Seguridade no correo electrónico empregando PGP

- Seguridade no correo electrónico empregando PGP
- Instalación de PGP
  - Instalación de PGP 7.0.3 para Windows
  - Crear un par de chaves PGP
  - Xerar certificado de revocación de chave
  - Enviar unha chave a un servidor PGP
  - Consultar e importar chaves dun servidor PGP
  - Enviar un certificado a un servidor de chaves
  - Firmar ou cifrar mensaxes de correo a enviar
- Uso de GNUPG (GPG)
  - Listar anel de chaves dun usuario
  - Xerar un par de chaves PGP
  - Importar unha chave ó anel de chaves do usuario
  - Enviar unha chave pública a un servidor
  - Exportar unha chave
  - Xerar un certificado de renovación de chave
  - Enviar certificado de revoación a un servidor de chaves
  - Frmar un documento
  - Verificar firma dun documento

Seguridade no correo electrónico empregando PGP

Este documento pretende indicar cómo utilizar PGP (Pretty Good Privacy), especialmente como ferramenta para verifica-la autenticidade e integridade de correos (firmado dos correos) e como ferramenta para garantizar a confidencialidade dos correos (cifrado dos correos). PGP é unha ferramenta moi útil para estos fins, aínda que non a única.

Na páxina web de Rediris pódese encontrar máis información sobre PGP, software para distintas plataformas e información sobre o servidor de claves públicas PGP de Rediris. Para visitar esta páxina pulse aquí.

O paquete PGP e o seu equivalente con licencia GNU, GPG, teñen a ventaxa de que existen diversas versións gratuitas deste software para distintas plataformas (Windows, Unix, Mac, etc.), de non ser desenvolvido de forma principal por ningunha compañia de software ou organización gubernamental e de estar moi extendido o seu uso.

PGP (Pretty Good Privacy) é un programa desenvolvido por Philip Zimmermann. Reelaborado para o seu uso internacional por Ståle Schumacher e que se basa no uso de criptografía de clave pública.

En este tipo de criptografía un usuario ten dúas claves, unha pública, da que outros usuarios poden dispor e que poden usar para verificar que unha mensaxe foi enviada por un usuario ou para cifrar unha mensaxe con destino a un determinado usuario, e unha privada, da que só pode dispor o propietario de ambas claves e que utiliza para firmar documentos ou para descifrar documentos firmados coa súa clave pública.

O uso de correos firmados ou cifrados (especialmente esto último) ten senso só cando se están a enviar a un determinado destinatario. É recomendable non usar esta opción ó enviar correos a unha lista de distribución, xa que ocuparán máis espacio, e poden ser rexeitados por este motivo polo servidor de listas de correo. Polo xeral non teñen senso en este contexto (en ocasións, e segundo sexa a finalidade da lista pode estar xustificado o enviar un correo firmado á mesma).

Este documento describe o uso de PGP 7 para Windows (este software inclúe un plugin moi útil para usar PGP dende Outlook) e GPG (para usar en plataformas Unix).

Instalación de PGP

Instalación de PGP 7.0.3 para Windows

No servidor ftp ftp.uvigo.es, en ftp://ftp.uvigo.es/pub/software/util/pgp pódese atopar unha versión de PGP (a 7.0.3) para Windows. Non use esta versión en Windows XP, xa que pode orixinar problemas (especialmente o programa PGPNet que inclúe). En breve sairá ó mercado a versión 8 de PGP, de todas formas esta versión non se inclúe no servidor FTP ftp.uvigo.es debido a que a licencia non será gratuira senón shareware.

O software e a documentación orixinal de PGP pódense atopar en esta páxina.

Inclúense dous parches de seguridade que compre aplicar a este software.

Para ter PGP en Windows compre instalar en primeiro lugar o paquete de PGP , PGPFW703.zip e despois os dous parches que se inclúen, PGPfreeware703Hotfix1.zip e PGP_Hotfix0904_Win32.zip.

