Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Xifra i signa digitalment el teu correu amb el certificat de la FNMT (amb Mutt) **(10739 lectures)**

Per **Kiko Piris**, ***kiko*** ()

Creado el 31/07/2004 01:50 modificado el 31/07/2004 01:50

> *El certificat X.509[1] expedit per la Fàbrica Nacional de Moneda y Timbre[2] no serveix només per a fer la declaració de renda[3] i obtenir informacions d'organismes com ara la Seguridad Social[4].*
>
> *També pot servir-nos per a xifrar i signar digitalment el nostre correu electrònic. I a més a més, es tractarà d'una signatura electrònica amb validesa legal reconeguda.*

El format criptogràfic *típic* que ens vé al cap quan parlam de xifrar i signar correu electrònic és el PGP (implementat per GnuPG[5]).

Idò bé, hi ha un altre format que es diu S/MIME i que fa servir certificats X.509 (els que utilitza el protocol https, i la capa ssl en general).

El certificat de la FNMT és un certificat X.509 estàndar i per lo tant podem utilitzar-lo per a xifrar i signar el nostre correu electrònic amb els clients de correu que suportin el format S/MIME (com per exemple Mutt[6], Mozilla[7], Mozilla Thunderbird[8], i altres).

Aquí explicaré com utilitzar aquest certificat[9] amb Mutt (he de dir que la informació està treta del README.SMIME de la documentació del paquet Debian[10] del Mutt).

El primer ingredient necessari serà el certificat personal que expedeix la FNMT (el de *clase 2 CA* que li diuen ells). Si no en tenim, aquí[11] ens expliquen que hem de fer per a obtenir-lo.

Suposant que ja el tenim (posats a suposar, suposarem que el tenim instal.lat al nostre Mozilla[12]).

El segon ingredient serà tenir instal.lats el OpenSSL[13] i el Mutt (compilat amb suport per a S/MIME). Jo ho he instal.lat tot amb apt-get a la meva **Debian *Sid*** i no m'ha fet falta rès més. Si utilitzau una altra *distro*, ***YMMV***.

Anam a configurar el smime per al Mutt pas a pas:

1.- Inicialitzar l'estructura de directoris smime:

Si mai hem fet servir S/MIME, haurem d'executar

```
$ smime_keys init
```

Això ens crearà el directori ~/.smime amb l'estructura adequada a dins.

2.- Descarregar i instal.lar el certificat arrel de la FNMT:

```
$ wget http://www.cert.fnmt.es/certificados/FNMTClase2CA.crt
$ openssl x509 -in FNMTClase2CA.crt -inform DER -outform PEM >> ~/.smime/ca-bundle.crt
```

~/.smime/ca-bundle.crt contindrà els certificats arrel, pot contenir tots els que vulguem. Per a utilitzar el certificat de la FNMT bastarà amb el seu (el FNMTClase2CA.crt[14]).

Un punt *obscur* i que trob que no està suficientment explicat a la web de la FNMT (bé, de fet no està gens explicat, ni ho esmenta), és com **comprovar que el certificat arrel és correcte**; i que no mos n'hem baixat un de fals.

El que hem de fer és aconseguir el BOE[15] de divendres dia 1 d'octubre de 1999[16], buscar el *fingerprint* (a la pàgina 35194[17]) i comparar-lo amb el del certificat que ens hem baixat:

```
      $ openssl x509 -in FNMTClase2CA.crt -inform DER -noout -fingerprint -md5
o bé
      $ openssl x509 -in FNMTClase2CA.crt -inform DER -noout -fingerprint -sha1
```

3.- Exportar el certificat del Mozilla a un arxiu:

```
3.1.- Obrirem el Mozilla i anirem a "Edit" / "Preferences".
3.2.- Allà escollirem "Privacy & Security" / "Certificates"
3.3.- Botó "Manage Certificates..."
3.4.- A la primera pestanya ("Your Certificates") marcam el nostre i triam "Backup"
3.5.- Triam un directori i un nom d'arxiu que recordem
3.6.- Posam el "master password for the Software Security Device" quan ens el demani.
3.7.- Triam un password per a protegir l'arxiu on estam exportant el certificat.
3.8.- "OK" i ja tenim el certificat exportat.
```

