de éstos en nuestro disco duro. WinPT también permite la gestión de las claves y el acceso a servidores de claves cuando estas son requeridas."

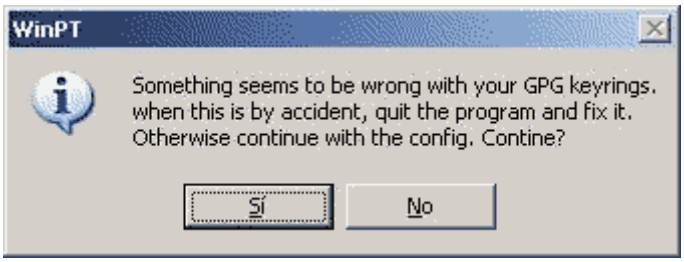
Aunque nos hemos referido a WinPT (Windows Privacy Tools) como un plugin para emplear GnuPG en Outlook Express, realmente es muy útil y recomendable instalarlo siempre que usemos GnuPG, ya sea Outlook o Outlook Express nuestro cliente de correo.

Una vez descargado de "http://winpt.sf.net/en/download.php" simplemente nos queda instalarlo:

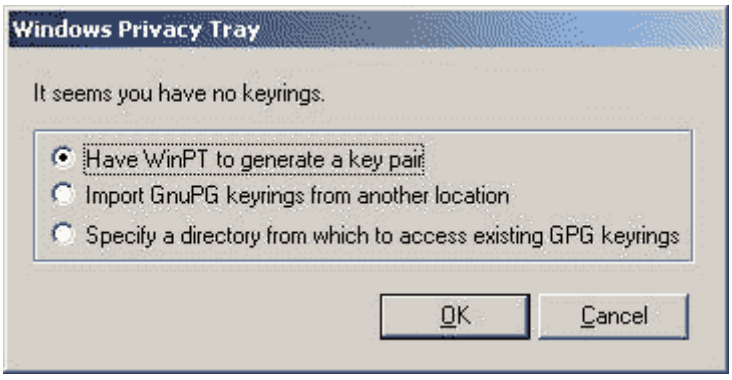
En el proceso de instalación deberemos elegir instalar el plugin para Outlook Express como se muestra en la imagen siguiente.



Justo antes de finalizar el proceso de instalación puede ser que WinPT nos dé un mensaje de error como el siguiente.



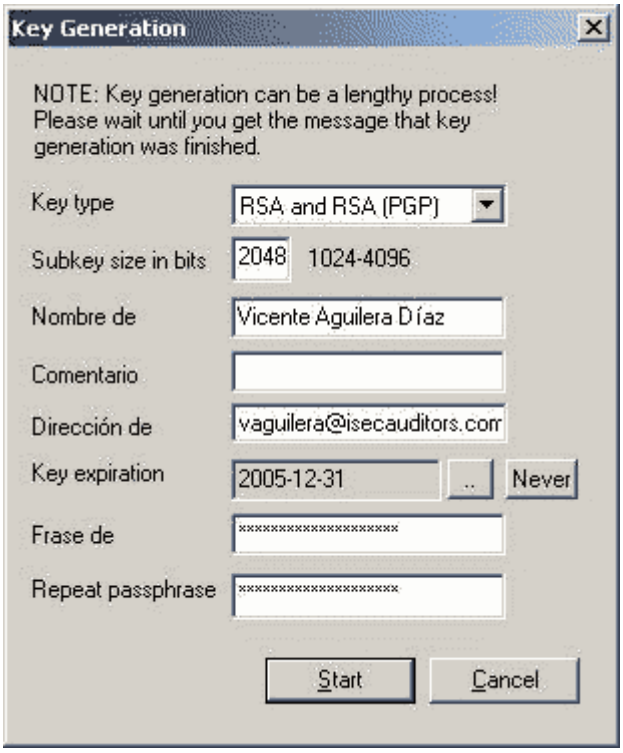
No hace falta preocuparse, simplemente elige "Sí" para avanzar (esto se debe a la no existencia de los anillos de claves que configuraremos a continuación) hasta la pantalla donde deberemos crearlas con WinPT, si queremos importarlas (si no es la primera vez que usamos GnuPG) o si tenemos ya archivos de claves de GPG en algún directorio. Esto se muestra en la pantalla siguiente:



Dado que vamos a suponer que jamás se ha usado GPG, elegiremos la primera opción y continuaremos el proceso.

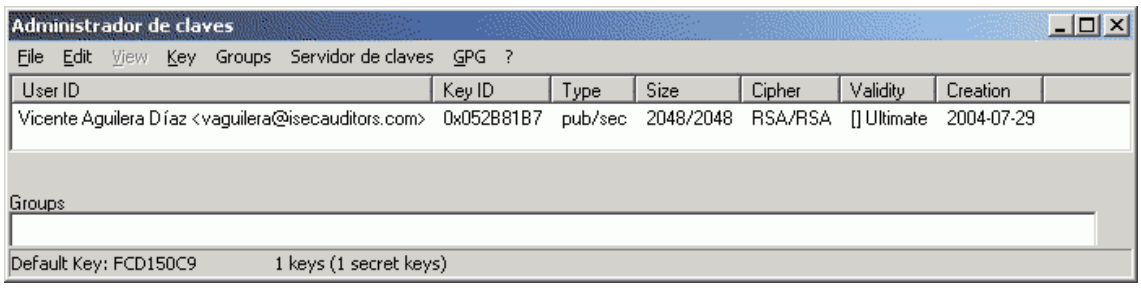
4.1 Generación de nuestra clave GPG

En la siguiente pantalla que nos aparecerá deberemos crear la pareja de claves pública y privada que usaremos para intercambiar correo cifrado/firmado.