- **PGPFW703.zip**

    - Se descomprime e instala o executable que inclúe, PGPfreeware7.0.3.exe
    - Cando pregunta "Do yoy already have keyrings?" indicar que non ("No, I am a new user"), salvo que se esté a instalar sobre unha versión xa existente de PGP
    - Instalar o seguinte:
        - PGP Key Management
        - PGP Plugin for Microsoft Outlook
        - PGP Plugin for Microsoft Outlook Express
        - PGP Documentation
    - Reiniciar o sistema (pregunta "Yes, I want to restart my computer now")
- **PGPFreeware703Hotfox1.zip**
  Este é o primeiro dos dous parches de seguridade que compre aplicar a esta versión de PGP
    - Extraer a un directorio
    - Executar PGPHotfix.exe
    - Reiniciar
- **PGP_Hotfix0904_Win32.zip**
  Segundo dos parches de seguridade para esta versión de PGP para Windows
    - Extraer a un directorio
    - Executar PGPHotfix.exe
    - Reiniciar

Despois de instalar PGP e os parches correspondientes, en Outlook aparecerá un novo botón, "Launch PGP Keys", dende o que se accede ó programa de administración de chaves PGP.

En este programa pódense crear ou borrar chaves no anel local, configurar un servidor de chaves PGP ó que facer consultas (pódese usar o proporcionado por RedIris), ou indicar se se desexa usar PGP nos correos enviados ou recibidos (firmar ou cifrar correos no envío, descifrar ou verificar firmas de forma automática na recepción).

Crear un par de chaves PGP

Cando se xenera unha nova chave aparecen as opcións:

"Name and Email Assignment"

"Full Name:" : Indicar o nome completo (nome e apelidos) do usuario

"Email" : Dirección de correo coa que se vai usar esta chave

"Passphrase"
Aquí compre indicar a palabra de paso da chave privada (unha palabra ou frase que é necesario indicar cada vez que se use a chave privada do usuario). Esta palabra de paso debe ser apuntada con coidado e non se pode perder, xa que é necesaria para firmar, cifrar ou descifrar correos. Isto é importante sobre todo se a chave pública vai ser enviada a un servidor público de chaves PGP.

Unha vez rematada a creación da chave compre manter unha copia de seguridade da mesma (por exemplo en disquete). Para facer isto existe unha opción para exportar o par de chaves xerado, pulsando o botó dereito do rato sobre a chave en cuestión no programa PGPKeys e elexindo, do menú que aparece, a opción "Export". Compre incluir a chave privada cando se exporte ("Include private key").

Xerar certificado de revocación de chave

É recomendable xerar un certificado de revocación para a chave PGP, especialmente se vai ser enviada a un servidor público de chaves.
Este certificado de revocación permitirá no seu momento eliminar unha chave do servidor e chaves PGP.
Esto pódese facer despois de xerada a chave e antes de usala por primeira vez, como precaución.

Se non se ten un sempre pode ser xerado antes de dar de baixa a chave, pero terá que lembrar a palabra de paso da chave privada. Se esqueceu a palabra de paso e non ten un certificado de revocación será imposible borrar a chave dos servidores públicos en que esté disponible (os servidor non ten forma de verificar a identidade do usuario).

Se dispón de un certificado de revocación de pode exportalo en formato ASCII en introducilo no formulario que hai na páxina web de Rediris para que sexa publicado no servidor pgp.rediris.es

Os pasos para xerar un certificado de revocación en PGP 7 para Windows son os seguintes:

1. Dende PGPKeys exportar e gardar (incluindo a chave privada) a chave da que se vai xerar o certificado de revocación.
   Pulsar o botón dereito sobre la chave e usar a opción "Export".
   Compre incluir a clave privada cando se exporte o par de chaves.
   Por exemplo exportar o par de chaves ó arquivo copia-chave.asc
2. Revocar a chave dende PGPKeys Pulsar co botón dereito do rato sobre a chave e elexir a opción "Revoke". Pedirá confirmación e a palabra de paso da chave privada. A chave aparecerá como revocada.
3. Exportar en ASCII esta chave revocada.
   Esto é o que quedará como certificado de revocación
   Exportar por exemplo ó arquivo revocacion.asc.
4. Borrar a chave revocada de PGPKeys Pulsar co botón dereito sobre a chave e elexir "Delete"

5. Importar a chave exportada no paso 1 "Keys" -> "Import"
6. Para que a chave importada sexa de confianza e poda ser usada para firmar e cifrar
   Pulsar o botón dereito do rato sobre a chave importada
   Elexir "Key properties" e marcar "Implicit trust" (con esta opción indícase que é de confianza).

