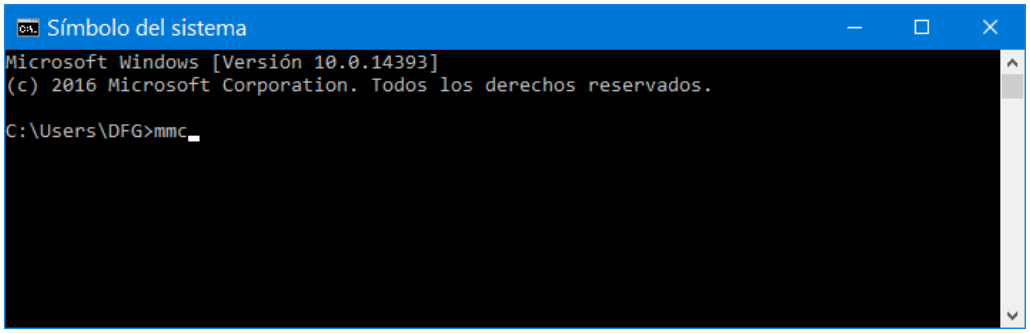
Gestión de Certificados Digitales
Práctica 5A

1. Objetivo

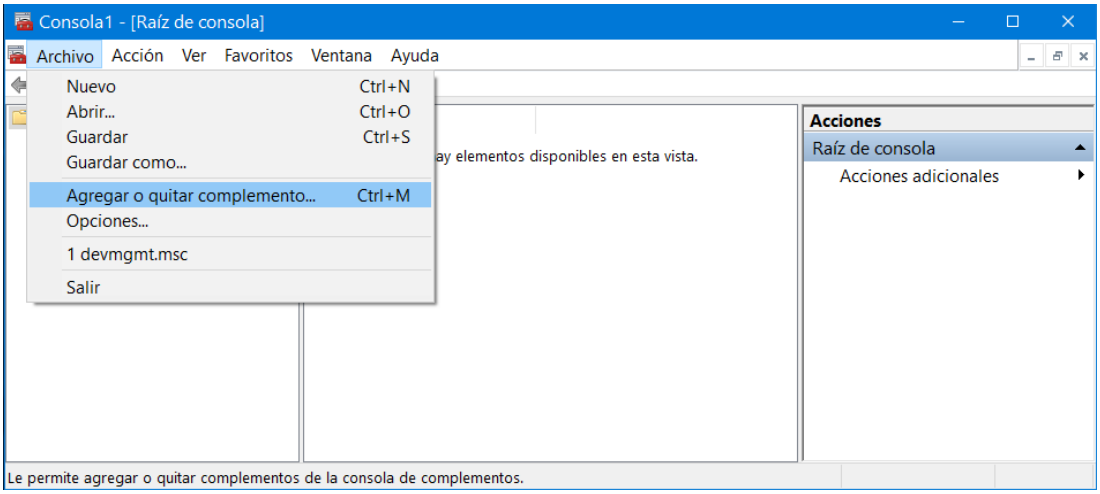
En esta práctica el alumno debe crear certificados que puedan ser instalados tanto en un servidor web como en los computadores en los que se ejecutan navegadores web. Además, cargará los certificados creados en el almacén de certificados de Windows. En una práctica posterior se utilizarán los certificados para que un servidor web y un navegador web puedan comunicarse de forma segura (cifrada) usando el protocolo TLS/SSL.

2. Gestionar los certificados instalados en un computador

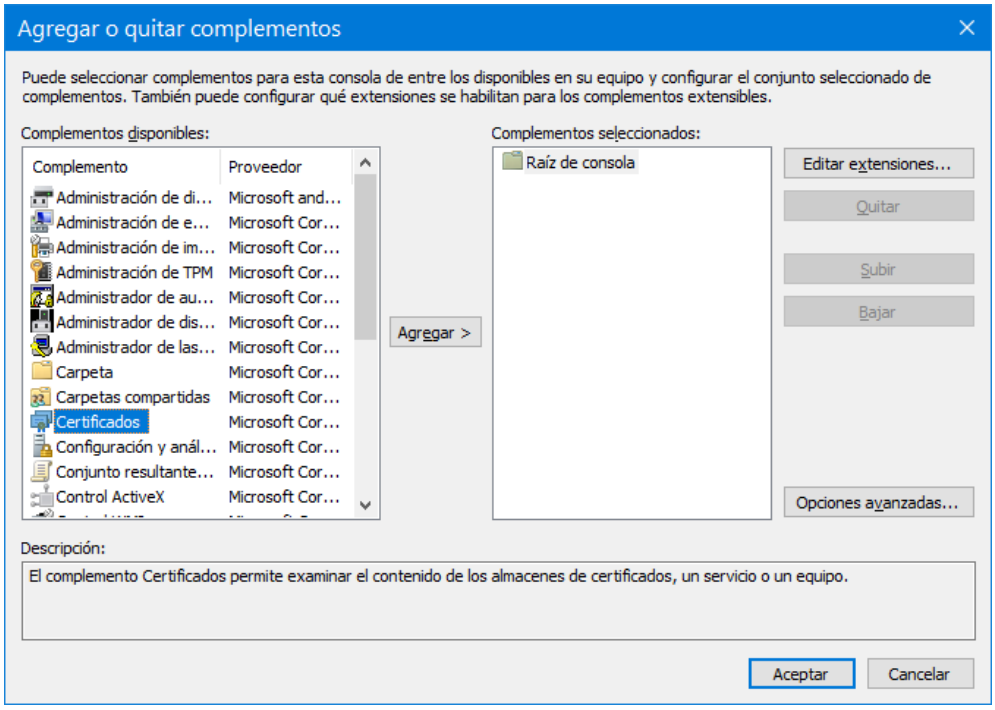
Para trabajar con certificados abrir una Microsoft Management Console. Teclear mmc en una ventana de comandos.



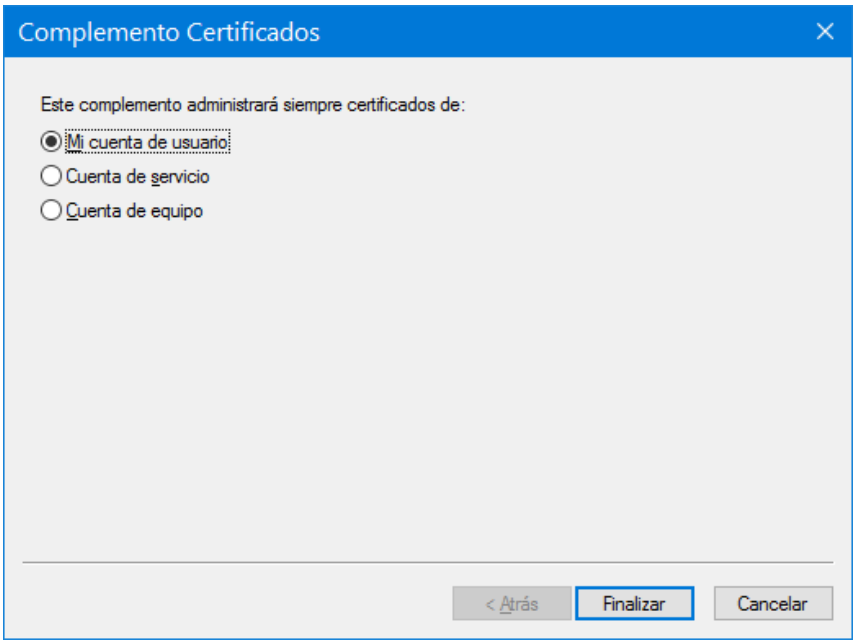
Se abre una ventana de consola y en el menú archivo seleccionar la opción de "Agregar o quitar complemento".



En la ventana de Agregar o quitar complementos seleccionar el complemento "Certificados".

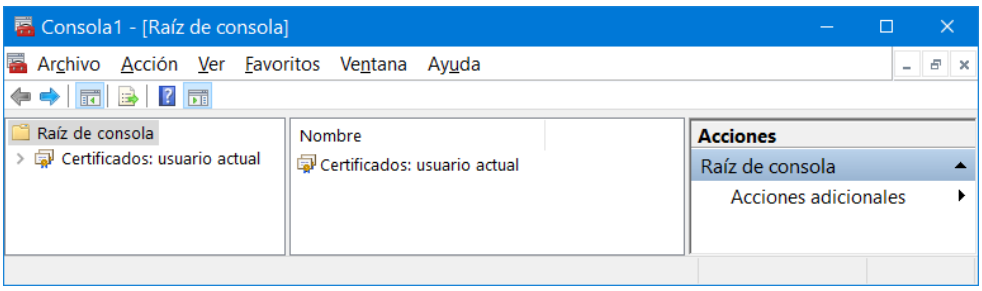


Al pulsar el botón agregar aparece un cuadro de dialogo solicitando el tipo de cuenta cuyos certificados se administrarán con el complemento seleccionado.

