

---

# Módulo 2.2

---



Redes y Seguridad  
Gr. Ing. Informática  
J.L. Vázquez Poletti

---

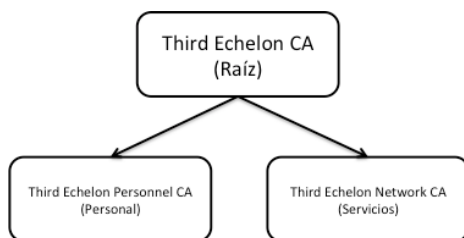
## Objetivo

En este módulo constituiremos una jerarquía simple de Autoridades de Certificación para luego expedir un certificado que permita a un servidor web ofrecer sus contenidos a través del protocolo SSL.

**Atención:** a lo largo de la práctica se fijarán diferentes contraseñas para diferentes servicios. Es muy recomendable apuntarlas.

## Punto de partida

La confianza es otro de los aspectos clave en Third Echelon. Por ello, se ha decidido constituir una Autoridad de Certificación (AC) de la que colgará unas Sub-ACs que serán la que expidan certificados al personal y los servicios informáticos de la agencia. De esta manera, se podrá compartimentalizar la gestión de confianza en caso de un agujero de seguridad.



Dado lo sensible de los datos expuestos a través del servidor web, éste será uno de los destinatarios de los certificados expedidos por la Sub-AC.

El toolkit escogido es OpenSSL debido a que es código abierto y por lo tanto mantenido por una gran comunidad, garantizando una respuesta inmediata ante cualquier fallo de seguridad.

Aunque OpenSSL se usa en la línea de comandos, se empleará un interfaz gráfico para la gestión (TinyCA). Éste se invoca con el comando **tinyca2**.

## Creación de la Autoridad de Certificación Raíz

En la ventana en la que se piden los datos para la creación se pondrán los siguientes (el resto queda a elección del alumno):

- Nombre (local): thirdechelonCA
- Nombre (AC): ThirdEchelonCA
- País: US
- Estado: Maryland
- Ciudad: Fort Meade
- Organización: Third Echelon
- Departamento (Unit): Network Security
- E-Mail: networkops@nsa.gov
- Validez: 365
- Digest: MD5

## Máquinas Virtuales

- RyS-ThirdEchelon  
(ubuntu:reverse)


## Más información

OpenSSL: <http://www.openssl.org/>


TinyCA: <http://tinyca.sm-zone.net/>

Apache HTTP: <http://httpd.apache.org/>

En la siguiente ventana se cambiará el comentario por “Third Echelon Certificate”.

Una vez creada, se verificarán los datos pulsando en el siguiente icono de la barra de tareas: 

## Creación de las Sub-Autoridades de Certificación



A continuación, se procederá a crear la sub-AC de Servicios (**Third Echelon Personnel**) a partir de la AC construida anteriormente. Para ello, comprobando que se está en la pestaña **CA**, se pulsará en el siguiente icono **ubicado en la parte derecha** de la barra de tareas: 

Se introducirán los siguientes datos (el resto queda a elección del alumno, salvo que ya aparezcan rellenados por defecto por la CA raíz):

- Nombre (local): thirdechelonnetworkCA
- Nombre (CA): Third Echelon Network CA
- E-Mail: networkops@nsa.gov
- Validez: 365
- Digest: MD5

**IMPORTANTE:** La contraseña para crear la nueva AC (primer campo) es la misma que se introdujo en la AC Raíz.

La verificación de los datos se realizará ahora de dos formas:

1. A través del icono ya empleado anteriormente:
2. A través de la información de la AC Raíz
  - a. Volver a la misma pulsando en: 
  - b. Escogerla en la lista (**thirdechelonCA**)
  - c. Acceder a la pestaña de certificados y visualizar la información con: 
  - d. Acceder a la pestaña de claves y verificar que la de la Sub-AC está listada

Siguiendo el mismo procedimiento anterior (creación y verificación), se creará la Sub-CA de Personal (**Third Echelon Personnel CA**) con los siguientes datos:

- Nombre (local): thirdechelonpersonnelCA
- Nombre (CA): Third Echelon Personnel CA
- E-Mail: hr@nsa.gov
- Validez: 365
- Digest: MD5

## Solicitud de un Certificado Personal

El certificado para el un miembro del personal se solicitará a la Sub-AC (**Third Echelon Personnel CA**). Por ello, se deberá cambiar a dicha AC.

En la pestaña solicitudes se marcará la opción de crear una nueva (las opciones se despliegan con el botón derecho del ratón).

En la ventana siguiente se pondrán los datos del alumno.

La verificación de la solicitud se realizará de dos maneras con el botón derecho del ratón:

- Visualizando la petición en crudo
- Visualizando los detalles por categorías

## Firma del Certificado Personal

Siempre con el botón derecho del ratón se marcará la opción de firma en la petición correspondiente, y de ahí, la opción de **Servidor**.

Se deberá usar la firma de la Sub-AC para firmar el certificado.

