

# Manual de gestió del certificat de servidor a l'Apache HTTP Server

## Control documental

<b>Estat formal</b>	<b>Elaborat per:</b>  Àrea Alcaide	<b>Aprovat per:</b>  Francesc Ferré
<b>Data de creació</b>	28/01/2008	
<b>Control de versions</b>	<b>Data:</b>	28/01/2008
	<b>Descripció:</b>	Creació del document
<b>Nivell accés informació</b>	pública	
<b>Títol</b>	Manual de gestió del certificat de servidor a l'Apache HTTP Server	
<b>Fitxer</b>	20080128_Gestio_certificats_CDS_Apache.doc	
<b>Control de còpies</b>	Només les còpies disponibles a Ubicació de les còpies controlades garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
<b>Drets d'autor</b>	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu <a href="http://creativecommons.org/licenses/by-nc-nd/2.5/es/">http://creativecommons.org/licenses/by-nc-nd/2.5/es/</a> o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

## Índex

---

<i>Manual de gestió del certificat de servidor a l'Apache HTTP Server</i> .....	1
<i>Control documental</i> .....	2
<i>Índex</i> .....	3
1. <i>Objecte</i> .....	4
2. <i>Generació del CSR</i> .....	5
3. <i>Instal·lació de les claus públiques</i> .....	6
4. <i>Instal·lació del certificat</i> .....	7

## 1. Objecte

L'objectiu del present document és el de descriure les instruccions necessàries per tal de portar a terme les següents tasques relatives a la gestió d'un CDS (Certificat de Dispositiu Segur) al servidor web Apache:

- Generar una sol·licitud de CDS (CSR: Certificate Signing Request).
- Instal·lar el CDS al servidor.
- Instal·lar les claus públiques de les entitats de certificació al servidor.

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.

## 2. Generació del CSR

Per generar una clau privada i la sol·licitud d'un Certificat de Dispositiu Servidor (CDS) en un servidor *Apache*, cal seguir els passos següents des de la línia de comandes:

```
openssl req -new -nodes -keyout nomserver.key -out server.csr
```

Això crea dos arxius: l'arxiu *nomserver.key* conté una clau privada, que cal protegir de forma curosa, i fer-ne una còpia de seguretat.

Després li demanarà escriure les dades que constaran al CSR: el que se'n diu un *nom distingit (Distinguished Name) o DN*. Les dades que demanarà son:

```
-----  
Country Name (2 letter code) [ ]: (Codi del país - 2 lletres)  
State or Province Name [ ]: (Província)  
Locality Name [ ]: (Ciutat)  
Organization Name [ ]: (Entitat)  
Organizational Unit Name [ ]: (Departament)  
Common Name* [ ]: (domini o subdomini pel que se sol·licita el certificat. Assegureu-vos de que tot és correcte i que conté un domini principal o subdomini -ex. seguretat.catcert.net, www.catcert.net, ...).  
Email Address [ ]: (adreça de correu-e)
```

Finalment li demanarà les següents dades:

```
Challenge password [ ]: (Contrasenya)  
Optional company name [ ]: (Nom alternatiu de l'organització)  
-----
```

**\*\*** Si a algun dels camps hi posa '.' aquest quedarà en blanc. Poden deixar-se en blanc els camps Email Address i Optional company name.

Amb això ja haureu generat el fitxer CSR. Guardeu en un fitxer ".csr" tot el contingut comprès entre:

```
-----BEGIN CERTIFICATE REQUEST-----  
fins a  
-----END CERTIFICATE REQUEST-----
```

### 3. Instal·lació de les claus públiques

Indicar el directori on s'emmagatzemen les Autoritats de Certificació en les quals es confia. Aquesta directiva del fitxer de configuració *http.conf* 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.  
Per convertir un certificat a format PEM, cal executar la següent instrucció, des de línia de comandes:  

```
openssl x509 -inform der -in nomfitxer -out nomfitxer.pem
```

on *nomfitxer* és el fitxer que conté el certificat en format binari.
- Un cop hem convertit el certificat a format PEM, l'editarem amb un editor de text, i copiarem el seu contingut al final del fitxer /usr/local/apache/conf/ssl.crt/ (començant en una nova línia). Guardem els canvis del fitxer ssl.crt.

## 4. Instal·lació del certificat

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
```