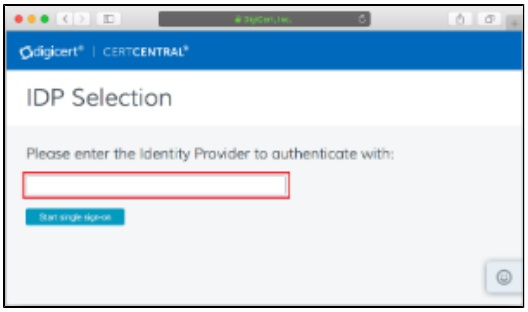
Con Safari (solicitar e instalar)

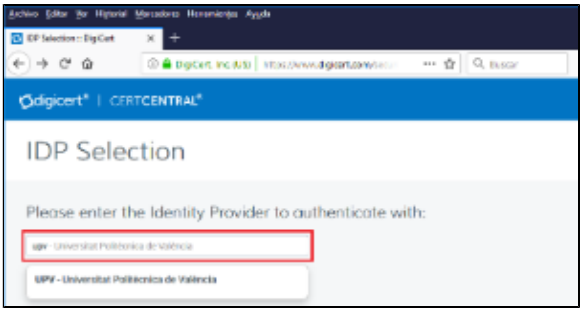
Si, desde el navegador Safari en Mac OS X es posible solicitar e instalar automáticamente el certificado electrónico personal.

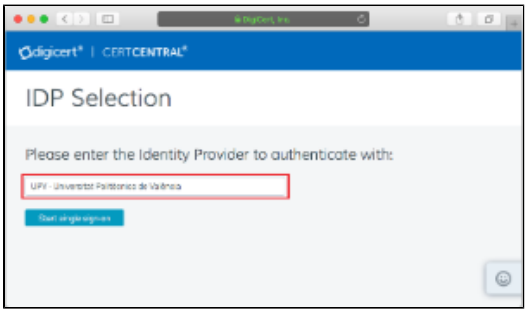
También puede seguir un procedimiento manual para la generación las claves con las instrucciones descritas en ¿Cómo genero un CSR desde Linux / Mac OS X? en esta misma ayuda.

Es necesario instalar, más tarde, el certificado de entidad intermedia (TERENA Personal CA 3) que hay que descargar tras generar el certificado.

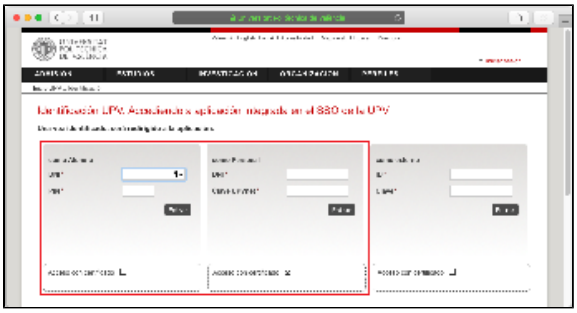
1.- Acceder a la web https://www.digicert.com/sso/ y generar el certificado. En el campo *Identity Provider* escribir "`upv`" (sin las comillas). Debe aparecer el resultado de `UPV-Universitat Politècnica de València` en el campo *Identity Provider*. Pulsar *Start single sign-on* (botón).