Debe gardar unha copia do certificado de revocación en lugar seguro. Con este certificado poderá dar de baixa a chave PGP de servidores de chaves ainda que esqueza a palabra de paso da mesma.

Enviar unha chave a un servidor PGP

Para distribuir unha chave PGP, pode enviala directamente á persoa coa que un quere establecer a comunicación, preferentemente por un canle seguro (nun disquete, por exemplo), se só vai a usar a chave para comunicarse cunhas poucas persoas.

Polo xeral é preferible publicar a chave nun servidor de chaves públicas PGP. Unha vez publicada nun servidor de chaves, este distribuirá as chaves ós servidores de este tipo que coñeza.
As chaves poden ser enviadas a un servidor de chaves por distintos métodos (correo, formulario no web, dende os propios programas de xestión de chaves PGP -gpg, pgp-, etc.).

A presencia dunha chave PGP nun servidor público non garantiza que corresponda ó usuario ó que pretende estar asociada. Pode consultar co usuario se a chave en cuestión é súa, preguntando por algún dato identificativo da chave pública (o identificador da firma ou o hash).

Rediris pon a disposición dos usuarios da comunidade académica o seu servidor de chaves, pgp.rediris.es, ó que se pode acceder dende a páxina web http://www.rediris.es/keyserver. Hai máis información ó respecto nas páxinas de Rediris de documentación de PGP e sobre o servidor de chaves públicas de Rediris

Unha vez enviada unha chave a un servidor a única forma de borrar esta clave do servidor é tendo un certificado de revocación. É recomendable xerar este certificado de revocación antes de enviar a chave ó servidor.

Consultar e importar chaves dun servidor PGP

Para a consulta de chaves PGP públicas pode empregar o servidor de Rediris, pgp.rediris.es.

As chaves PGP propáganse a través dos servidores de chaves, de forma que cando unha chave pública é engadida, modificada ou borrada en un servidor, estos cambios son propagados ós outros servidores PGP dos que teña coñecemento.

Estas chaves podeas consultar ou descargar dende a páxina web do servidor de chaves de Rediris ou pode configurar PGP (ou gpg) no seu propio ordenador para que efectúe esta operación de forma automática.

Esto configurase en PGP 7 para Windows no programa PGPKeys, coa opción: "Edit" -> "Options" -> "Servers" -> "New"

Indicando como características do servidor PGP:

- PGP KeyServer HTTP
- pgp.rediris.es
- 11371
- Any Domain

A URL é http://pgp.rediris.es:11371

Una vez configurado, dende PGPKeys na opción: "Server" -> "Search"

Seleccionar como servidor pgp.rediris.es
Indicar o criterio de búsqueda (por exemplo indicar unha dirección de correo da que se sepa que ten unha chave PGP no servidor).
Cando PGP mostre o listado resultante, seleccionar unha chave PGP e pulsar co botón dereito do rato sobre a mesma. Se elixe a opción "Import to local keyring" pasa a estar engadida o anel local de chaves.

Enviar un certificado a un servidor de chaves

Cando anule un par de chaves PGP es recomendable anular tamén a chave pública nos servidores de claves (se foi publicada en algún). O mellor é anulalo no servidor de chaves de Rediris, que propagará os cambios a outros servidores PGP.

Importar o certificado de revocación ou revocar dende PGPKeys a chave que se desexa anular (pulsando sobre la chave co botón dereito e seleccionando a opción "revoke", o programa pedirá a palabra de paso da chave privada).

