



Manual de càrrega de claus per a servidors Apache

Aquest document descriu el procediment a seguir per configurar el servidor Apache per admetre transmissions segures d'informació sota SSL per part d'un client amb un certificat digital vàlid emès per qualsevol entitat de certificació.

El mòdul MOD_SSL proporciona una sèrie de funcionalitats criptogràfiques a Apache, entre elles, la gestió de l'autenticació de client/servidor. Farem servir aquest mòdul, i en concret, les seves directives, per poder adaptar Apache per treballar amb certificats de les diferents EC que no siguin de la jerarquia CATCERT.

Per poder utilitzar aquest mòdul és imprescindible tenir una versió 1.3.x d'Apache, una versió 0.9.x d'OpenSSL, i descarregar el paquet MOD_SSL 2.8.x, des de <http://www.modssl.org/>.

Instal·lació MOD_SSL

El procés d'instal·lació és el següent:

1. Un cop descarregat el mòdul, s'ubica al directori /libexec d'Apache
2. Executar les següents comandes:

```
> cd /usr/local/modssl
> ./configure \
    --with-apache=../apache \
    --with-ssl=../openssl \
    --enable-shared=ssl \
> make
> make install
```

3. Recompilar i reinstal·lar Apache amb l'opció

```
--enable-module=modssl
```

Des d'aquest moment, per engegar Apache amb funcionalitat SSL, s'ha de fer:

```
> /usr/local/apache/bin/apachectl startssl
```

Configuració

El servidor Apache disposa d'un fitxer de configuració des d'on es gestionen les comunicacions entre els usuaris del servei i el propi servidor. Aquest fitxer, anomenat `http.conf`, conté tota una sèrie de directives de MOD_SSL que permeten dur a terme aquesta gestió. A continuació es detalla com carregar les EC amb les quals es vol treballar.



1. Localitzar la configuració SSL dins `http.conf`

```
<IfDefine SSL>  
...  
</IfDefine SSL>
```

2. Comprovar si el protocol SSL està habilitat

```
SSL SSLEngine on
```

3. Comprovar el certificat de servidor i la seva clau privada

```
SSLCertificateFile /usr/local/apache/conf/ssl.crt/certificatSERV.crt  
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/clausSERV.key
```

4. Indicar el directori on s'emmagatzemen les Autoritats de Certificació amb les quals es confia. Aquesta directiva s'utilitza per verificar si es confia en l'emissor del certificat del client.

```
SSLCACertificatePath /usr/local/apache/conf/ssl.crt/
```

Per carregar una nova EC en la qual es confiarà, el procediment és el següent:

- Ubicar el certificat en el directori esmentat en format PEM.
- Crear un nom simbòlic de la forma `hash.N` per al certificat. Això es pot fer amb la comanda `Makefile` que proporciona el mateix `MOD_SSL`.

5. Comprovar que l'autenticació de client està habilitada

```
SSLVerifyClient require
```

Existeixen moltes altres directives que proporcionen altres funcionalitats. Per consultar-les, es pot visitar el lloc Web de `MOD_SSL`: http://www.modssl.org/docs/2.8/ssl_reference.html#ToC13