



**inteco**

Instituto Nacional  
de Tecnologías  
de la Comunicación

# **GUÍA DE IMPORTACIÓN DE CERTIFICADOS RAÍZ Y SUBORDINADOS DE LA AUTORIDAD DE CERTIFICACIÓN PARA EL DNI-E EN APACHE**

**CENTRO DE RESPUESTA A INCIDENTES DE  
SEGURIDAD (INTECO-CERT)**

**NOVIEMBRE 2007**

## ÍNDICE

|           |                               |          |
|-----------|-------------------------------|----------|
| <b>1.</b> | <b>INTRODUCCIÓN</b>           | <b>3</b> |
| <b>2.</b> | <b>INSTALACIÓN DE MOD_SSL</b> | <b>4</b> |
| <b>3.</b> | <b>CONFIGURACIÓN</b>          | <b>5</b> |

## 1. INTRODUCCIÓN

---

### Guía de importación de certificados raíz y subordinados de la Autoridad de Certificación para el DNI-e en Servidores Apache

Este documento describe el procedimiento a seguir para configurar el Servidor Web Apache para aceptar transmisiones seguras por parte de un cliente con DNI electrónico.

El módulo MOD\_SSL proporciona una serie de funcionalidades criptográficas en Apache, y entre ellas está la gestión de la autenticación de cliente/servidor. Utilizaremos este módulo, y en concreto sus directivas, para poder adaptar Apache para que trabaje con certificados digitales en general y específicamente con el DNI electrónico.

Para poder utilizar este módulo, es imprescindible tener una versión 1.3.x de Apache, una versión 0.9.x de OpenSSL, y descargar el paquete MOD\_SSL 2.8.x desde <http://www.modssl.org/>

## 2. INSTALACIÓN DE MOD\_SSL

---

El proceso de instalación es el siguiente:

1. Una vez descargado el módulo, se ubica en el directorio /libexec de Apache.
2. Seguidamente será necesario ejecutar los siguientes comandos:

```
> cd /usr/local/modssl
```

```
> ./configure \
```

```
    -- with-apache=../apache \
```

```
    -- with-ssl=../openssl \
```

```
    -- enable-shared=ssl \
```

```
> make
```

```
> make install
```

3. Recompilar y reinstalar Apache con la opción:

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

Desde este momento, para arrancar Apache con funcionalidad SSL, se ha de ejecutar el siguiente comando:

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

### 3. CONFIGURACIÓN

---

El servidor Apache dispone de un fichero de configuración desde donde se gestionan las comunicaciones entre los usuarios del servicio y el propio servidor. Este fichero, denominado http.conf, contiene toda una serie de directivas de MOD\_SSL que permiten llevar a término esta gestión. A continuación se detalla cómo cargar la Autoridad de Certificación del DNle.

1. Localizar la configuración SSL dentro de http.conf

```
<Indefine SSL>
```

```
...
```

```
</Indefine SSL>
```

2. Comprobar si el protocolo SSL está habilitado

```
SSL SSLEngine on
```

3. Comprobar el certificado de servidor y su clave privada

```
SSLCertificateFile /usr/local/apache/conf/ssl.crt/certificatSERV.crt
```

```
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/clausSERV.key
```

4. Indicar el directorio donde se guarda la Autoridad de Certificación del DNle. Esta directiva se utiliza para verificar si se confía en el emisor del certificado del cliente.

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

Para cargar el resto de Autoridades de Certificación subordinadas en las cuales se confiará, el procedimiento es el siguiente:

- Ubicar el certificado en el directorio indicado en formato PEM
    - Crear un nombre simbólico de la forma hash.N para cada certificado. Se puede hacer con el comando Makefile que proporciona el mismo MOD\_SSL
  5. Comprobar que la autenticación de cliente está habilitada
- ```
SSLVerifyClient require
```

Existen muchas otras directivas que proporcionan otras funcionalidades relacionadas. Para consultarlas, se puede visitar la web MOD\_SSL: [http://www.modssl.org/docs/2.8/ssl\\_reference.html#ToC13](http://www.modssl.org/docs/2.8/ssl_reference.html#ToC13)