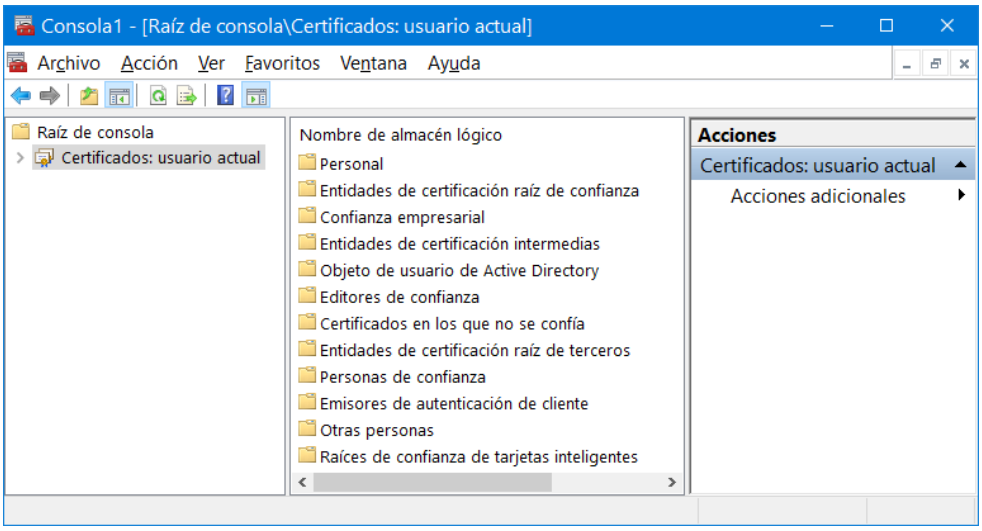


Inicialmente utilizar la cuenta del usuario. Tras pulsar el botón Finalizar en este cuadro y luego el botón Aceptar en la ventana anterior, aparece el nuevo complemento en la consola denominado "Certificados: usuario actual".

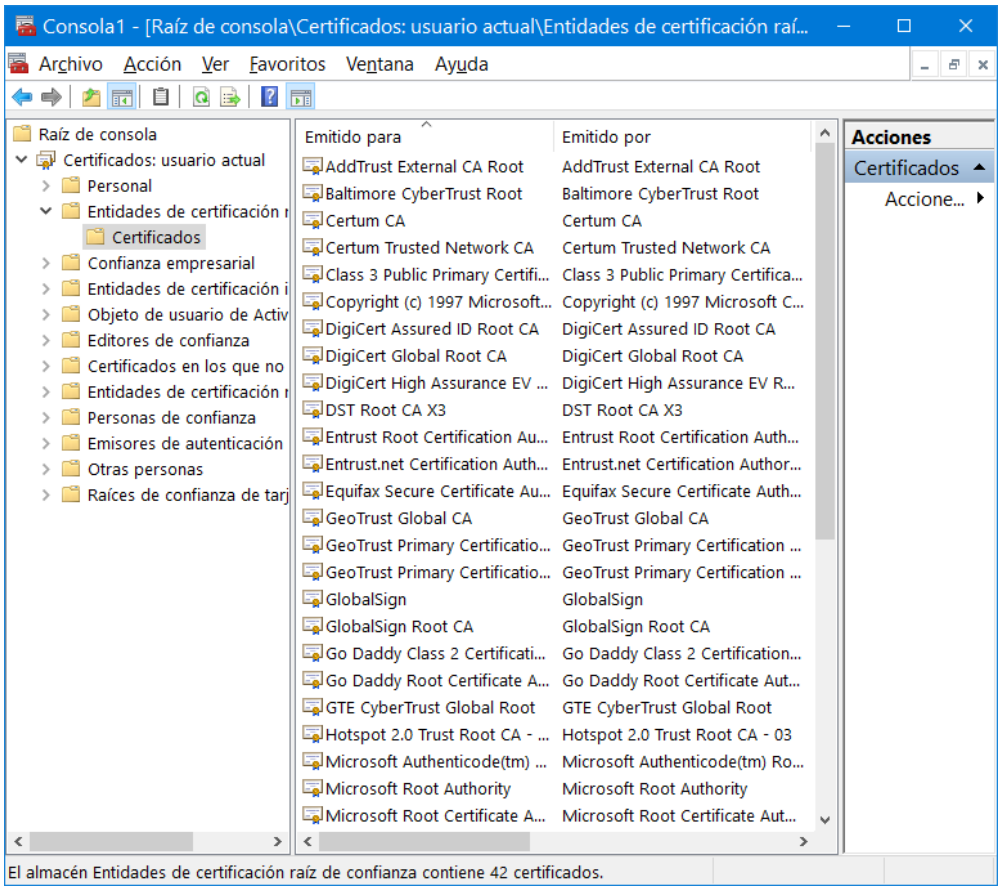
NOTA: la ventana anterior tiene tres opciones porque la ejecuta un administrador del sistema. Generalmente, un usuario sin privilegios de administración solo puede administrar los certificados de su propia cuenta de usuario.



Al pulsar en el nombre "Certificados: usuario actual" se despliegan en la consola los almacenes lógicos para los certificados del usuario.

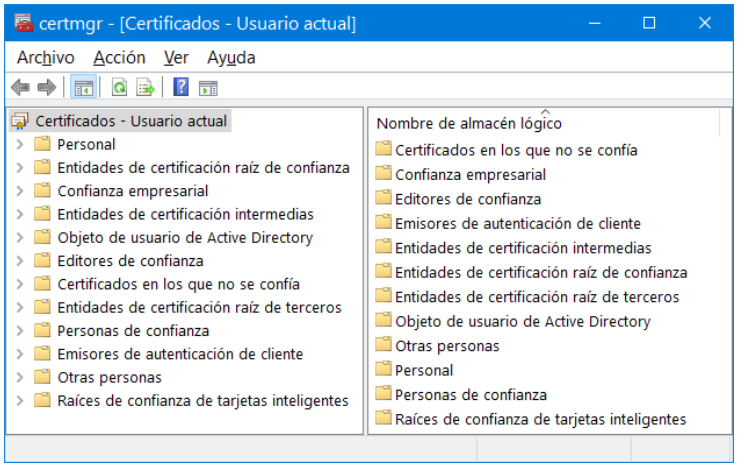


Se puede entrar en cada almacén lógico para ver los certificados que contiene. Por ejemplo dentro de "Entidades de certificación raíz de confianza\Certificados" se puede ver:

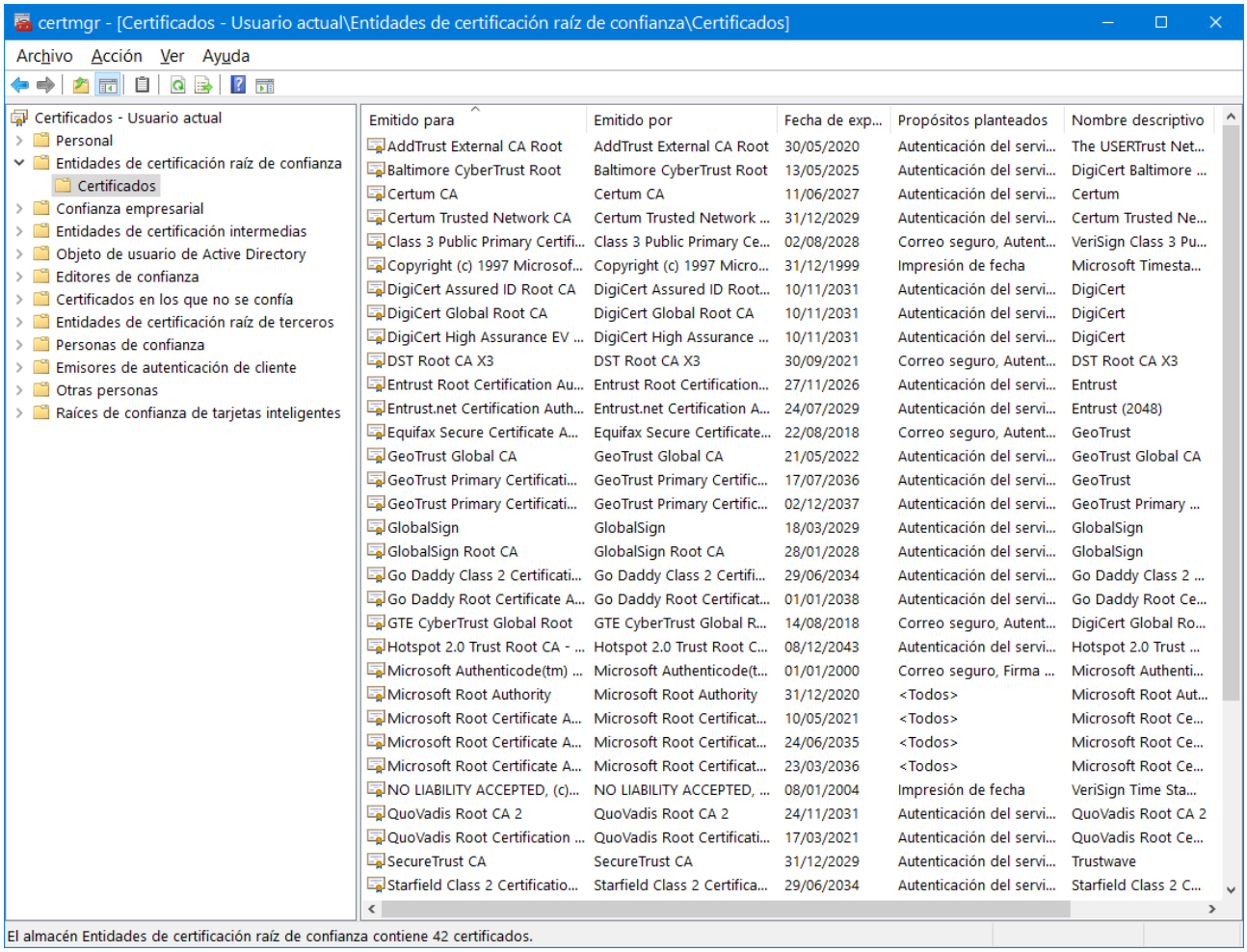


OTRA FORMA MÁS DIRECTA DE ACCEDER A LOS CERTIFICADOS:

Teclear en una consola **certmgr**, o bien en Cortana teclear: **certmgr.msc**. En ambos casos aparece la ventana siguiente:



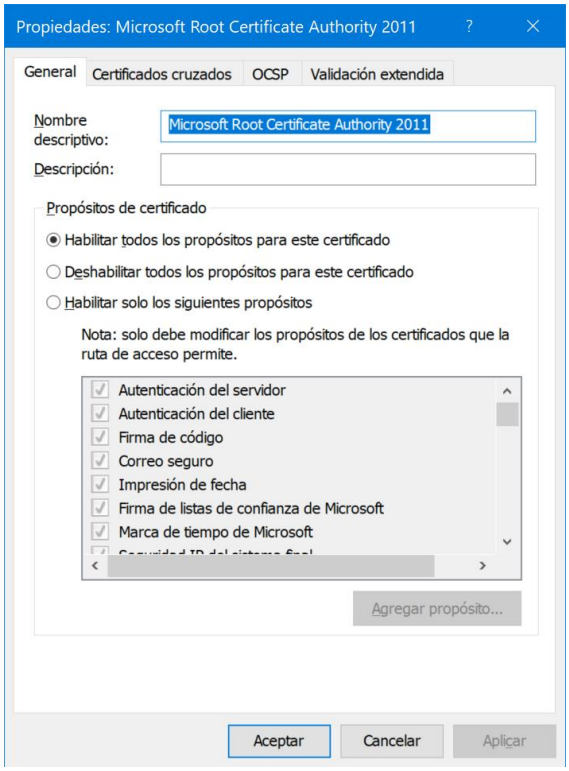
Si desplegamos el árbol de la consola (ventana de la izda) y entramos en Entidades de certificación raíz de confianza > Certificados, vemos los siguientes certificados:



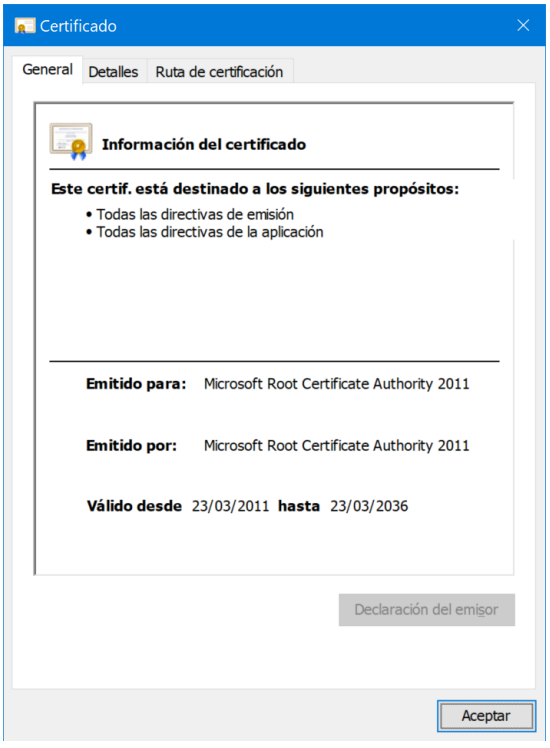
Observar que el cuarto botón por la izquierda está pulsado porque se está mostrando el árbol de la consola. Cuando se selecciona un certificado en el panel derecho, aparecen botones a la derecha que permiten cortar, copiar, eliminar, ver propiedades, y exportar la lista. Estas tareas también se pueden realizar desplegando el menú "Acción".

PROPIEDADES DE UN CERTIFICADO:

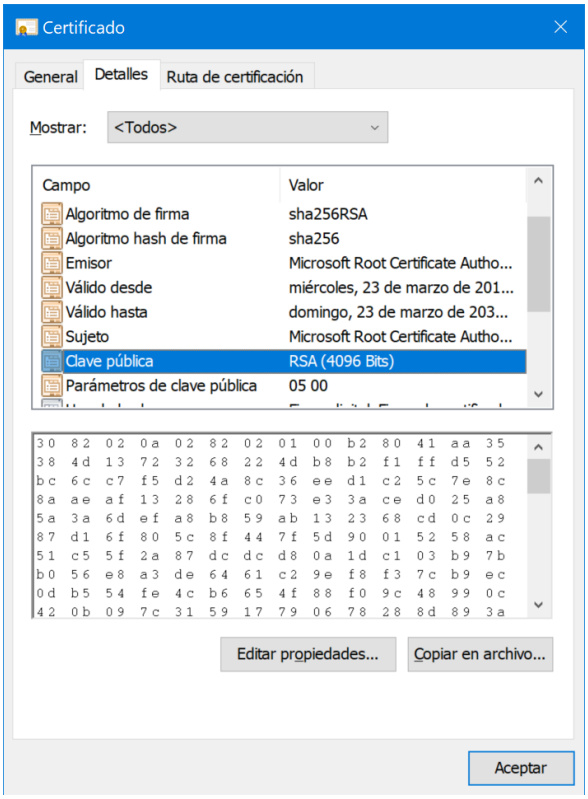
En el menú Acción elegir la opción Propiedades, o pulsar el botón derecho del ratón sobre el certificado seleccionado, o pulsar el botón Propiedades y aparece esta ventana cuando está seleccionado un certificado. Observar que este certificado está habilitado para todos los propósitos. Las otras pestañas tienen sus opciones vacías.



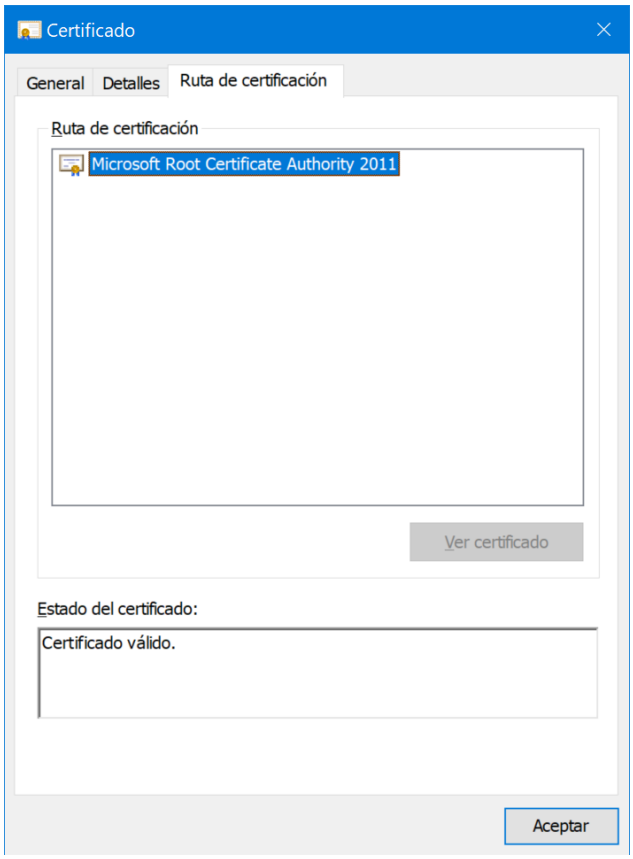
Si elegimos la opción de Abrir el certificado aparece la ventana Certificado que tiene tres pestañas. En la pestaña General se muestra la información general del certificado. Los propósitos del certificado, emitido para, emitido por y su periodo de validez. Observar que como éste es un certificado raíz, entonces "Emitido para == Emitido por".



En la pestaña Detalles se muestra el contenido del certificado. Observar como al seleccionar un campo del certificado se muestra el contenido del campo seleccionado en la ventana inferior. En la figura siguiente se ha seleccionado el campo Clave pública.



En la pestaña Ruta de certificación se muestra la ruta. Observar que en el caso de un certificado raíz no hay ruta alguna.



3. Creación de certificados usando el entorno PowerShell

Hay múltiples formas de crear los certificados necesarios.

1) Utilizando una autoridad de certificación pública a la que se puede acceder vía web. Como ejemplo se puede visitar https://letsencrypt.org/es/.

2) Instalando una autoridad certificadora propia que emita certificados. Un ejemplo es el servicio "Certificate Server" de Windows Server, que permite implementar un Infraestructura de Clave Pública (PKI) corporativa. También se puede emular el funcionamiento de una autoridad certificadora con una herramienta como https://www.openssl.org/ que es de uso común.

3) Usando un sencillo programa que permita crear certificados. Los programas makecert.exe y pvk2pfx.exe están disponibles en un subdirectorio del Sistema Windows o de Visual Studio. En el Campus Virtual están disponibles en sus versiones de 32 y 64 bits. El inconveniente de makecert es que solo puede generar certificados con unas características limitadas.

Por ello se generarán certificados usando PowerShell en la Máquina Virtual de Prácticas.

A partir de los sistemas operativos Windows 10 y Windows Server 2016 el entorno de PowerShell proporciona el comando (cmdlet) New-SelfSignedCertificate que permite crear certificados para comprobar el funcionamiento de sistemas y aplicaciones. Estos certificados solo se deben utilizar para hacer pruebas, no para un uso normal.

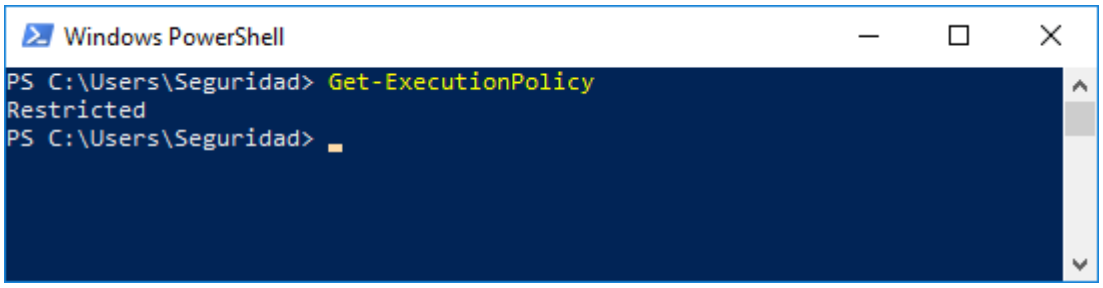
Abrir una consola de PowerShell en un sistema operativo Windows 10. Para ello pulsa el BOTÓN INICIO y al final del menú de aplicaciones mostrado aparece la carpeta de “Windows PowerShell”. En un SO de 64 bits aparece la aplicación “Windows PowerShell” de 64 bits y también la aplicación “Windows PowerShell (x86)” de 32 bits. También aparece “Windows PowerShell (ISE)” que es el “Integrated Scripting Environment”, un entorno de desarrollo de scripts integrado.

