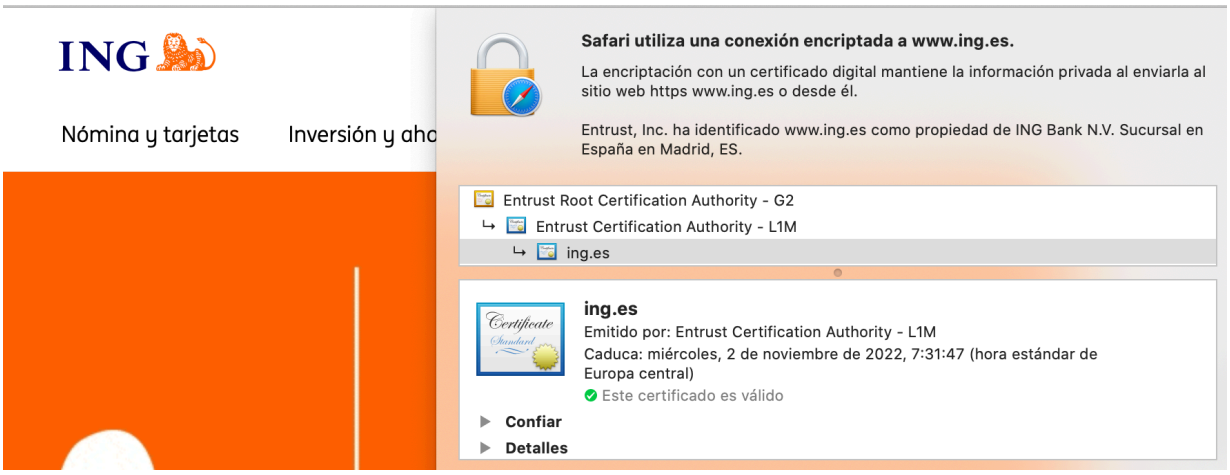
ACCESO A WEB USANDO UN CERTIFICADO DIGITAL (HTTPS)

Si queremos que el acceso a nuestra web se haga de forma seguro, cifrando las comunicaciones, debemos usar un certificado digital. Hay dos tipos de certificados:

- **certificado autofirmado**: no auténtica realmente la web, solo nos va a valer para cifrar las comunicaciones. Es un certificado que emitimos nosotros mismos.

- **certificado SSL** (firmado por una CA): este certificado, además de lo anterior, certifica que la web a la que accedes es la auténtica, por tanto, este tipo de certificado va asociado a un dominio o una URL, del tipo jacuela.com Para obtener este certificado tenemos que ser dueños del dominio y lo podemos comprar en varias compañias de hosting. Es emitido por alguna de las varias autoridades de certificación que existen, como VeriSign, GlobalSign, etc.



El protocolo a usar es el HTTPS, que usa el puerto 443. Para crear una web segura que funciona mediante dicho protocolo https, debemos realizar los siguientes pasos:

- Activar el módulo de SSL (esto vale para activar el puerto 443)
- Crea una pareja de claves, la privada y la pública mediante un certificado autofirmado
- Crear un nuevo VirtualHost que use el puerto 443
- Añadir al VirtualHost las directivas para usar la pareja de claves
- Crear el index.html en el directorio correspondiente indicado en el DocumentRoot

Activar el módulo de SSL
Activaremos el módulo SSL con el comando

```
# a2enmod SSL
```

Comprobaremos que esta activado de dos formas:

✓Mirando que tenemos el puerto 443 abierto con el comando `#nmap localhost`

✓Mirando que el módulo SSL aparezca activado en el directorio *mods_enabled*

Crea una pareja de claves, la privada y la pública
Para crear una contraseña y un certificado, después de tener instalado el paquete *openssl*, deberemos ejecutar los siguientes comandos:

Ejemplo para la web www.redinterna.org

```
#mkdir /etc/apache2/ssl

#openssl req -newkey rsa:2048 -x509 -sha256 -days 365 -nodes
          -out /etc/apache2/ssl/www.redinterna.org.crt
          -keyout /etc/apache2/ssl/www.redinterna.org.key
```

-newkey rsa:2048 —> creamos una nueva clave privada y especificamos la longitud de clave
-x509 —> crear un certificado autofirmado
-sha256 —> usar algoritmo de resumen sha256
-days256 —> crear el certificado para una validez de 365 días
-nodes —> la clave privada no será encriptada (evita tener que introducir cada vez la contraseña para acceder a la clave privada)
-out —> archivo de salida donde almacenar el certificado
-keyout —> archivo de salida donde almacenar la clave privada

```
Generating a 2048 bit RSA private key
.....................................++++++
.............................++++++
writing new private key to '/etc/apache2/ssl/apache.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Almeria
Locality Name (eg, city) []:Huercal-Overa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Cura
Valera
Organizational Unit Name (eg, section) []:Dpto. Informatica
Common Name (eg, YOUR name) []:www.redinterna.org
Email Address []:admin@redinterna.org
```

El *Common Name* es conveniente que sea la página web de la que queramos crear el certificado. De esta forma, aunque SI que nos aparecerá el mensaje de que el certificado no ha sido firmado por una CA de confianza, al menos NO nos aparecerá el mensaje de que es para otro sitio diferente.

La clave pública realmente es el certificado autofirmado por nosotros mismos.

Crear un nuevo VirtualHost que use el puerto 443 con las directivas adecuadas
Un ejemplo del mismo sería:

```
<VirtualHost *:443>
      …

      ServerName XXXXXXXXX
      DocumentRoot /var/www/XXXXXXXXXXXXXXXXX
      SSLEngine On
      SSLCertificateKeyFile RUTA_ABSOLUTA_ARCHIVO.key
      SSLCertificateFile RUTA_ABSOLUTA_ARCHIVO.crt
      …

</VirtualHost>
```