Lo más importante de esta generación de la clave es que la frase de acceso o passphrase se nos pedirá cuando alguien cifre un mail con nuestra clave pública y nosotros queramos leer su contenido, por lo tanto debe ser una frase que recordemos con facilidad y con una longitud cuanto mayor mejor (sin pasarse, con 15-20 caracteres, números, mayúsculas y minúsculas será suficiente).

Una vez generada la clave se nos recomendará que hagamos una copia de seguridad de los anillos de claves. Es recomendable hacerlo y mantenerla en un sitio seguro (un CD o disquete). A continuación veremos como en nuestra herramienta de gestión de claves aparece nuestra flamante clave GPG.

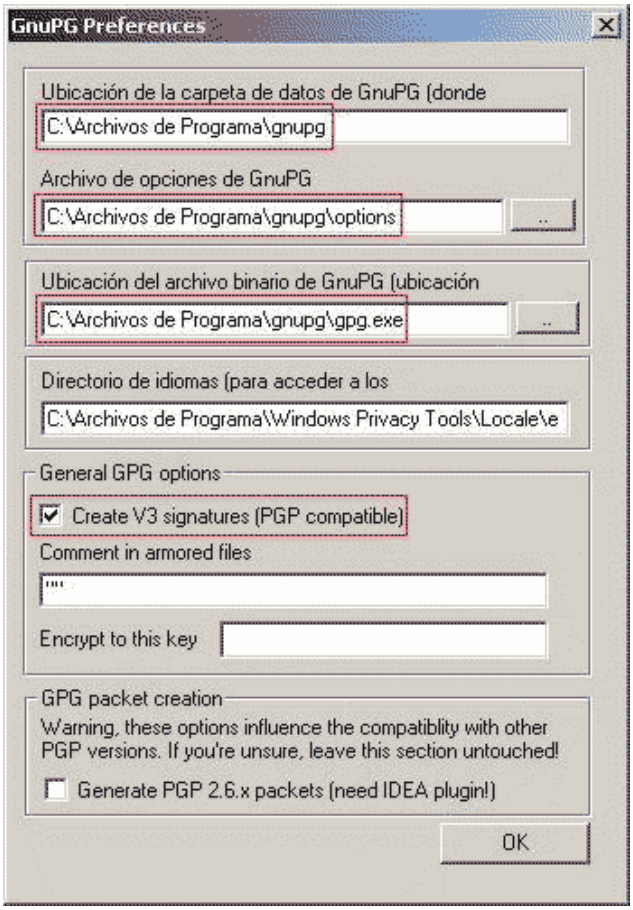


4.2 Finalizando la configuración de WinPT

Tras el proceso de instalación será necesario configurar WinPT de manera que emplee la versión de GnuPG que hemos instalado antes y no la que incorpora por sí mismo.

Para hacer esto desplegaremos el menú pulsando con el botón derecho sobre el nuevo icono que ha aparecido junto al reloj de la barra de tareas y elegiremos la opción Preferences->GPG (como se muestra en esta imagen):

En el diálogo que se abrirá podremos cambiar las rutas a los directorios donde tenemos instalado GnuPG, y que contendrá los anillos de claves que emplearemos según se muestra en la nueva imagen:

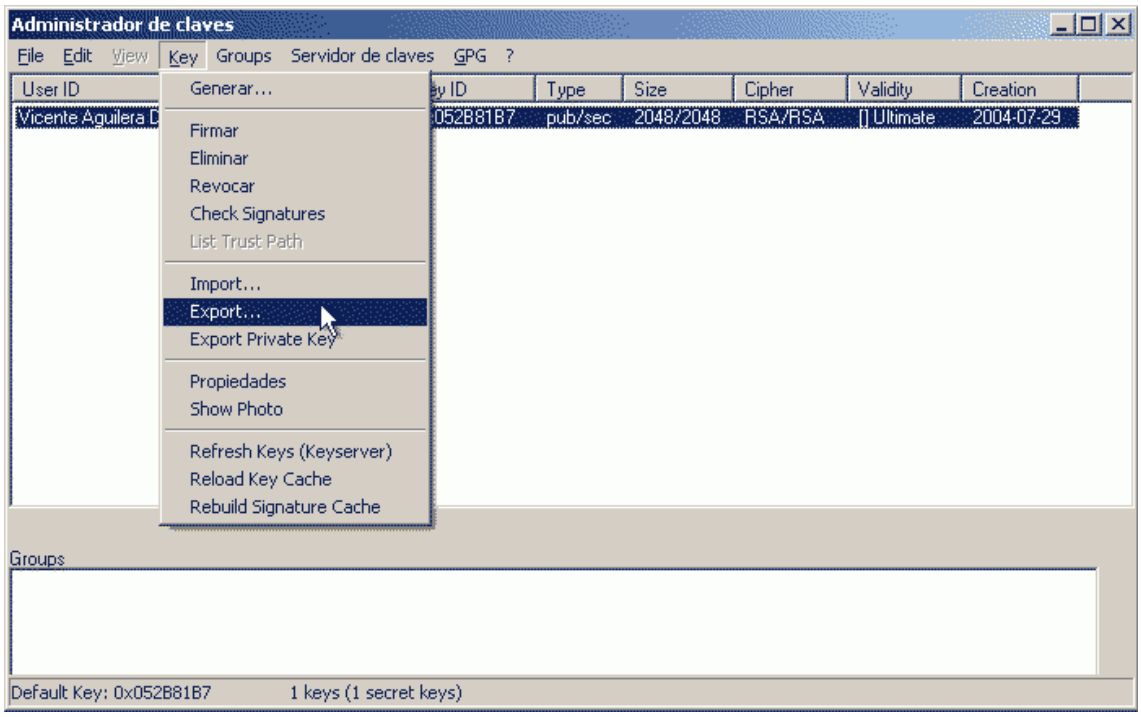


Una vez llegado este punto es mejor que reiniciemos el sistema para que automáticamente (si no desactivamos la selección durante la instalación de WinPT) se cargue el módulo de Outlook Express, cosa que veremos al reiniciar en que aparece un nuevo icono a parte del de WinPT (una arroba en forma de llave) es el de GPGOE DLL Loader (un candado).

5 Gestión de claves GPG mediante WinPT

Una vez instalado WinPT y creado nuestro par de claves pública/privada ahora es necesario que distribuyamos la pública a todos aquellos que quieran poder comprobar la firma de nuestros correos electrónicos.

Para poder exportar la clave, deberemos abrir el "Gestor de claves" de WinPT, y mediante la opción de menú Export (ojo, no elegir la exportación de la clave privada ya que esa clave debemos tenerla sólo nosotros). Véase la siguiente captura:



El resultado será un archivo con extensión ".asc" que contiene nuestra clave pública con un contenido como este:

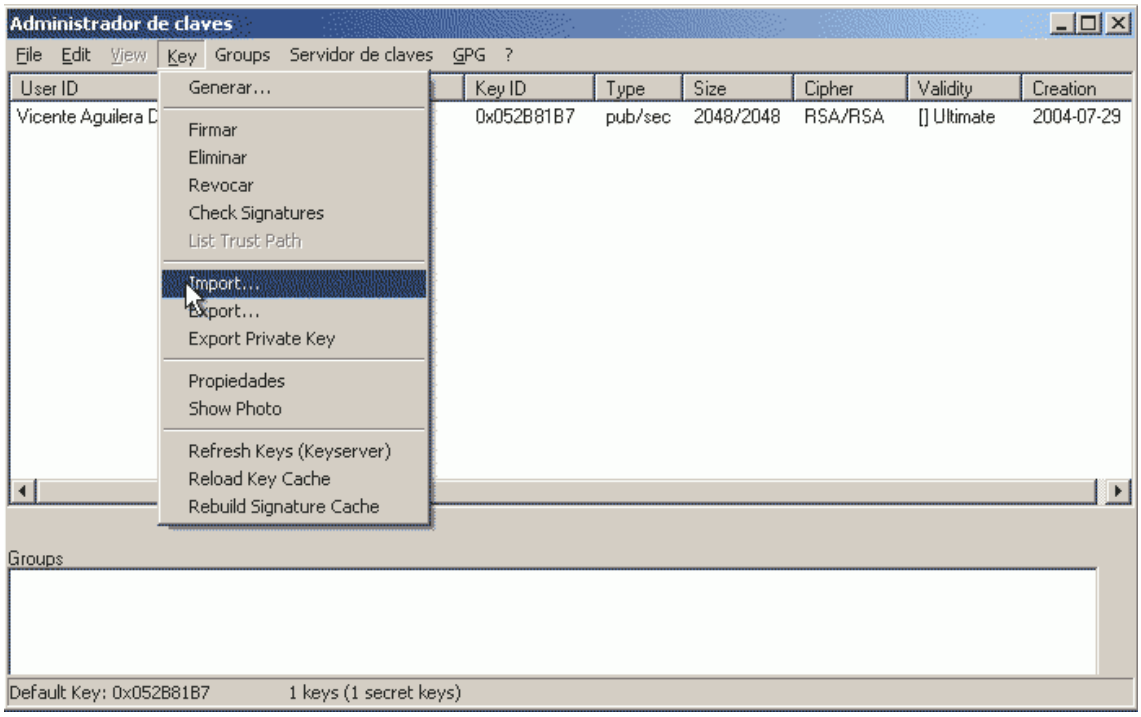
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (MingW32)