La web con toda la documentación de PowerShell (PS) es:

https://docs.microsoft.com/en-us/powershell/

Abre el PowerShell ISE, ya que proporciona ayuda para desarrollar los scripts.

Generalmente, la ejecución de scripts en un sistema estará restringida. Usar el comando Get-ExecutionPolicy para comprobarlo:



Para activar la ejecución usar el comando: Set-ExecutionPolicy –Scope CurrentUser Unrestricted. Si se cierra la sesión de PS y luego se abre una nueva, en la nueva sesión la política de ejecución permanece Unrestricted.

PARA GENERAR UN CERTIFICADO RAÍZ

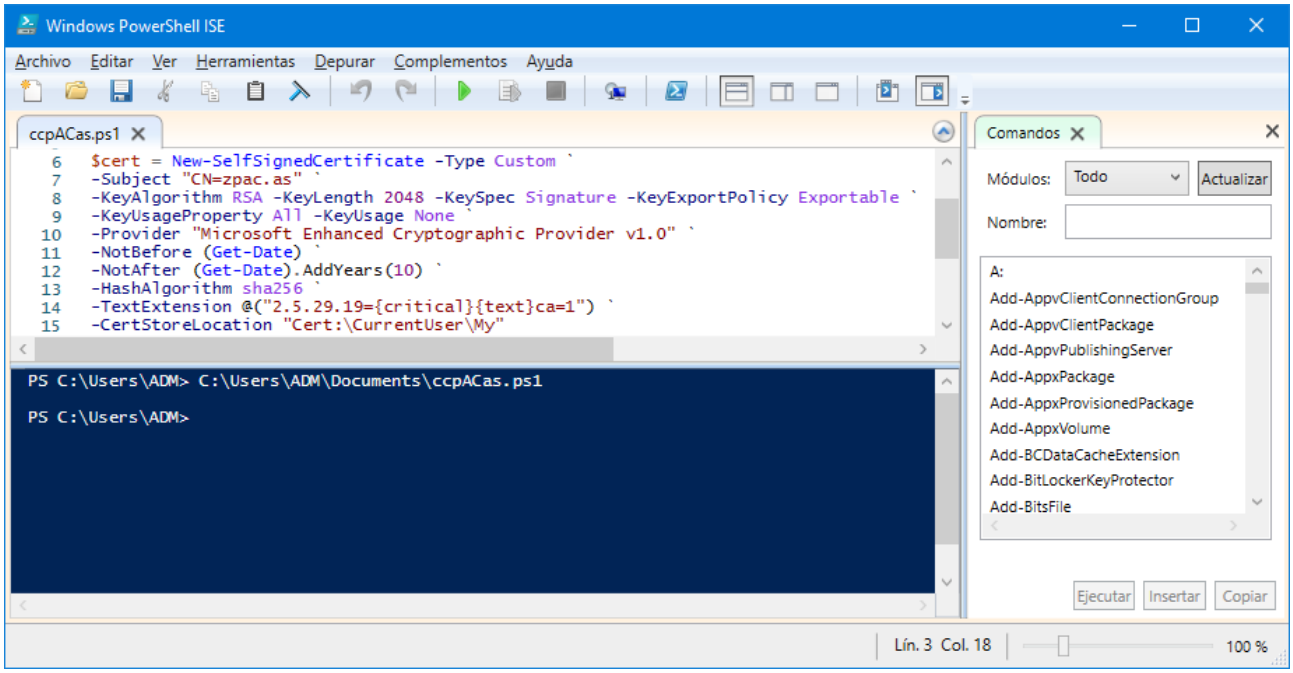
Se puede utilizar el siguiente script:

```
$cert = New-SelfSignedCertificate -Type Custom `
-Subject "CN=zpac.as" `
-KeyAlgorithm RSA -KeyLength 2048 -KeySpec Signature -KeyExportPolicy Exportable `
-KeyUsageProperty All -KeyUsage None `
-Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" `
-NotBefore (Get-Date) `
-NotAfter (Get-Date).AddYears(10) `
-HashAlgorithm sha256 `
-TextExtension @("2.5.29.19={critical}{text}ca=1") `
-CertStoreLocation "Cert:\CurrentUser\My"
```

Este script simplemente utiliza el cmdlet New-SelfSignedCertificate para generar un nuevo certificado autofirmado y su clave privada asociada. El certificado se carga en el almacén de certificados del usuario y su clave asociada en el almacén de claves del usuario. Además, ambos elementos (certificado y su clave) se asignan a la variable $cert, para su posterior uso en la sesión de PowerShell.

Observar que se utiliza el carácter ` (acento invertido) como indicador de continuación de línea. Se puede insertar en el texto con Alt+96 (poner 96 en el teclado numérico).

La imagen siguiente muestra la edición del script en el ISE y su ejecución:



Esta figura muestra la edición del script ccpACas.ps1 (crea certificado powershell Autoridad Certificadora). Guarda el script en el fichero. Observar los parámetros del comando:

-Type: Especifica el tipo de certificado creado. Aquí se utiliza el tipo Custom. Otros tipos son CodeSigningCert, DocumentEncryptionCert y SSLServerAuthentication (defecto).

-KeyAlgorithm: Especifica el algoritmo para el que se crean las claves asimétricas asociadas al certificado. Los valores posibles son RSA y ECDSA.

-KeyLength: Especifica la longitud en bits de la clave que es asociada con el nuevo certificado. No existe un valor por defecto.

-KeySpec: Especifica si la clave privada asociada con el nuevo certificado se puede usar para firmar, cifrar o ambas cosas. Los valores aceptables son KeyExchange, Signature y None (defecto). El valor None indica que se usa el valor por defecto que utiliza el proveedor de servicios criptográficos.

-KeyExportPolicy: Especifica la política que gobierna la exportación de la clave privada asociada con el certificado. Los valores aceptables son: Exportable, ExportableEncrypted (defecto) y NonExportable.

-keyUsageProperty: Especifica los usos de la clave para la propiedad "Usos de clave" de la clave privada. Los valores aceptables para este parámetro son: All, Decrypt, KeyAgreement, None (defecto) y Sign. El valor None indica que el comando usa el valor por defecto que utilice el proveedor de servicios de claves.

-KeyUsage: Especifica los usos de clave establecidos en la extensión de uso de clave del certificado. Los valores aceptables para este parámetro son: CertSign, CRLSign, DataEncipherment, DecipherOnly, DigitalSignature, EncipherOnly, KeyAgreement, KeyEncipherment, None (defecto) y NonRepudiation. El valor predeterminado, None, indica que este cmdlet no incluye la extensión KeyUsage en el nuevo certificado. El uso de la clave se restringe a los valores especificados en este parámetro. Por ello es mejor no restringir el uso indicando None.

-Provider: Especifica el nombre del proveedor de servicios criptográficos (CSP) o del proveedor de almacenamiento de claves (KSP). Consultar la ayuda para determinar los proveedores disponibles. Si no se indica nada se determina un proveedor en función del parámetro –KeySpec. Por defecto: "Microsoft Base Cryptographic Provider v1.0". Es **esencial** usar "Microsoft Enhanced RSA and AES Cryptographic Provider" para evitar limitaciones en el uso de las claves privadas.

-NotBefore: Indica la fecha de inicio del período de validez del certificado.

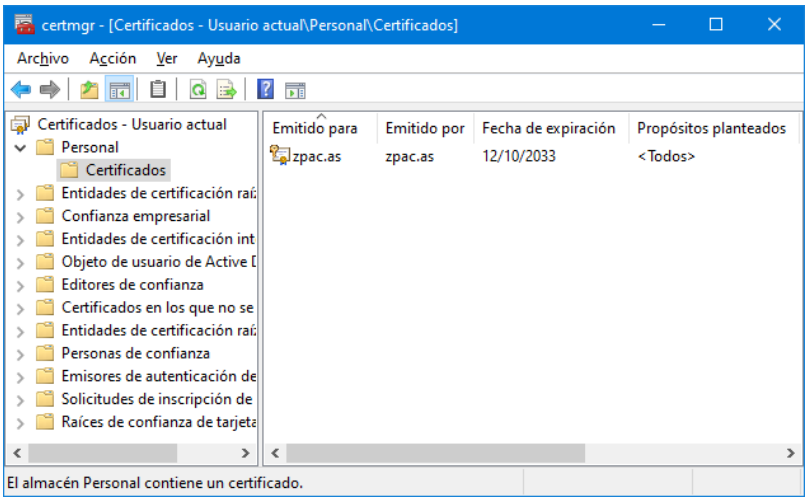
-NotAfter: Indica la fecha de finalización del período de validez del certificado.

-HashAlgorithm: Especifica el nombre del algoritmo de hash usado en la firma del nuevo certificado. El algoritmo por defecto depende del proveedor que almacena la clave privada usada para firmar el nuevo certificado.

-TextExtension: En este caso se utiliza para indicar que el certificado es de una Autoridad Certificadora. Es necesario para que el navegador Firefox permita cargarlo en el almacén de raíces de confianza.

-CertStoreLocation: Especifica el almacén en que se almacena el nuevo certificado. Solo se puede especificar dos almacenes de certificados: Cert:\CurrentUser\My o Cert:\LocalMachine\My. NO se pueden usar otros almacenes de certificados.

