¿Puedo solicitar el certificado electrónico personal generando las claves manualmente?

Sí, es posible generar las claves manualmente antes de proceder a la solicitud del certificado. Puede seguir los procedimientos en esta ayuda:

¿Cómo genero un CSR desde Linux / Mac OS X?

Con la herramienta OpenSSL se pueden generar las claves asimétricas y obtener el CSR apropiado para solicitar el certificado electrónico personal.

Descargar a una carpeta temporal el fichero `openssl.cnf` es un fichero de texto creado previamente, cuyo contenido debe ser el siguiente:

openssl.cnf

```
HOME = .

#----------------------------------------------------------------------
[ req ]
string_mask = utf8only
default_bits = 2048
default_keyfile = certificado.key
default_md = sha256
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

[ req_distinguished_name ]
C = ES
O = "Universitat Politècnica de València"
CN = usuario.upv.es

[ req_ext ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature,keyEncipherment
extendedKeyUsage = serverAuth,clientAuth
```

Abrir una consola, y pasarse a dicha carpeta. Ejecutar la siguiente orden para generar la solicitud:

consola

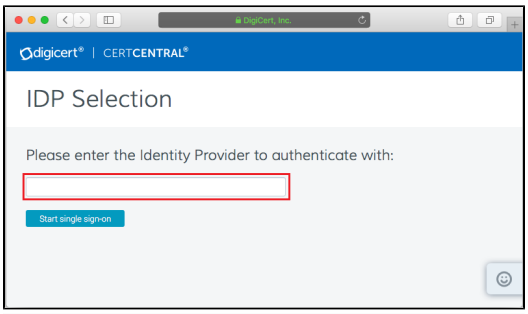
```
openssl req -new -config openssl.cnf -out certificado.csr
```

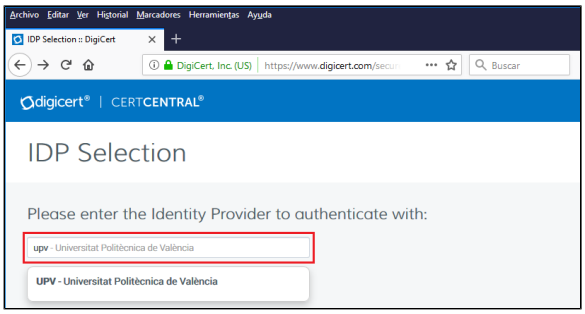
El contenido del fichero CSR resultante es literal, no hay que realizar cambios cuando lo incorporamos al formulario de solicitud del cetificado (copiar y pegar en el campo CSR del formulario web de solicitud). Los datos personales del solicitante (nombre y apellidos, dirección de correo electrónico, organización) se obtienen durante el proceso de autenticación.

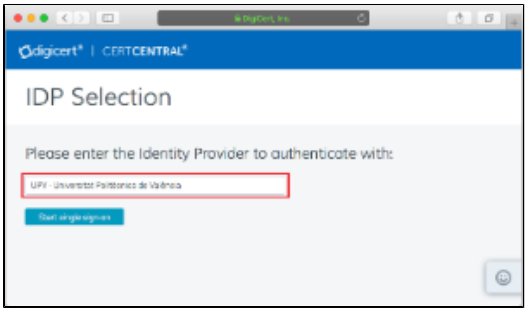
¿Cómo completo la petición desde Linux / Mac OS X?

Desde la consola, y estando en la carpeta temporal creada en el apartado ¿Cómo genero un CSR desde Linux / Mac OS X?, copiar al portapapeles el contenido del fichero `certificado.csr`.

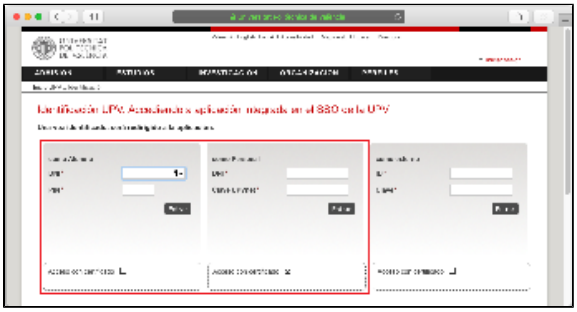
Acceder a la página https://www.digicert.com/sso/. En el campo *Identity Provider* escribir "upv" (sin las comillas). A continuación debe aparecer el resultado de UPV-Universitat Politècnica de València. Pulsar *Start single sign-on* (botón).