mQELBEEJCa0BCADC9Wtke/rWO0UWYvLmmf2qi07jFgMXmRhEP3fvgEsrVIOFQvna
C1MHe2AFYW9Gf5mHyGyNTT0y2hiOlMFHVubaxv5/xwrFnS+DPdNuOK3L/MxUJPdx
HFkBLwcC1lOJdT117VSCCEfLcfYBVuMjgx0QVyVlEE2+nMzjSY7Y4gq+S9wHqXAE
pshVfK4kfOFqlI+66Bsp+XjheETXXFBWWgq3IZNZt5HcNzkiLHweGLIzFKP5W3h3
u5Ky1I4aKr9n41BuRqPqZUQz61C0OKs1yxa54RCkMtiBfnkX8NXi6oPrvjnFsr9L
JeCJBlcRbS3MWFE51kAYI7CeShiPEzVHbS67AAYptDNWaWNlbnRlIEFndWlsZXJh
IETCoWF6IDx2YWd1aWxlcmFAaXNlY2F1ZGl0b3JzLmNvbT6JATUEEwECAB8FAkEJ
Ca0FCQKtjAAECwcDAgMVAgMDFgIBAh4BAheAAAoJEAN0CfkFK4G3qF0IAItYDcAA
UyDkgbgvAhPpx+JxO3HDZldGZfp6wJlDrCBqugvWaNjPwt3aGyTyxpq+I/MZ7beB
VqchQCRw/mPj9d89tpVG7+Kew5lvsIMhy49TZDWLteVVo+aGFQvJYMAXuEe52SdN
X1lyrujpVMbiO//KLuxufUEfV/VPxuKmlIPhM1UKExzXM7TRRBzkseJtYOS08un3
lpYa9OBjb/3fGdJXHMecP+IIWSjcRVKvKInlqWBGRrooDdaRVl7KmmyHkvMO9MWc
```