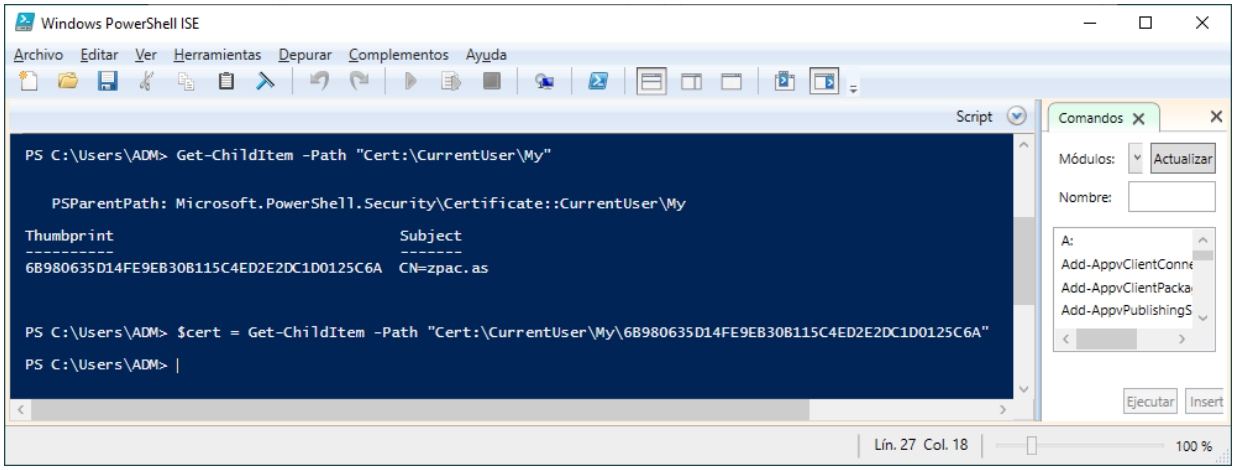
Utiliza la herramienta certmgr.msc para comprobar que el certificado emitido para zpAC está en el almacén de certificados "Personal".



Este almacén NO es el apropiado para contener el certificado de una autoridad certificadora. Pero recordar que este certificado y su clave asociada se usarán para crear otros certificados, y no como raíz de confianza en el computador.

PARA GENERAR UN CERTIFICADO DE SERVIDOR

Si se cerró la sesión de PowerShell en la que se generó el certificado de la Autoridad Certificadora y se cargó el certificado en la variable $cert, hay que ejecutar el par de comandos siguientes:

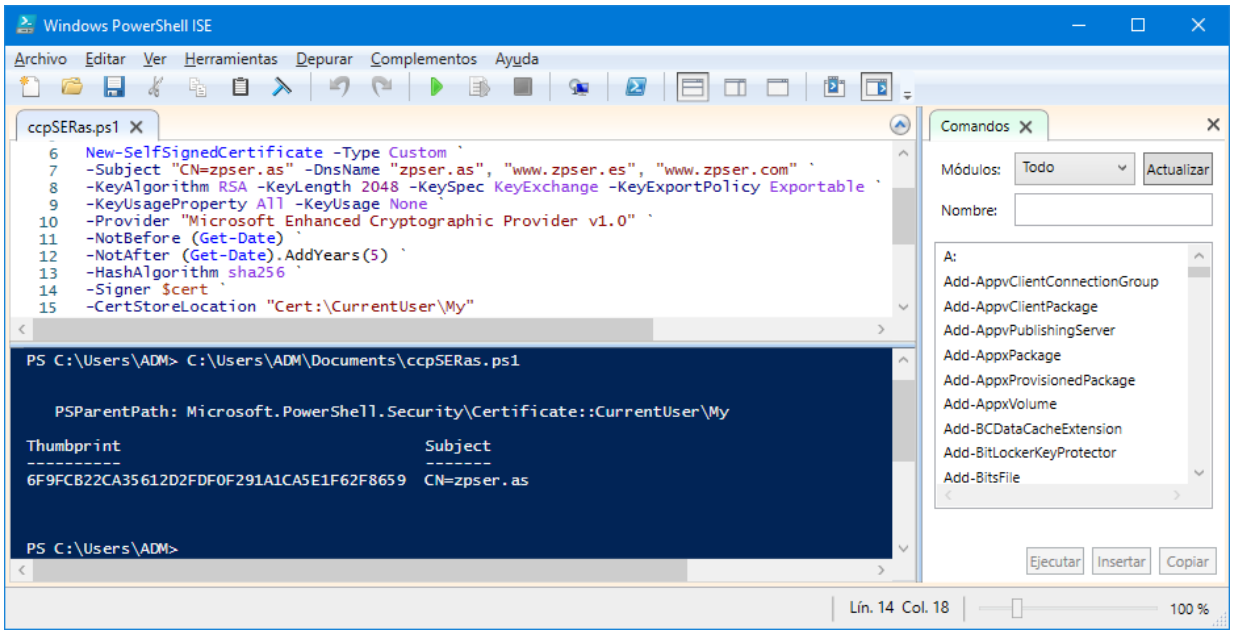


El primer comando permite ver la huella digital (Thumbprint) de los certificados. Hay que copiar la huella del certificado de zpac.as en el segundo comando para cargar la información del certificado en la variable $cert.

Ahora se puede generar un certificado para un servidor con el siguiente script:

```
New-SelfSignedCertificate -Type Custom `
-Subject "CN=zpser.as" -DnsName "zpser.as", "www.zpser.es", "www.zpser.com" `
-KeyAlgorithm RSA -KeyLength 2048 -KeySpec KeyExchange -KeyExportPolicy Exportable `
-KeyUsageProperty All -KeyUsage None `
-Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" `
-NotBefore (Get-Date) `
-NotAfter (Get-Date).AddYears(5) `
-HashAlgorithm sha256 `
-Signer $cert `
-CertStoreLocation "Cert:\CurrentUser\My"
```

Tras ejecutar este script, el ISE indica la generación del nuevo certificado:



Observar los nuevos parámetros de este script.

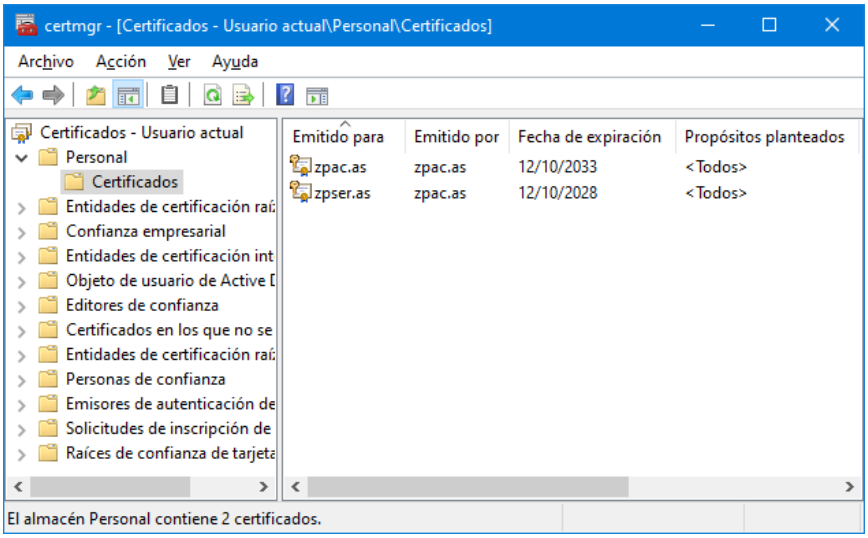
-DnsName: Especifica uno o más nombres DNS para colocar en la extensión "nombre alternativo del sujeto". Si no se especifica el parámetro -Subject, el primer nombre utilizado en el parámetro DnsName se asigna también como nombre el sujeto del certificado. Tras la ejecución del script, se puede comprobar con certmgr que la extensión "Nombre alternativo del titular" tiene los valores "Nombre DNS=zpser.as" "Nombre DNS=www.zpser.es" y "Nombre DNS=www.zpser.com".

-Signer: Especifica un objeto de tipo certificado y el cmdlet utiliza su clave privada asociada para firmar el nuevo certificado. El certificado indicado debe estar en el almacén de certificados personales y debe haber acceso de lectura a la clave privada del certificado.

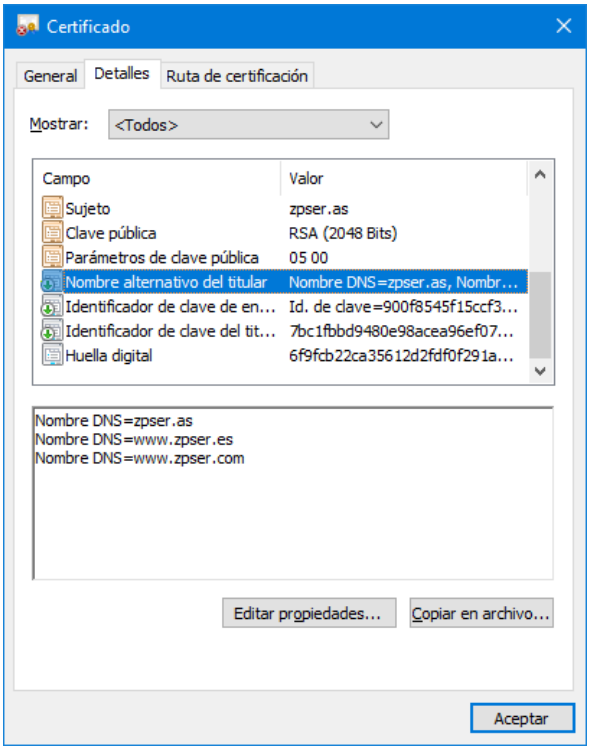
-TextExtensions: NO SE HA UTILIZADO

En el script anterior se podría haber utilizado oid=2.5.29.37 que representa "*Enhanced Key Usage*" y Cadena=1.3.6.1.5.5.7.3.1 que representa "*Server Authentication*". Esto permite restringir el uso del certificado al de autenticación de un servidor. Pero si nuestros programas no comprueban las extensiones no es útil incluirlas.