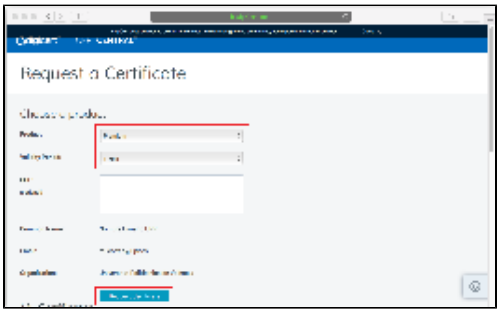




Si no estábamos previamente identificados en la Intranet de la UPV (con el navegador con el que estamos realizando la solicitud), se nos abrirá una página para la identificación en la UPV (*Identificación UPV. Accediendo a aplicación integrada en el SSO de la UPV*).



Aparece una página que permite solicitar un nuevo certificado y gestionar los certificados ya emitidos. En el campo *Product* seleccionar *Premium*. En *Validity Period*, 1, 2 o 3 años. Desde el portapapeles, pegar el contenido en el campo *CSR (optional)*. Pulsar *Request Certificate* (botón).



En la página *Request a Certificate* aparece la sección *My Certificates* con los certificados solicitados, y el ID del que se acaba de solicitar (*Certificate Order Requested. (Order # 1234567)*). Descargar el certificado a la carpeta temporal utilizada anteriormente con el nombre `certificado.crt`.

Generar un fichero PKCS12, que contenga el certificado y la clave privada, ejecutando la siguiente orden en la consola:

consola

```
openssl pkcs12 -export -inkey certificado.key -in certificado.crt -out certificado.p12
```

Es conveniente realizar una copia de seguridad del fichero `certificado.p12`. El resto de ficheros utilizados (`certificado.key, certificado.csr`) debería eliminarlos (es la opción más segura).

Puede instalar el certificado (con su clave privada correspondiente) en el contexto en el que lo necesite, a partir del fichero `certificado.p12` recién creado.

Cómo Instalar un certificado.

¿Cómo genero un CSR desde Windows?

En Windows se puede utilizar la herramienta OpenSSL, pero no viene instalada en el sistema operativo; así que es más cómodo utilizar las propias herramientas de Windows (certreq.exe) para generar las claves asimétricas y obtener el CSR apropiado para solicitar el certificado.

Descargar a una carpeta temporal el fichero `certreq.inf,` o crear uno cuyo contenido debe ser el siguiente:

certreq.inf

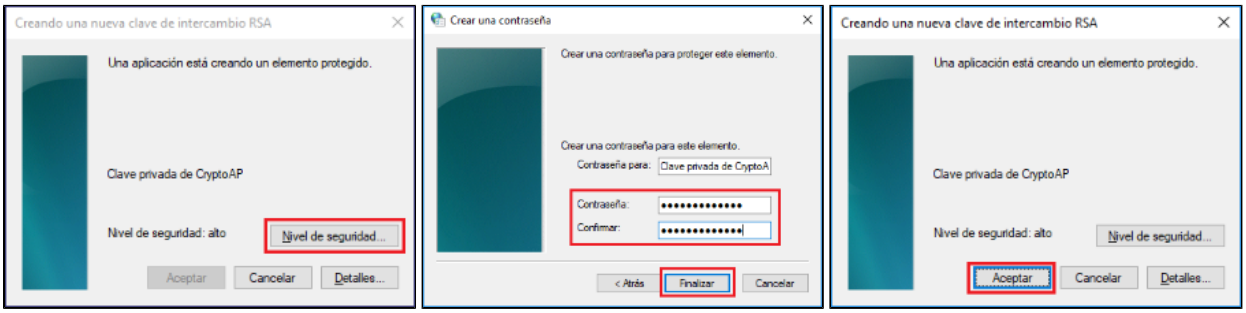
```
[NewRequest]
Subject = "CN=upv.es"
Exportable = TRUE
KeyProtection = NCRYPT_UI_FORCE_HIGH_PROTECTION_FLAG
KeyLength = 2048
KeyUsage = 0xFF
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
Silent = false RequestType = PKCS10
```

Abrir una consola, y pasarse a dicha carpeta. Ejecutar la siguiente orden para generar la solicitud:

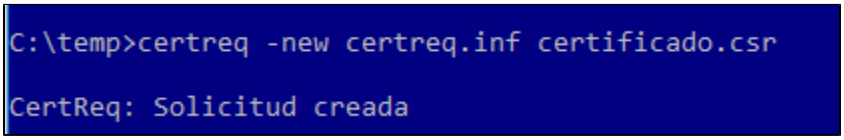
consola

```
certreq -new certreq.inf certificado.csr
```

A continuación se nos muestra una ventana para gestionar la creación de una nueva clave de intercambio RSA. Pulsar *Nivel de seguridad...* (botón). Establecer una contraseña que proteja la clave; pulsar *Finalizar* (botón). A continuación pulsar Aceptar (botón).



En la carpeta temporal seleccionada, se ha creado el fichero CSR con el nombre `certificado.csr`.