Unha vez feito isto o certificado de revocación aparecerá en PGPKeys cun aspa á súa esquierda, indicando que se trata dunha chave anulada.

Pode enviar esta chave anulada a un servidor pulsando co botón dereito sobre este certificado de revocación e seleccionando a opción "Send to". Dentro de esta opción seleccionar o servidor de chaves PGP de Rediris (nun apartado anterior indícase como engadir servidores PGP á configuración de PGPKeys).

Firmar ou cifrar mensaxes de correo a enviar

No programa PGPKeys, na opción: "Edit" -> "Options" -> "Email"

Pódense indicar distintas opcións a aplicar a correos enviados ou recibidos:

1. * Use PGP/MIME when sending email
2. Encrypt new messages by default
3. * Sign new messages by default
4. * Automatically decrypt/verify

Pode ter, por exemlo, activadas por defecto as opcións 1, 3 e 4 e só activar a 2 (cifrado automático de mensaxes) cando o considere necesario.

O plugin de PGP para Outlook non emprega os botóns de cifrado o firmado de mensaxes e Outlook, hai que configurar o uso de PGP en Outlook dende o programa PGPKeys.

Compre ter xerado e cargado no programa PGPKeys un par de chaves PGP para a dirección de correo que se esté a usar en Outlook.

Por exemplo se está a empregar unha identidade en Outlook que sexa usuario@uvigo.es, compre ter un par de chaves PGP no programa PGPKeys para esta dirección de correo. Se non ten chaves PGP para o mesmo hai que xeralas ou importalas dun arquivo ou servidor de chaves.

Antes de enviar un correo, se PGPKeys está configurado para firmar e/ou cifrar correos de forma automática, PGP pedirá a palabra de paso da chave privada PGP para firmar ou cifrar o correo a enviar.

Se os correos que se reciben foron firmados con PGP bastará con pulsar dúas veces en Outlook sobre o correo, PGP analizará a firma e a mensaxe e indicará se a firma corresponde á mensaxe e ó remitente da mesma. Deberá ter a chave pública do remitente importada en PGP para que este programa poda verificar a firma.

Uso de GNUPG (GPG)

GPG é a versión GNU de PGP. Este software é distribuido coas distribucións de Linux máis habituais. O contrario que o anterior está orientado a ser usado mediante órdenes na liña de comandos. Aquí resumiremos algunhas opcións disponibles, aínda que na páxina man de gpg pode atopar un inventario de todas as opcións existentes (a enumeración das mesmas excede o propoósito de este documento). Pode atopar mais información sobre GPG en esta páxina.

Listar anel de chaves dun usuario

@

```
gpg --list-keys
/home/usuario/.gnupg/pubring.gpg
------------------------------
pub  1024D/B46AFC40 2002-08-20 Usuario de proba
sub  2048g/0086AC14 2002-08-20
```

Xerar un par de chaves PGP

Úsase para isto a opción de gpg --gen-key, que crea o par de chaves e as engade ó anel de chaves do usuario.

Normalmente as opcións por defecto (DSA e RSA, 2048 bits) son suficientes.

- Xerar clave

  @

  ```
  gpg --gen-key
  ```

- Pedirá o tipo de chave desexado (a opción por defecto normalmente é suficiente)

@

```
...
Por favor seleccione tipo de clave deseado:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
```

- Pedirá a lonxtidue da chave, normalmente a que se ten por defecto (2048 bits) é suficiente

@

```
...
Su elección:
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
```

- Pedirá a expiración
  Normalmente non é razonable que esta sexa indefinida

@

```
...
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)? 2y
La clave caduca jue 08 nov 2018 13:59:48 CET
¿Es correcto? (s/n) s
```

- Indicar datos identificativos: nome, comentario, dirección de correo

@

```
...
Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo Electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Perico de los Palotes
Dirección de correo electrónico: usuario@uvigo.es
Comentario:
Ha seleccionado este ID de usuario:
    "Perico de los Palotes <usuario@uvigo.es>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
```

- Tardará un rato en xerar a chave nova

Importar unha chave ó anel de chaves do usuario

Úsase para importar chaves PGP a opción --import

Se desexa importar un par de chaves pública e privada (poden ser as chaves do usuario que foron xeradas en outro equipo) debe engadir a opción --allow-secret-key-import. Isto non é habitual, o normal é importar chaves públicas de outros usuarios dos que se quere verificar unha firma nun documento.