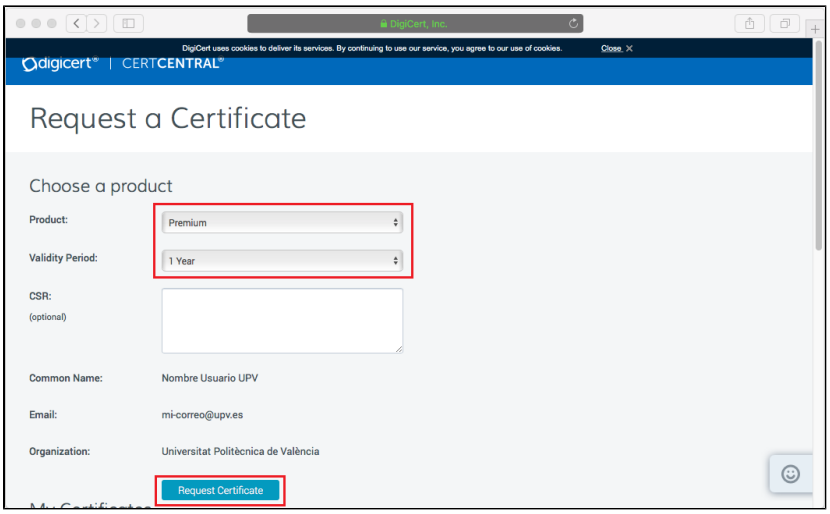




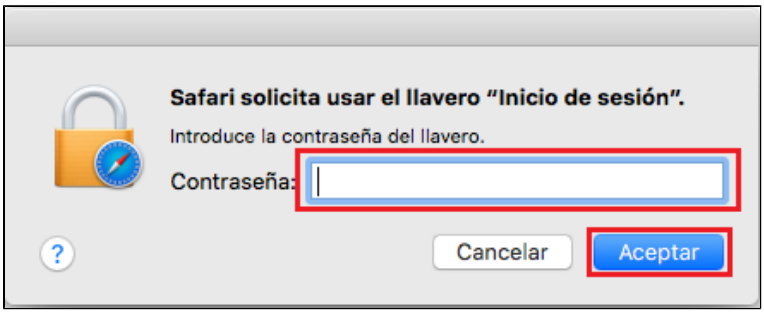
2.- Si no estábamos previamente identificados en la Intranet de la UPV (con el navegador utilizado para la solicitud), se nos abrirá una página para la identificación en la UPV (*Identificación UPV. Accediendo a aplicación integrada en el SSO de la UPV*).



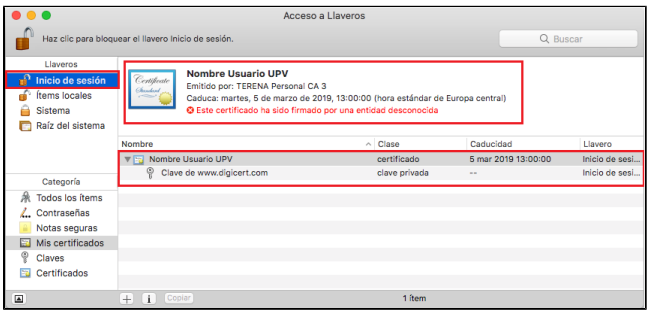
3.- Aparece una página que permite solicitar un nuevo certificado y gestionar los certificados ya emitidos. En el campo *Product* seleccionar ***Premium***. En *Validity Period*, 1, 2 o 3 años. Pegar el contenido del fichero `certificado.csr`, que habíamos copiado antes en el portapapeles en el campo *CSR (optional)*. Pulsar *Request Certificate* (botón).



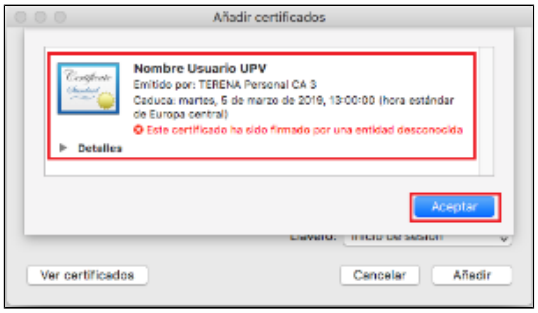
4.- Se abre la aplicación *Acceso a Llaveros.* Si el llavero *Inicio de sesión* está bloqueado (candado cerrado), deberá facilitar la contraseña que utilizó en el inicio de la sesión para desbloquearlo.



5.- Si el llavero *Inicio de sesión no* está bloqueado (candado abierto) se nos muestra *Anadir certificados* (ventana). Pulsar *Añadir* (botón).

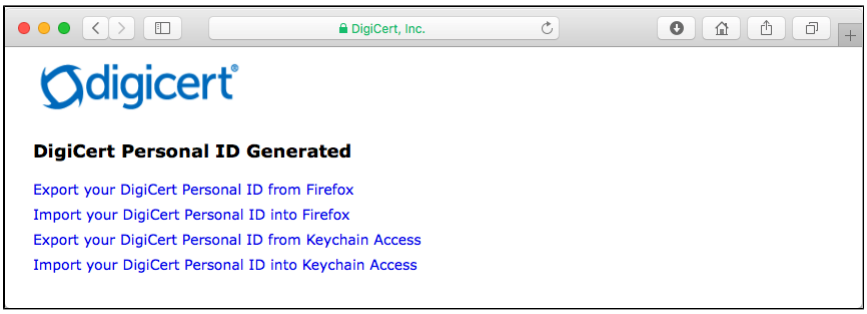


6.- Si previamente hemos pulsado *Ver certificados* (botón) comprobaremos que nos muestra un error (*Este certificado ha sido firmado por una entidad desconocida*), ya que aún está pendiente la instalación del certificado de la CA intermedia (TERENA Personal CA 3), que instalaremos más tarde.