```
xML62W4EsD95GTrDedmR5vfHoBwRS/HBga8XrF8tcM0kGrjRw0xxpnZis8INis/2
yv0tOAMM4uFwsFW5AQsEQQkJswEIANUDf1JAq1FAfyCb0IYiVA8xI6NjXvGHoNa3
4DakwejEWFau7URUt9kVHpKxSa0M5+qHBGIhgbnNyX6gq1eiwRj5n5FO3+DQmtRW
1bkmcPq8Ozitbl4Yl7GzJCPfJHg2Vel4qhdwVMHvbImr0F0wBcPqwY+Gfw1rsplb
P5v/qAhsXbt7wDKREL0XRNEx3as3GK7UhA6+5w714Ruug0YNLLfDp6+D6A3Pn37Z
uXA69oaHxcoRvCfP0CVN+OH0WVSD1EvNXmlGbdTN06spXEkZEYfhBAaq7XNf7JwQ
YiXrhOpSRNaRkpLi2NX0FSU0KXumvd9E4TPiX3uPLW6aobyQVYcABimJASIEGAEC
AAwFAkEJCbMFCQKtjAAACgkQA3QJ+QUrgbcqSQf/YWHYcNwkARnNynMW4iL5fHpq
4YcNUbt0sh7ny640aUkb0FG78H7f5bkeIjvGH3NzRaojrVAnsdL1nhIJX+NYI8Q7
yrKtFdNaWx3o7jAp2BSk4QkzEZjJddAyWgFnquugKYnJQ8DdOAx6/wyvwUOmRZRV
pH+NvE134BEfY5Hc/1LM23p76lPMiUp6ZNx/S/P4at4mC5HgECR4xg2n1P0GoCYu
x5Gu7FWofqqlP3NqHD2qqU43uZE3U34KjbhWYY2DK9xLc7FUwtOKela+Hp7446Yx
OmJrV2cJzUG5rn9ebWaDgpAl0kJKMgBKjmaDmOu1rb/p+lw6f2bpeTs/2Zy0nA==
=du5d
-----END PGP PUBLIC KEY BLOCK-----
```

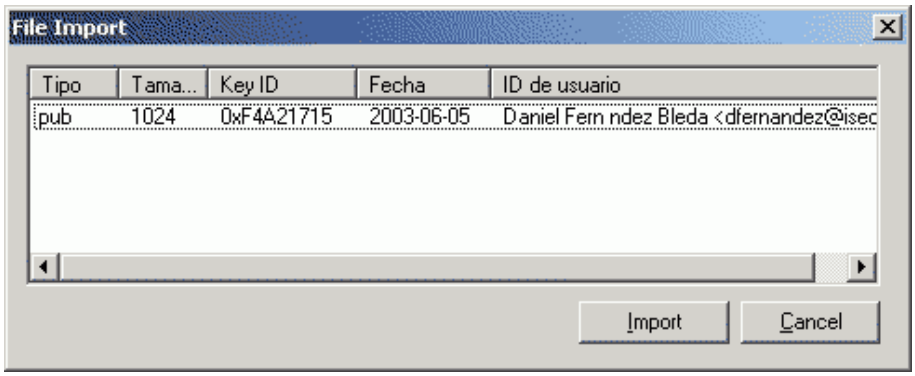
Desde este punto deberemos enviar este archivo .asc a todos los destinatarios de nuestros correos firmados. Para incorporar nuevas claves públicas de aquellos con los que intercambiemos correos el proceso será similar. Desde el "Gestor de claves" de WinPT seleccionaremos un Key->Import y seleccionaremos aquellos archivos ".asc" que nos envíen.

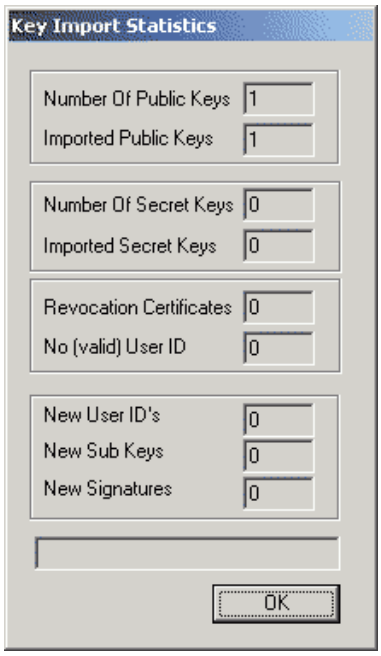
Supongamos que un compañero me ha enviado su clave, vamos a importarla y los pasos:

1. Elegimos la opción Import, para elegir un fichero.

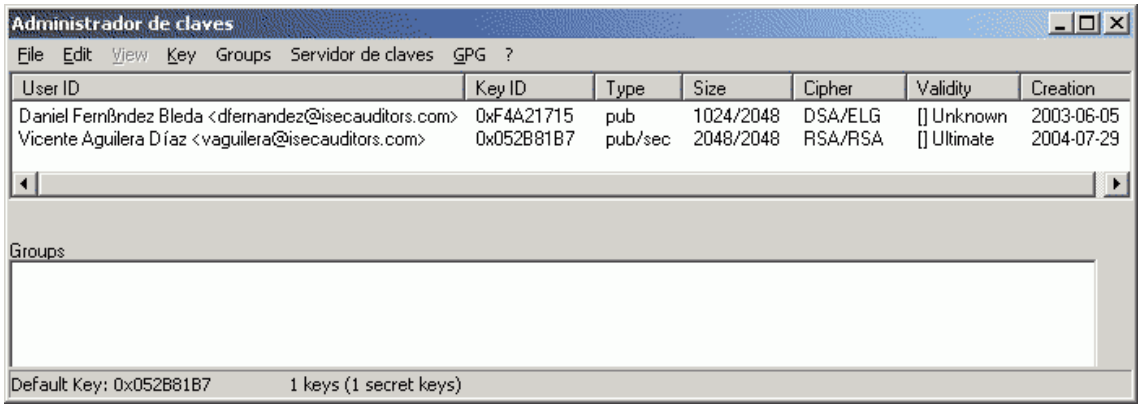


2. Una vez escogido el fichero se nos informa de las características de la/las claves contenidas en el fichero .asc escogido.





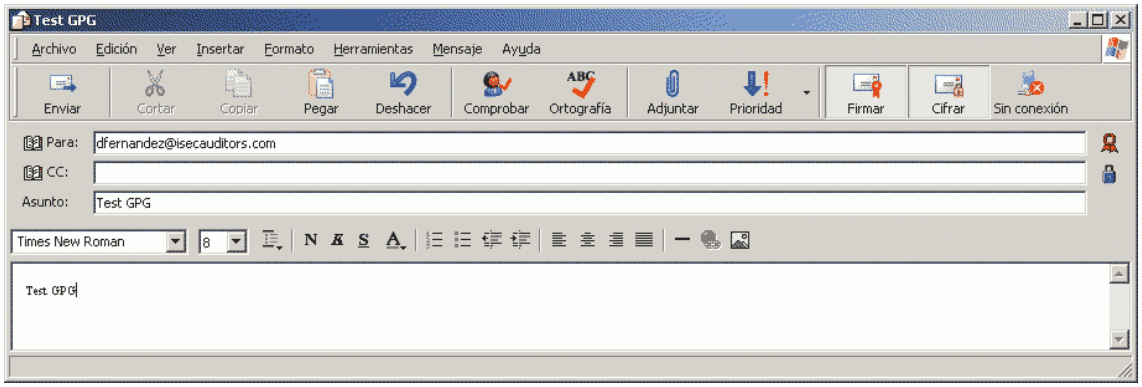
3. Finalmente veremos como aparecerá la nueva clave importada. Si no apareciese de forma automática, simplemente debemos escoger la opción Key->Reload Key Cache.