@

```
gpg --import --allow-secret-key-import copia-chave.asc
gpg: key 710E2B01: secret key imported
gpg: key 710E2B01: public key imported
gpg: Total number processed: 2
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

Enviar unha chave pública a un servidor

Por exemplo, para enviar a chave pública que corresponde á dirección de correo usuario@uvigo.es no anel local do usuario (ver coa opción --list-keys as chaves no anel) ó servidor pgp.rediris.es (o servidor PGP público de RedIris) faise o seguinte:

- Obter o identificador da chave

  @

  ```
  gpg --list-keys --keyid-format short
  pub   2048R/7EC48E37 2016-11-08 [caduca: 2017-11-30]
  uid                          Perico de los Palotes <usuario@uvigo.es>
  ```

- Enviar a chave a un servidor PGP (neste caso o de RedIRIS)
  O identificador é o que se ten na primeira columna da saída do comando anterior

  @

  ```
  gpg --keyserver pgp.rediris.es --send-keys 7EC48E37
  gpg: success sending to `pgp.rediris.es' (status=200)
  ```

Exportar unha chave

Para esto pódese empregar a opción "armor":

```
gpg --armor --export usuario@uvigo.es > chave.asc
```

Xerar un certificado de renovación de chave

En GPG é sinxelo crear o certificado de revocación, basta con usar a opción --gen-revoke.

```
@
gpg --gen-revoke usuario@uvigo.es
sec  1024D/B46AFC40 2002-08-20   Usuario de proba
Reason for revocation: Key is no longer used
(No description given)
Is this okay? y

You need a passphrase to unlock the secret key for
user: "Usuario de proba <usuario@uvigo"
1024-bit DSA key, ID B46AFC40, created 2002-08-20

ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org
Comment: A revocation certificate should follow

...
-----END PGP PUBLIC KEY BLOCK-----
```

Enviar certificado de revoación a un servidor de chaves

Para enviar o certificado de revocación de chave a un servidor PGP público, debe importar este certificado en GPG usando a opción --import en primeiro lugar para que sexa incluido no anel local de claves:

```
@
gpg --import revocacion.asc
gpg: key B46AFC40: revocation certificate imported
gpg: Total number processed: 1
gpg:    new key revocations: 1
Enviar o certificado de revocación unha vez importado en GPG coa opción --send-keys:$> gpg --keyserver
pgp.rediris.es --send-keys usuario@uvigo.es
gpg: success sending to `pgp.rediris.es' (status=200)
```

Frmar un documento

Para firmar un documento con, por exemplo, a chave do usuario usuario@uvigo.es (debe estar no anel local de chaves) úsase a opción --sign. En este caso indícase como tipo de saída ASCII (-armor), de forma que a firma en formato ASCII quedará no arquivo arquivo.txt.asc (o nome do arquivo de entrada engadindo a extensión .asc):

```
@
gpg --sign -armor -u usuario@uvigo.es arquivo.txt
```

Ou:

@

```
gpg --clearsign -u usuario@uvigo.es mensaje.txt
```

Verificar firma dun documento

Para verificar a firma do documento a partir do documento orixinal (arquivo.txt) e a firma (arquivo.txt.asc) no directorio local e a chave PGP do remitente incluida no anel de chaves locals úsase a opción --verify do seguinte xeito:

@

```
gpg --verify arquivo.txt.asc
gpg: Signature made Wed Oct 23 10:51:28 2002 MEST using DSA key ID B46AFC40
gpg: Good signature from "Usuario de proba "
```

En este caso a firma é correcta.