Utiliza la herramienta certmgr.msc para comprobar que el certificado emitido para zpser.as está en el almacén de certificados "Personal", además del certificado de la autoridad certificadora que lo ha emitido.

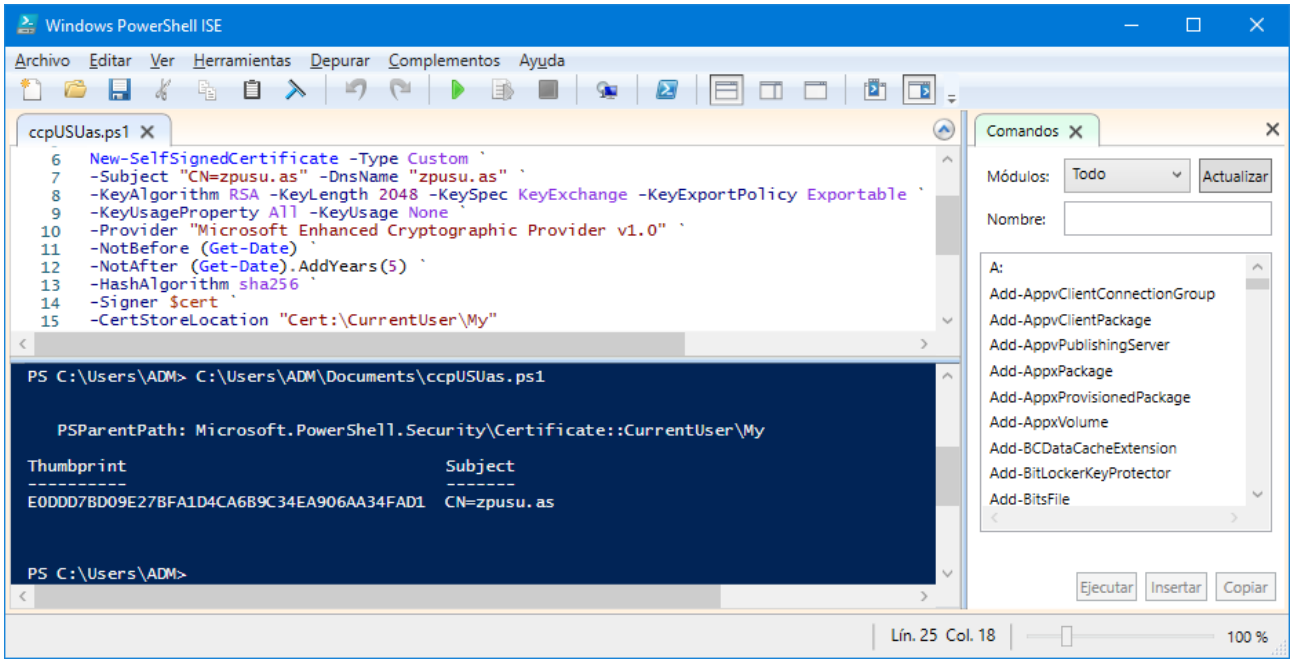


Haz doble-clic en el certificado zpser.as y en ventana Certificado selecciona la pestaña Detalles, y después selecciona el Campo "Nombre alternativo del titular". La imagen siguiente muestra el efecto del parámetro –DnsName al generar el certificado.



PARA GENERAR UN CERTIFICADO DE USUARIO

Repite los pasos realizados para generar un certificado de servidor. A continuación se muestran los parámetros utilizados con New-SelfSignedCertificate y el resultado de la ejecución.



Con la herramienta certmgr.msc podrás comprobar que el certificado emitido para zpusu.as está en el almacén de certificados "Personal".

4. Exportación de los certificados

En la exportación hay que considerar dos posibilidades:

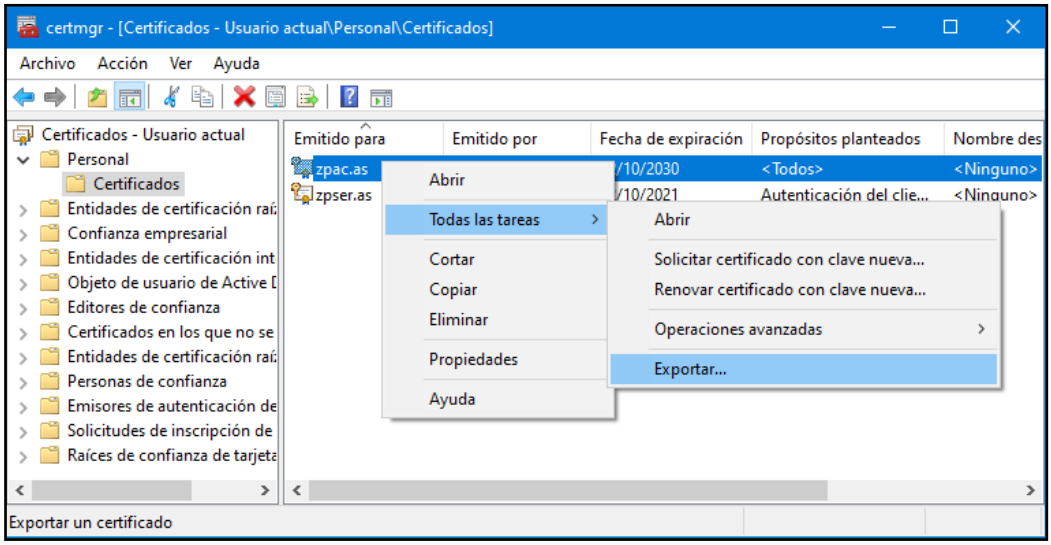
1.-Exportar solamente el certificado

2.-Exportar el certificado conjuntamente con su clave privada asociada.

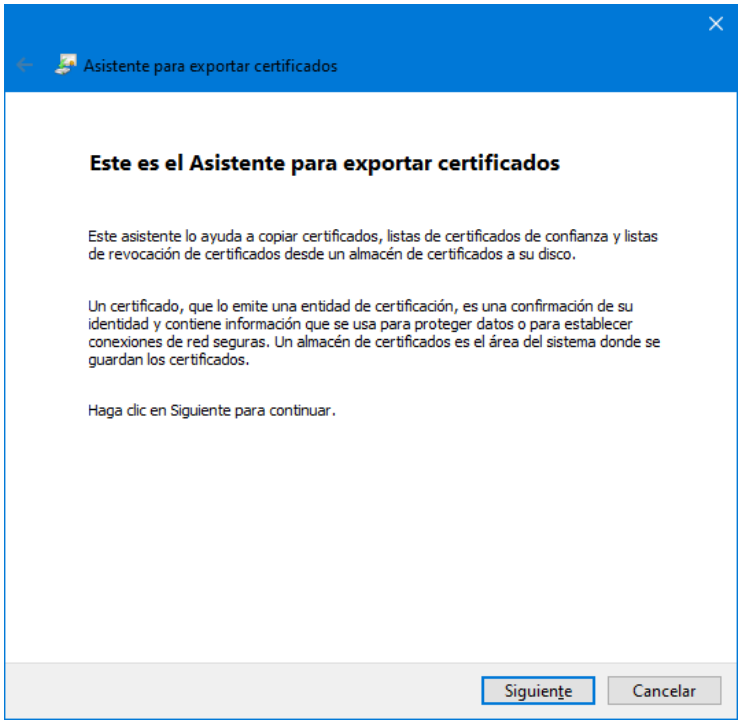
En esta práctica se considerarán las dos.

EXPORTACIÓN PARA LA AUTORIDAD CERTIFICADORA

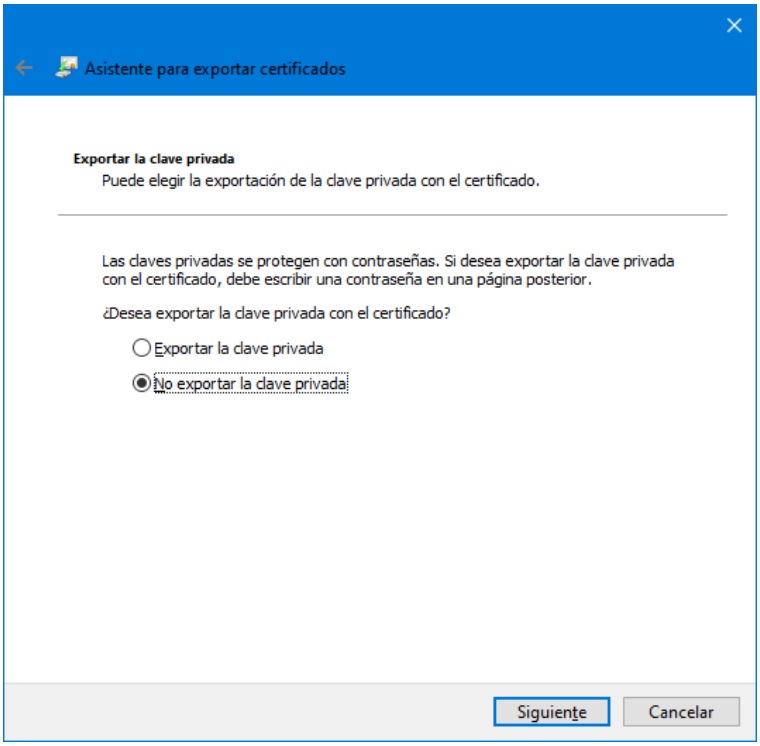
Utilizar la herramienta certmgr.msc para mostrar los certificados del almacén Personal y seleccionar el certificado de la autoridad certificadora zpac.as. Hacer clic-derecho para que se muestre la opción Exportar…



Entonces se abre al asistente para exportar certificados:

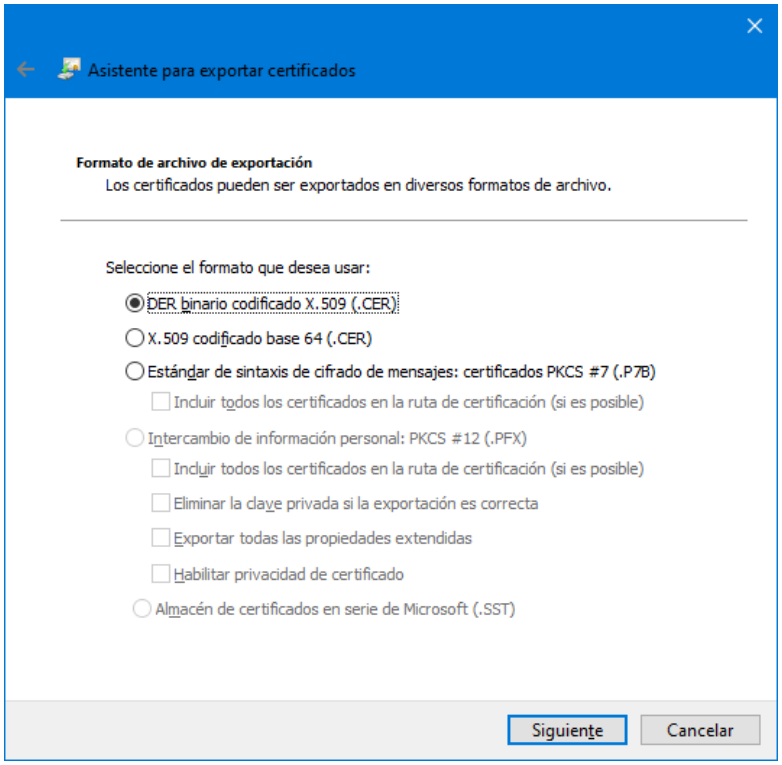


La primera opción a seleccionar es si desea exportar la clave privada con el certificado.



EXPORTAR CERTIFICADO **SIN** LA CLAVE PRIVADA

Selecciona NO exportar la clave privada. Entonces el asistente permite seleccionar 3 formatos para el certificado a exportar: DER, Base 64 y PCKS#7.



Utiliza el formato más común, que es el **formato DER**. Para dejar claro el formato en el que se ha exportado el certificado, se puede reflejar en el nombre del fichero. Por ejemplo: zpACas-DER.cer.

Ahora vuelve a exportar el certificado en **formato Base 64**. Por ejemplo usa el nombre de fichero zpACas-B64.cer para diferenciar esta exportación de la anterior. Comprueba que puedes abrir y ver este fichero con el block de notas, pero no puedes con el fichero exportado en formato DER.

Finalmente exporta el certificado en **formato PKCS#7**. Por ejemplo usa el nombre de fichero zpACas-PKCS7.p7b con la extensión estándar para este tipo de formato.

Comprueba que si haces doble clic sobre este fichero se abre automáticamente una nueva instancia de la aplicación certmgr.msc para visualizar el contenido del fichero. Pero si haces doble clic en los otros dos formatos se abre la ventana Certificado, que incluye un botón para la instalación del certificado en el almacén de certificados del sistema.

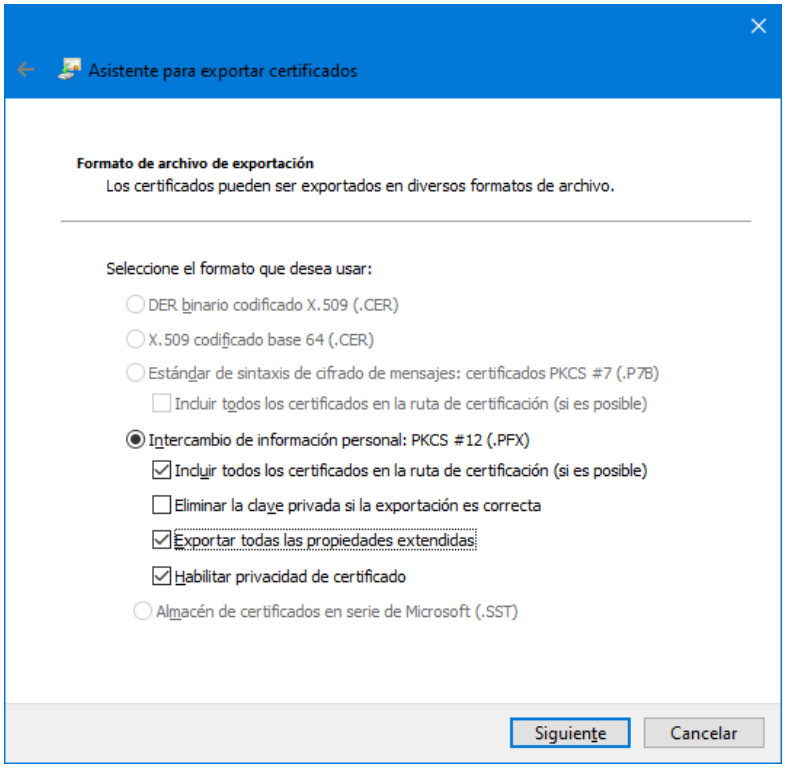
El formato PKCS#7 puede ser útil cuando hay que almacenar una cadena de certificados, pero en el caso de una autoridad certificadora, solo se almacena un fichero, por lo que no es útil.

Quédate con el certificado en formato DER que puedes renombrar por simplicidad a zpACas.cer.

EXPORTAR CERTIFICADO **CON** LA CLAVE PRIVADA

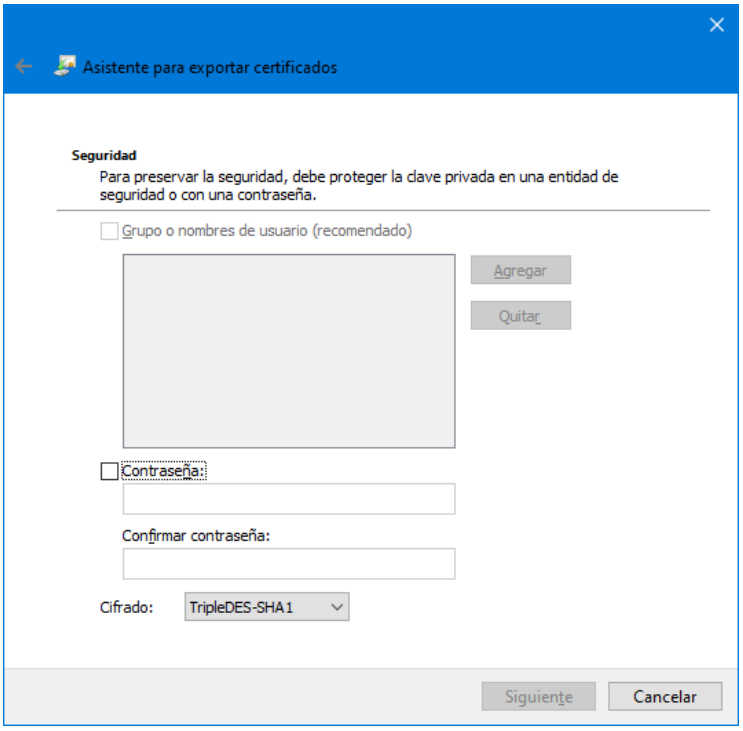
Una Autoridad Certificadora **solo** debe exportar la clave privada para disponer de un backup. El objetivo de esta exportación es obtener un fichero que contenga el certificado y su clave privada asociada. El formato utilizado es el PKCS#12.

Al seleccionar el formato PKCS#12, el asistente para exportar certificados permite varias opciones, y algunas de ellas ya están seleccionadas.



Se recomienda seleccionar TODAS las opciones, EXCEPTO Eliminar la clave privada si la exportación es correcta.

A continuación, para proteger la clave privada, el asistente va a cifrar el contenido del fichero con una clave simétrica que se derivará de una contraseña y realizar un resumen para poder comprobar posteriormente la integridad del fichero. El asistente muestra la ventana siguiente:



Como contraseña se recomienda proporcionar **conacpfx** (contraseña de la ac para el pfx).

Usando las contraseñas indicadas en el guion de esta práctica siempre existe la posibilidad de recordarlas consultando nuevamente el guion de la práctica.

Observar que para el cifrado se selecciona por defecto TripleDES-SHA1, pero se puede elegir también AES256-SHA256. Aunque la segunda opción sería la correcta, a veces da algún problema de compatibilidad. Por ello elige la primera.

Como nombre, para el fichero con ambas claves se recomienda usar zpACas.pfx.

EXPORTACIÓN PARA EL SERVIDOR

Realiza los mismos pasos que para la autoridad certificadora.

Exporta el certificado SIN clave privada solamente en formato DER binario. El fichero se puede denominar zpSERas.cer.

Exporta el certificado CON clave privada, usando como contraseña **conserpfx** (contraseña del servidor para el pfx). El fichero se puede denominar zpSERas.pfx.

EXPORTACIÓN PARA EL USUARIO

Realiza los mismos pasos que para la autoridad certificadora.

Exporta el certificado SIN clave privada solamente en formato DER binario. El fichero se puede denominar zpUSUas.cer.