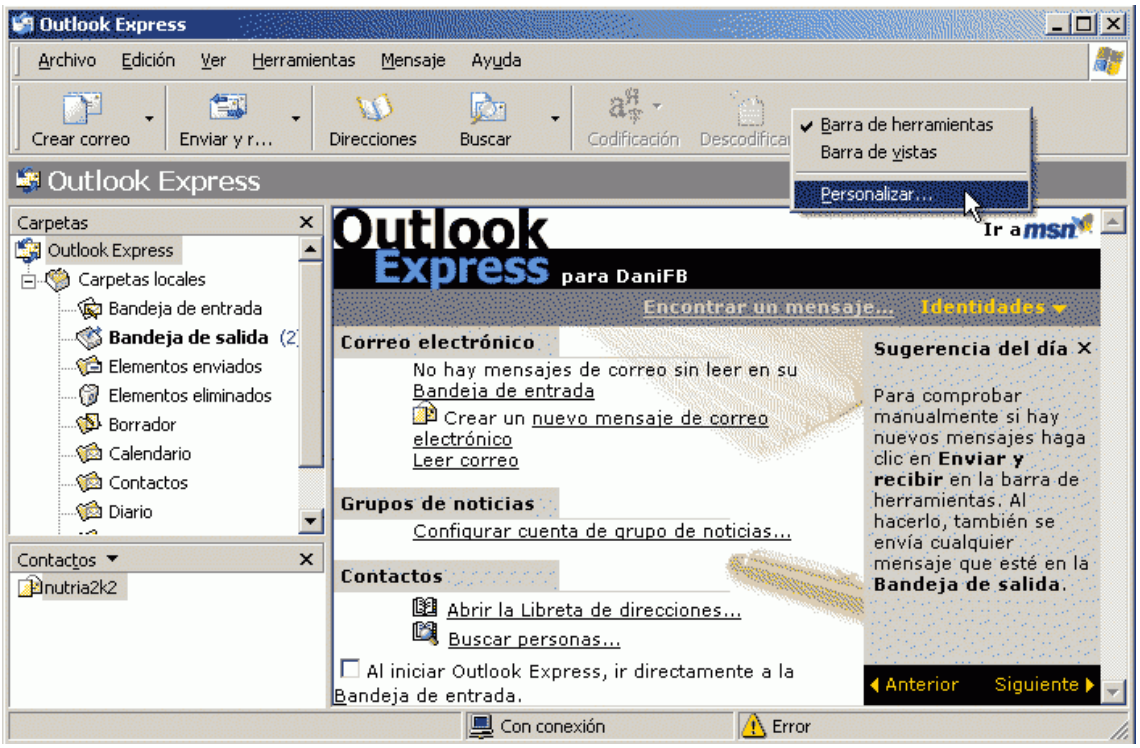
Como vemos en la imagen anterior ahora disponemos de dos claves, una únicamente de Tipo (Type) pública (pub) con la que podremos cifrar mails para aquellos destinatarios de los que tengamos sus claves públicas. A parte dispondremos de nuestra clave publica/privada (pub/sec) para la firma y cifrado de correos.

6 Enviando correos cifrados/firmados con Outlook Express

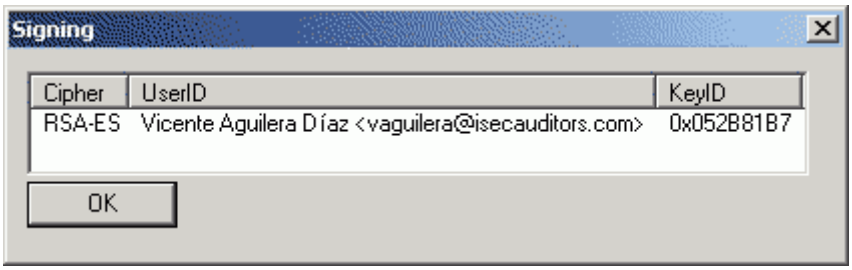
Para poder firmar o cifrar nuestros correos en Outlook Express deberemos asegurarnos que tenemos los botones que deben aparecer al enviar un nuevo correo según aparece en la siguiente imagen:



Si no fuera nuestro caso, deberemos añadir dichos botones desde la opción personalizar según la siguiente captura:



Suponiendo que tenemos dichos botones, sólo nos queda "Enviar y recibir" y veremos como nos informa que el mensaje se va a firmar con nuestra clave.



Como resultado, veremos que el contenido del mensaje enviado ya es ilegible dado que está cifrado.

De esta forma nos hemos asegurado que quien reciba el mensaje sabrá que lo hemos enviado nosotros (comprobando la firma del mensaje) y si alguien lo captura no podrá leer su contenido (a no ser que tuviese la clave privada del destinatario y su "passphrase").

7 Instalación y configuración de GnuPG-Plugin para Outlook

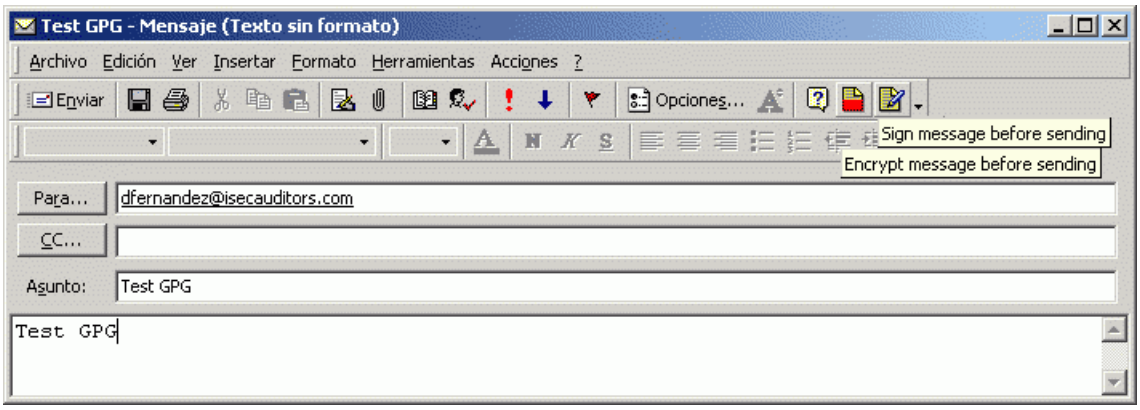
La instalación de GnuPG-Plugin es incluso más sencilla que la de WinPT, con lo que lo único que debemos decidir es si simplemente queremos instalar GnuPG-Plugin o también éste junto con el gestor de claves y la versión de GnuPG que incorpora. Realmente el gestor de claves de este plugin es muy intuitivo y cómodo (a pesar de esto, la importación de claves me ha dado ciertos problemas).