4.- Importar el certificat personal (i.e. el parell de claus pública i privada) **a l'arbre smime**:

```
$ smime_keys add_p12 ArxiuGuardatAlPasTresPuntCinc.p12
```

```
4.1.- Primer ens demana el password que hem posat en fer el backup al Mozilla (al pas 3.7).
4.2.- Després ens demana el password amb que hem de guardar el certificat a l'arbre smime (aquest password
l'haurem d'escriure al Mutt quan vulguem signar o desxifrar missatges.
4.3.- També li hem de posar una etiqueta a cada certificat que importem, en triam una que ens vagi bé
4.4.- El script ens dirà alguna cosa com

      added private key: /home/perico/.smime/keys/12345678.0 for perico@delospalotes.com

      Aquest 12345678.0 (incloent el .0 del final és el nostre keyid).

4.5.- L'arxiu que hem exportat amb el Mozilla (el del pas 3.5) podem esborrar-lo (o guardar-lo com a backup a
un lloc segur)
```

5.- Configurar el Mutt:

Li hem de dir al Mutt quina és la clau per defecte que ha d'utilitzar per a signar els missatges. **Ho farem afegint al nostre *.muttrc***:

```
set smime_default_key=keyid
set smime_sign_as=keyid
```

Segurament també us interessarà canviar els valors per defecte de ***smime_timeout*** i ***smime_encrypt_with***.

Llegiu el manual[18] i posau-hi lo que trobeu més adequat a les vostres necessitats (jo particularment he posat ***smime_encrypt_with=des3*** (el *smime_timeout* és cosa de cada un).

I ja està, amb això ja podem utilitzar el nostre certificat de la FNMT per a signar el correu tal i com ho feiem fins ara amb GnuPG (amb la tecla ***S*** en lloc de la ***p*** que utilitzam per a GnuPG).

Aconseguir i importar les claus públiques per a xifrar els missatges:

El dubte que sorgeix ara és: **i com aconsegueixo les claus públiques dels destinataris** dels missatges per a xifrar-los?

Aquí la cosa va un poc distinta que amb PGP, no hi ha servidors on poguem extreure les claus públiques, quan signam un missatge, la clau pública signant va adjunta al missatge.

El que hem de fer és intercanviar-mos un missatge signat abans i extreure'n la clau pública del mateix. Llavors la incorporam a l'arbre smime i ja la podrem utilitzar per a xifrar.

Això ho farem de la següent manera:

0.- Tenim un missatge signat amb S/MIME i volem extreure'n la clau pública per a poder xifrar-hi missatges amb ella.

1.- Entram al Mutt i editam el missatge (amb la tecla ***e***) i el guardam amb l'editor a un fitxer temporal (anomenem-lo msg.txt).

2.- Sortim del Mutt

3.- N'extreim el certificat (la clau pública):

```
$ cat msg.txt | openssl smime -verify -CAfile ~/.smime/ca-bundle.crt -signer cert.pem > /dev/null
```

4.- El pas anterior ens ha d'haver dit ***Verification successful*** sense donar-mos cap error

5.- I finalment l'incorporam a l'arbre smime:

```
$ smime_keys add_cert cert.pem
```

De moment, això és tot

Ja aniré completant l'article amb més coses a mesura que vagin sorgint. De moment això és suficient per a començar a *jugar-hi* una mica ;-)

Lista de enlaces de este artículo:

1. http://www.ietf.org/html.charters/pkix-charter.html
2. http://www.fnmt.es/
3. https://aeat.es/
4. http://www.seg-social.es/
5. http://www.gnupg.org/
6. http://www.mutt.org/

7. http://www.mozilla.org/products/mozilla1.x/
8. http://www.mozilla.org/products/thunderbird/
9. http://www.cert.fnmt.es/
10. http://www.debian.org/
11. http://www.cert.fnmt.es/clase2/main.htm
12. http://www.mozilla.org/
13. http://www.openssl.org/
14. http://www.cert.fnmt.es/certificados/FNMTClase2CA.crt
15. http://www.boe.es/
16. http://www.boe.es/g/es/boe/dias/1999-10-01/
17. http://www.boe.es/boe/dias/1999-10-01/tiffs/A35194.tif
18. http://www.mutt.org/doc/manual/

E-mail del autor: bulma _ARROBA_ pirispons.net