El contenido del fichero CSR resultante es literal, no hay que realizar cambios cuando lo incorporamos al formulario de solicitud del cetificado (copiar y pegar en el campo CSR del formulario web de solicitud). Los datos personales del solicitante (nombre y apellidos, dirección de correo electrónico, organización) se obtienen durante el proceso de autenticación.

¿Cómo completo la petición desde Windows?

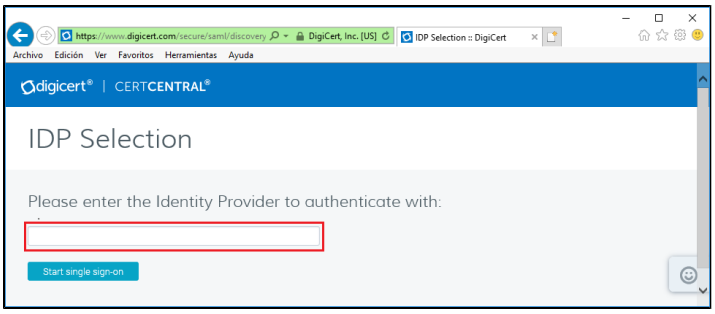
Copiar el contenido del fichero `certificado.csr` generado anteriormente al portapapeles según se describe en ¿Cómo genero un CSR desde Windows?

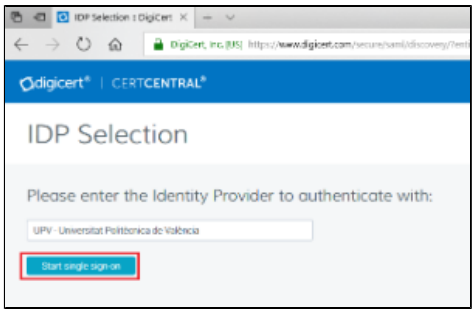
Podemos copiarlo desde la consola, y estando en la carpeta temporal creada en ¿Cómo genero un CSR desde Windows?, siguiendo el siguiente comando:

consola

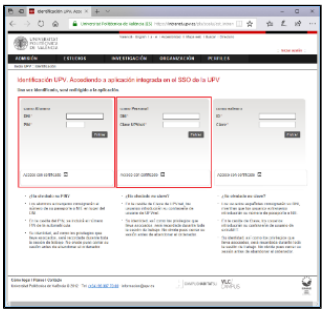
```
clip < certificado.csr
```

Acceder a la página https://www.digicert.com/sso/. En el campo *Identity Provider* escribir "upv" (sin las comillas). A continuación debe aparecer el resultado de UPV-Universitat Politècnica de València. Pulsar *Start single sign-on* (botón).

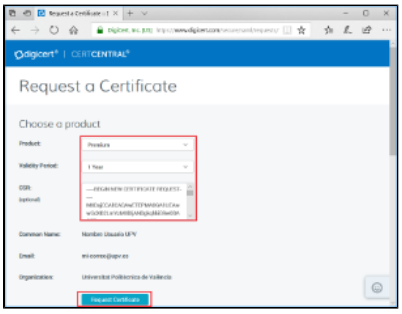




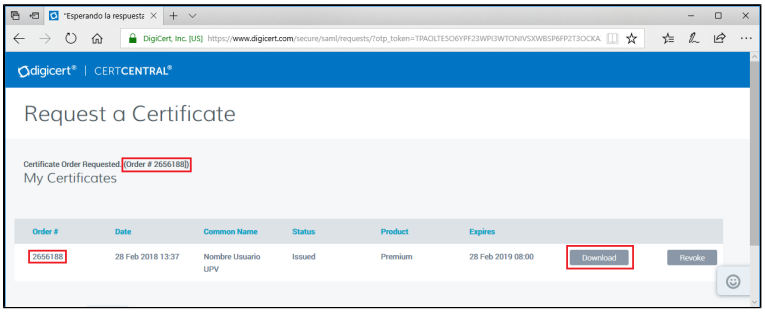
Si no estábamos previamente identificados en la Intranet de la UPV (con el navegador con el que estamos realizando la solicitud), se nos abrirá una página para la identificación en la UPV (*Identificación UPV. Accediendo a aplicación integrada en el SSO de la UPV*).



Aparece una página que permite solicitar un nuevo certificado y gestionar los certificados ya emitidos. En el campo *Product* seleccionar *Premium*. En *Validity Period*, 1, 2 o 3 años. Desde el portapapeles, pegar el contenido en el campo *CSR (optional)*. Pulsar *Request Certificate* (botón).



En la página *Request a Certificate* aparece la sección *My Certificates* con los certificados solicitados, y el ID del que se acaba de solicitar (*Certificate Order Requested. (Order # 1234567)*). Descargar el certificado a la carpeta temporal utilizada anteriormente con el nombre `certificado.crt`.



Instalar el certificado ejecutando la siguiente orden en la consola:

consola

```
certreq -accept certificado.crt
```

El certificado queda instalado en el almacén de certificados del sistema operativo.