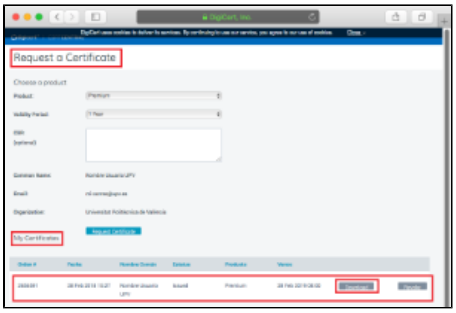
7.- Al final del proceso de solicitud se nos muestra una página web con enlaces a tutoriales para la exportación e importación del certificado generado, que ha sido instalado en el llavero de inicio de sesión del usuario activo, y que se puede gestionar con la aplicación *Acceso a Llaveros* (*Keychain Access*):

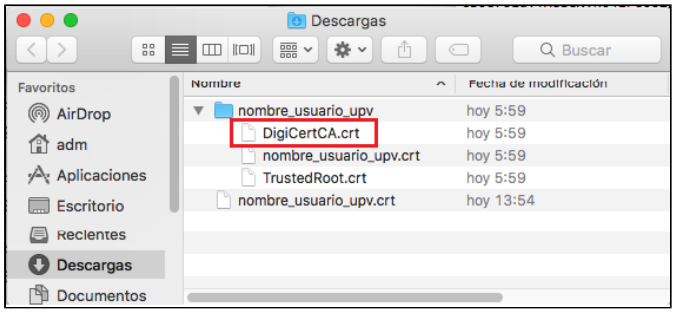
- Export your DigiCert Personal ID from Keychain Access
- Import your DigiCert Personal ID into Keychain Access



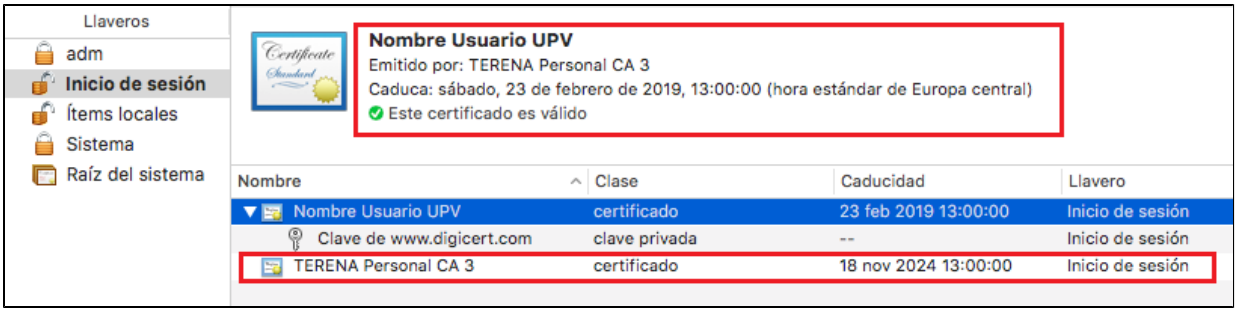
8.- Como comentamos antes, queda pendiente la instalación del certificado de la CA intermedia (TERENA Personal CA 3); accederemos de nuevo a la web https://www.digicert.com/sso/ siguiendo los pasos indicados al principio.

En la página titulada *Request a Certificate*, en la sección *My Certificates* veremos el certificado generado en los pasos antes descritos. Pulsar sobre *Download* (botón); en el directorio de descargas del usuario, se descarga un fichero comprimido (.zip) con el nombre del usuario, cuyo contenido es: *DigiCertCA.crt* (certificado de entidad intermedia TERENA Personal CA 3), *nombre_usuario_upv.crt* (el certificado solicitado), *TrustedRoot.crt* (certificado raíz de la CA DigiCert).





Con un doble clic en el fichero `DigiCertCA.crt`, instalamos el certificado de entidad intermedia *TERENA Personal CA 3*, y el certificado de usuario es reconocido como certificado válido por el sistema:



Nota: No es necesario instalar los otros ficheros (ni el certificado solicitado y ni el certificado raíz de la CA).

9.- Es importante realizar una copia de seguridad del certificado instalado.

Ver también:

¿Cómo envío correos firmados/cifrados?