## Solicitud del Certificado para el Servidor Web

El certificado para el servidor web (**thirdechelon**) se solicitará a la Sub-AC (**Third Echelon Network CA**). Por ello, se deberá cambiar a dicha AC.

En la pestaña solicitudes se marcará la opción de crear una nueva (las opciones se despliegan con el botón derecho del ratón). En la ventana en la que se piden los datos para la creación se pondrán los siguientes (el resto queda a elección del alumno):

- Nombre: thirdechelon
- E-Mail: webmaster@nsa.gov
- Digest: MD5

La verificación de la solicitud se realizará de dos maneras con el botón derecho del ratón:

- Visualizando la petición en crudo
- Visualizando los detalles por categorías

## Firma e instalación del Certificado para el Servidor Web

Siempre con el botón derecho del ratón se marcará la opción de firma en la petición correspondiente, y de ahí, la opción de **Servidor**.

Se deberá usar la firma de la Sub-AC para firmar el certificado.

A continuación, en la pestaña de **certificados**, se elegirá la opción de **exportar**. El nombre del fichero deberá estar en **/home/ubuntu/** y llamarse **thirdechelon-cert.pem**.

Realizaremos el mismo proceso en la pestaña de claves. En este caso, se deberá exportar **sin** clave y el fichero deberá llamarse **thirdechelon-key.pem**. Se nos pedirá la contraseña asociada al certificado.

Por último, exportaremos la cadena de certificados. Esto se realizará en la pestaña de la **AC** y ahí se pulsará en el primer icono de la derecha:



**Atención:** Las operaciones que se solicitan a continuación se deberán realizar con permisos de **root**, por tanto, hay que añadir **sudo** al comienzo de los comandos que se ejecutarán.

1. Copiar los tres archivos **.pem** generados al directorio **/etc/ssl/private/**
2. Activar el módulo SSL con el siguiente comando: **a2enmod ssl**
3. Crear un fichero llamado **thirdechelon** en el directorio **/etc/apache2/sites-enabled** con el siguiente contenido:

```
<virtualhost *:443>

ServerAdmin webmaster@thirdechelon

ServerName thirdechelon

DocumentRoot /var/www/

ErrorLog /var/log/apache2/thirdechelon-ssl-error.log

LogLevel warn

CustomLog /var/log/apache2/thirdechelon-ssl-access.log combined

ServerSignature On

SSLEngine on

SSLCertificateFile /etc/ssl/private/thirdechelon-cert.pem

SSLCertificateKeyFile /etc/ssl/private/thirdechelon-key.pem

SSLCertificateChainFile /etc/ssl/private/thirdechelonnetworkCA-cachain.pem

</virtualhost>
```

4. Reiniciar el servidor web con **/etc/init.d/apache2 restart**

Ahora es el momento de abrir el navegador (**Firefox**) y entrar en la siguiente página: <https://thirdechelon/>

¿Qué problema surge y por qué?

## Estableciendo confianza en la AC Raíz

Hay dos maneras de establecer confianza en la AC Raíz (**Third Echelon CA**): una que afecta exclusivamente al navegador y otra a todo el sistema.

Para ambas hay que exportar el certificado de la AC. Para ello, hay que abrirla en **TinyCA** y, siempre en la pestaña de la **AC**, pulsar en el segundo icono de la derecha:



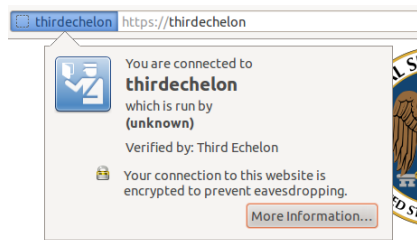
Se usará el nombre por defecto del archivo (**thirdechelonCA-cacert.pem**).

### Instalación del certificado en el navegador

1. En las preferencias, acceder a la pestaña de las avanzadas
2. En la pestaña de encriptación, ver los certificados
3. Importar el certificado que se ha exportado anteriormente desde **TinyCA**
4. Marcar los tres propósitos para los cuales se confiará en la AC raíz

5. Verificar que la AC raíz ahora aparece en la lista
6. Reiniciar **Firefox**

Ahora se debería acceder a <https://thirdechelon/> sin problemas. Se verificarán los **datos del certificado** (y la **jerarquía de los certificados**) a través del área a la derecha de la barra de direcciones:



¿Por qué no hay problemas en la conexión si se importó el certificado de la AC Raíz (**Third Echelon CA**) habiendo sido la Sub-AC (**Third Echelon Network CA**) la que emitió el certificado del servidor?

A continuación, se **borrarán** los certificados (AC Raíz y Sub-AC) de la lista en el navegador y se comprobará que el acceso a la página vuelve a dar problemas.

#### **Instalación del certificado en el sistema**

1. Copiar el certificado que se ha exportado anteriormente desde **TinyCA** al directorio `/usr/share/ca-certificates/`
2. Ejecutar **update-ca-certificates**

Tras reiniciar **Firefox**, volver a entrar en <https://thirdechelon/> y verificar la información de la conexión y los certificados.

¿Qué ventajas y desventajas tiene instalar el certificado en el sistema?