Al igual que para el caso de Outlook Express, vamos a suponer que utilizaremos el gestor de claves y ficheros de WinPT y el GPG descargado de gnupg.org (eligiendo la opción "G DATA GnuPG-Plugin for Outlook" en el proceso de instalación).

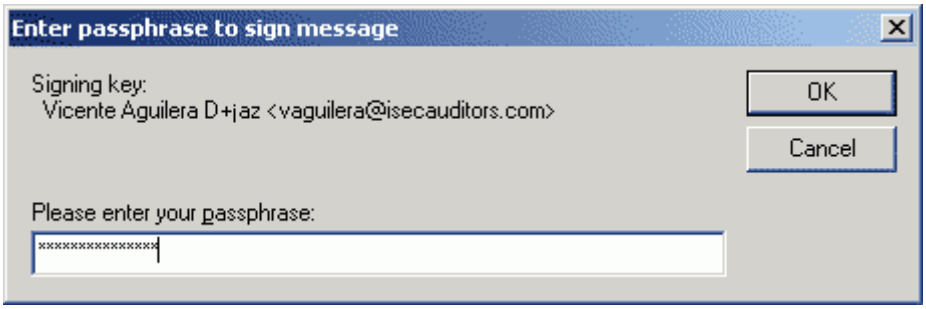
Cuando hayamos finalizado la instalación será necesario acceder a la configuración del plugin de Outlook a través de Herramientas->Opciones. Veremos que aparece una pestaña nueva con el nombre de "Encryption" donde pulsando en el botón "Advanced" podremos actualizar los directorios donde localizar gpg.exe. En ambos casos las casillas deben contener el directorio donde hayamos instalado GPG, es decir, "C:\Archivos de Programa\GnuPG\gpg.exe".

8 Enviando correos cifrados/firmados con Outlook

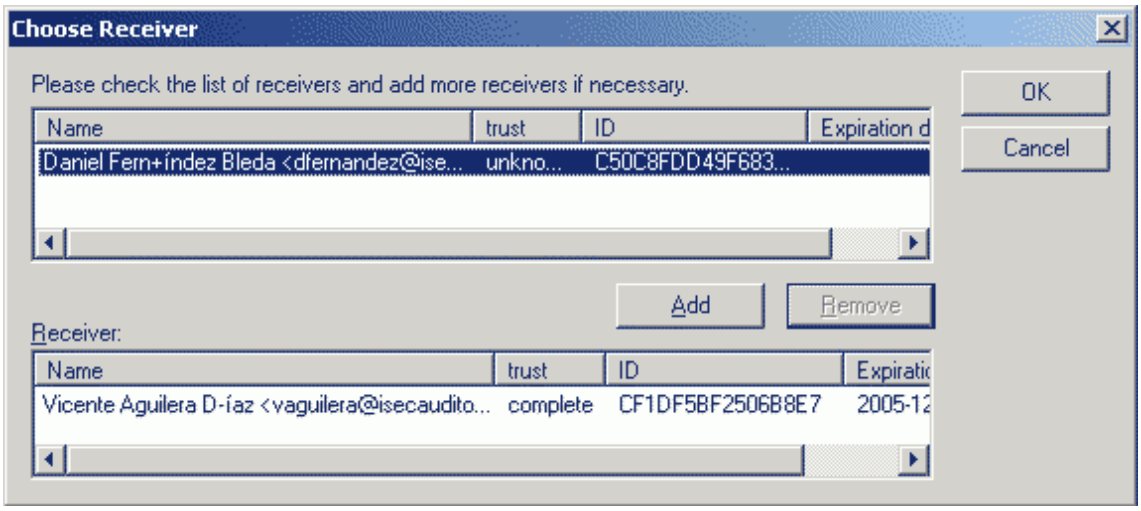
El envío de correo cifrados y firmados con Outlook será igualmente sencillo. Dispondremos de dos nuevos botones como se muestra en la siguiente imagen, cada uno para una de las dos funciones de seguridad:



El siguiente paso será introducir nuestra passphrase para la firma del correo.



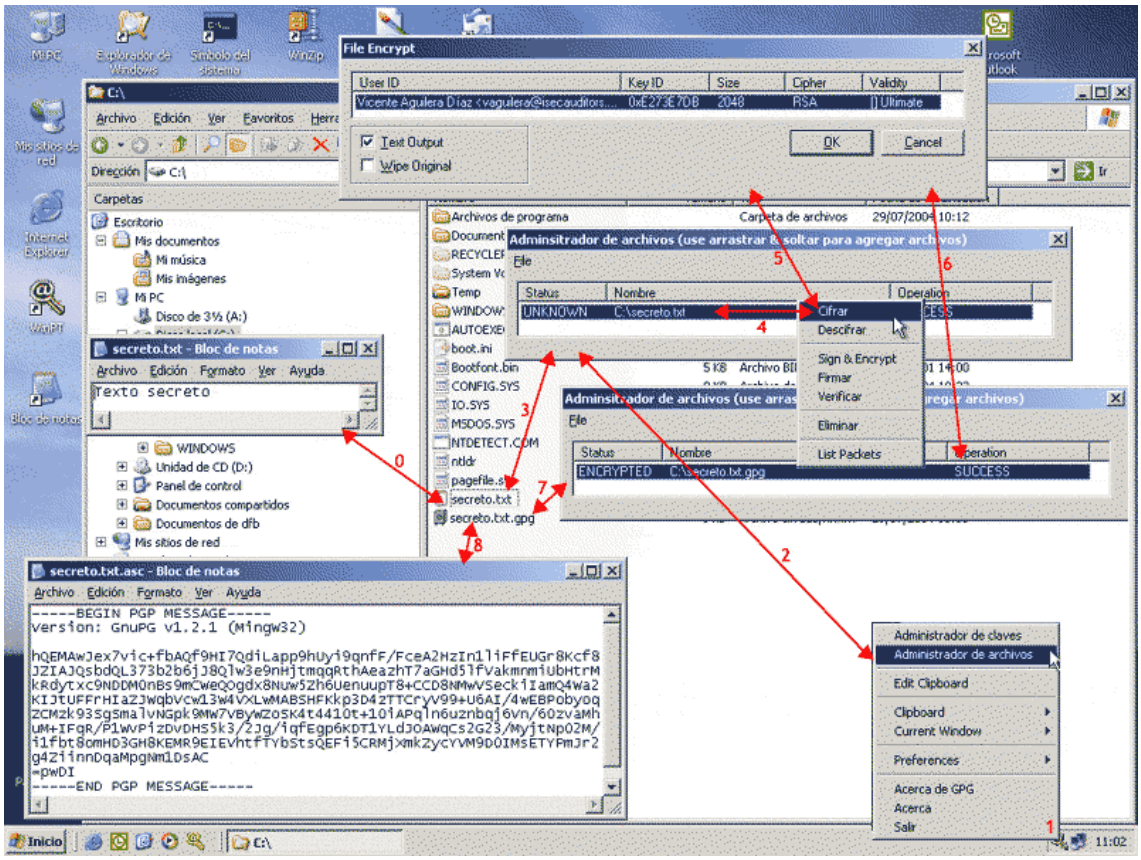
Cuando enviemos este correo se nos pedirá igualmente los destinatarios para los que queremos cifrar el mensaje (aquellos de los que tenemos clave pública).



Añadiendo los destinatarios adecuados habremos enviado nuestro correo seguro.

9 Cifrando Ficheros mediante GnuPG

A parte de poder enviar correos electrónicos cifrados y firmados, puede interesarnos en algunos casos, enviar correos cuyo contenido no esté cifrado pero cuyos archivos adjuntos si estén protegidos. Para poder hacer esto, WinPT incorpora un gestor de cifrado/descifrado de ficheros. Su uso es muy sencillo y creo que con la captura siguiente se entiende claramente cual es su uso, que merece la pena conocer y perder un poco de tiempo acostumbrándose a su uso.



10 Consejos de Utilidad

1. Cada uno de los programas comentados incorporan archivos "readme.txt" que define los pasos para su instalación, y puede ser muy recomendable echarles un vistazo si nos perdemos en alguno de los pasos.

2. En este documento hemos cubierto la parte de cifrado y envío de mails, dejamos a la curiosidad (realmente requiere muy poca) del lector el conocer el método inverso para descifrar los correos que nos lleguen cifrados/firmados.

3. Es muy recomendable revisar cada cierto tiempo (dos o tres meses máximo) la aparición de nuevas versiones de las aplicaciones instaladas.

Y las más importantes:

4. Si queremos poder leer los correos que enviamos nosotros mismos en nuestra bandeja de salida es imprescindible que nos añadamos en la lista de destinatarios para los que ciframos los mensajes, ya que si no únicamente los destinatarios a los que hubiésemos enviado nuestros mails serán capaces de leernos, siendo no visibles para nosotros.

5. Mantén una copia de seguridad de los ficheros de claves (secring.gpg y pubring.gpg) que se encuentran en el directorio donde hayamos instalado GnuPG o hayamos configurado nuestro plugin.

6. Si no queremos que el método (cuando ciframos) pierda su seguridad, no almacenes en la bandeja de entrada los mensajes descifrados, ya que si alguien tiene acceso a tu ordenador, de nada habrá servido el cifrado, es decir, la mejor manera de mantener la seguridad será descifrarlo cada vez que queramos leerlo. El mayor inconveniente será que las búsquedas en los contenidos de los mails en busca de algún mail "perdido" no funcionará, dado que el cliente de correo no verá un contenido legible en estos.

11 Enlaces de Interés

- G DATA GnuPG-Plugin: http://www3.gdata.de/gpg/index.html
- Windows Privacy Tools (WinPT): http://winpt.sourceforge.net/en/
- GnuPG: www.gnupg.org