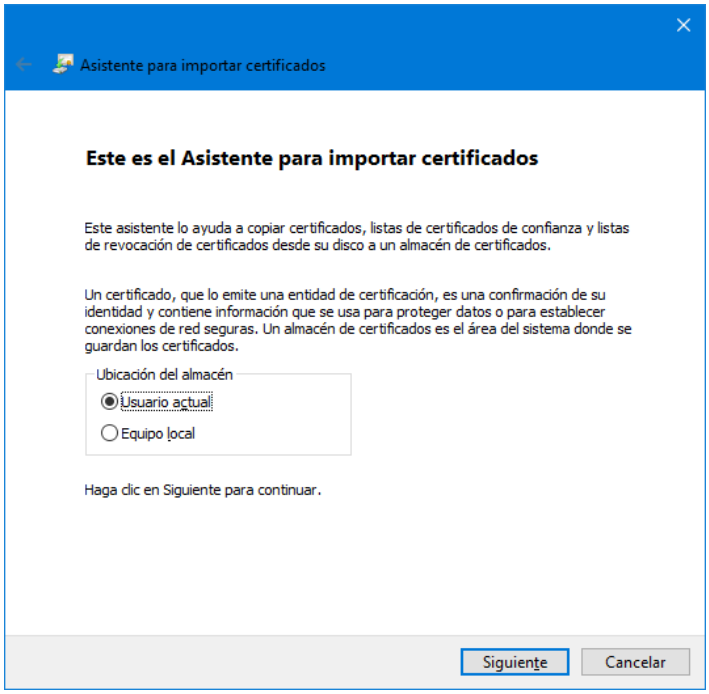
Exporta el certificado CON clave privada, usando como contraseña **conusupfx** (contraseña del usuario para el pfx). El fichero se puede denominar zpUSUas.pfx.

5. Cargar los certificados en el Almacén de Certificados de Windows

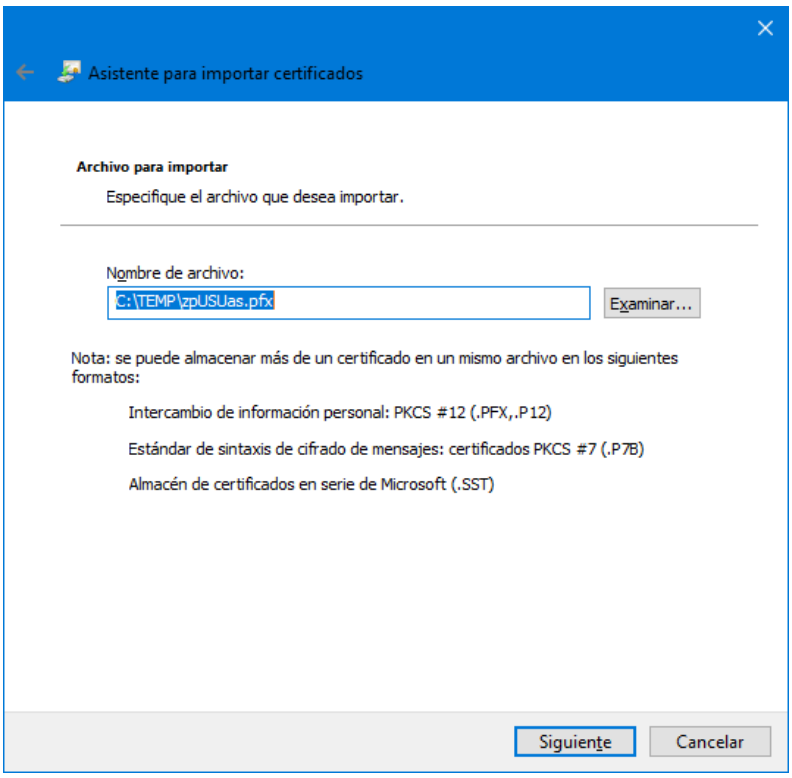
La carga de certificados debes hacerla en la máquina física. Copia los ficheros zpACas.cer y zpUSUas.pfx de la máquina virtual a la máquina física, por ejemplo al directorio C:\TEMP\.

Para cargar los certificados en el almacén de certificados de Windows, en primer lugar hay que elegir si se desea cargar un certificado "clásico" (.cer) que contiene solamente la clave pública del sujeto o bien uno "completo" (.pfx) que contiene las claves pública y privada del sujeto.

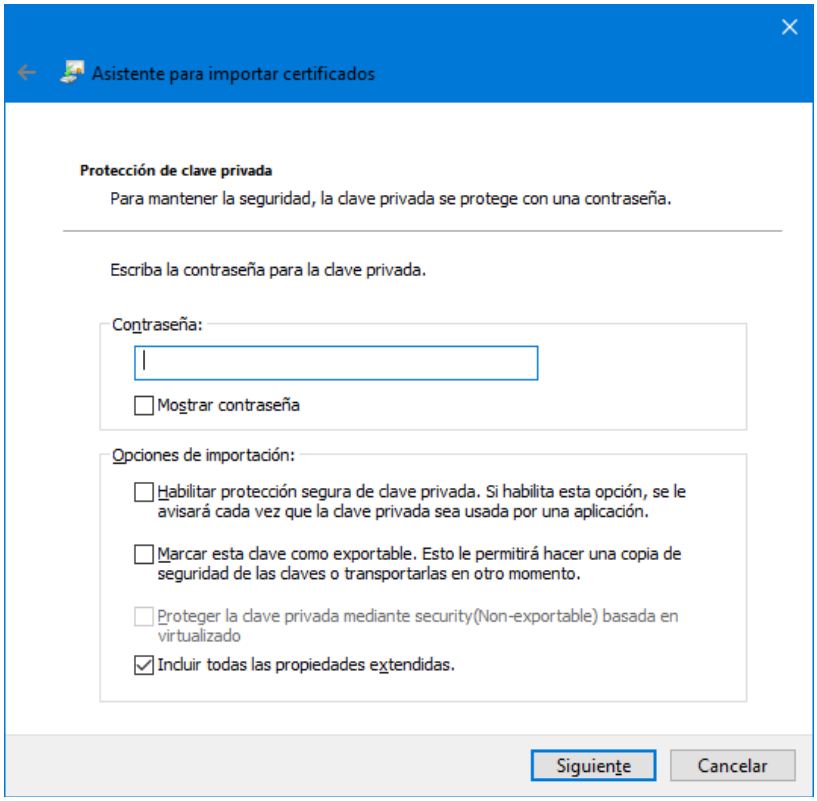
Para cargar el certificado del usuario y su clave privada asociada, hacer doble clic con el ratón sobre el fichero zpUSUas.pfx, y aparece el asistente para la importación de certificados.



Seleccionar Usuario actual. Un administrador de un computador también puede instalar el certificado como de Equipo local. El Asistente pide confirmación del fichero a importar.

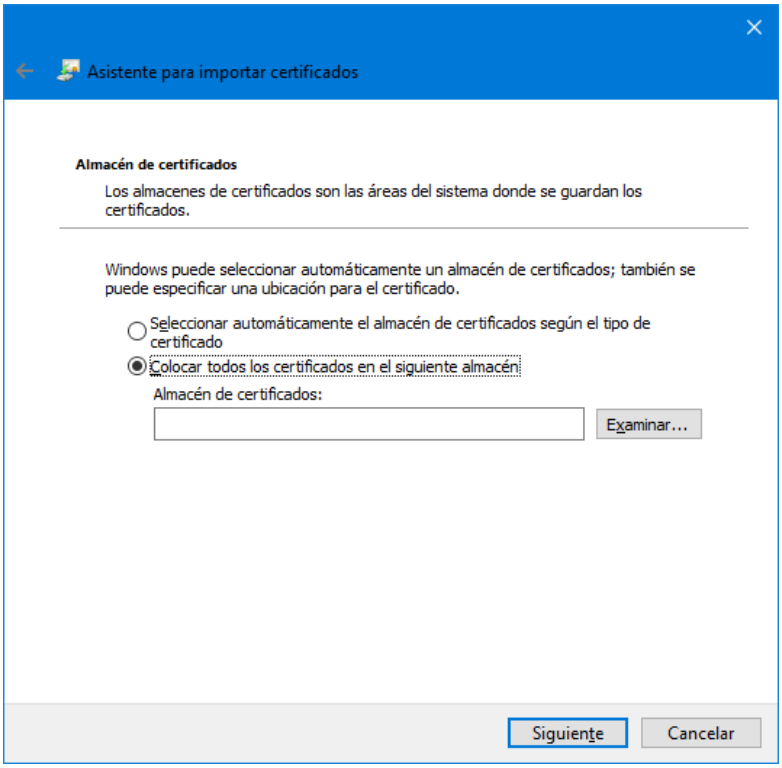


Como el fichero zpUSUas.pfx contiene una clave privada protegida el asistente solicita la contraseña utilizada para protegerla.

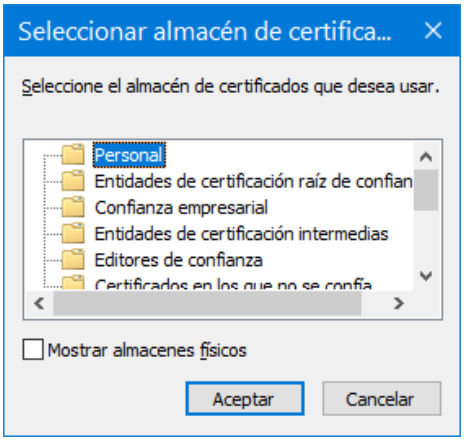


Si se han seguido las indicaciones de la práctica la contraseña será **conusupfx**. No habilites la protección segura de clave privada, marca la clave privada como exportable e incluye las propiedades extendidas del certificado.

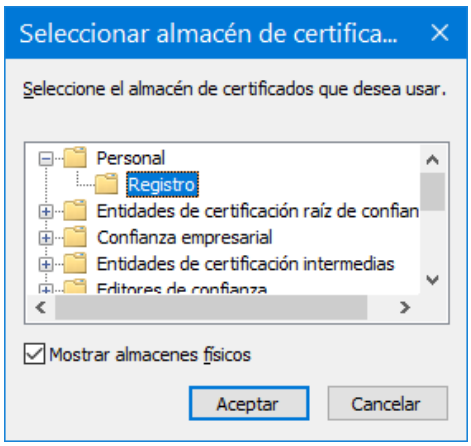
Ahora hay que elegir el almacén de certificados en el que se desea realizar la importación. Se puede permitir que el asistente seleccione automáticamente el almacén o bien elegirlo. Utilizar esta segunda opción como muestra la pantalla siguiente:



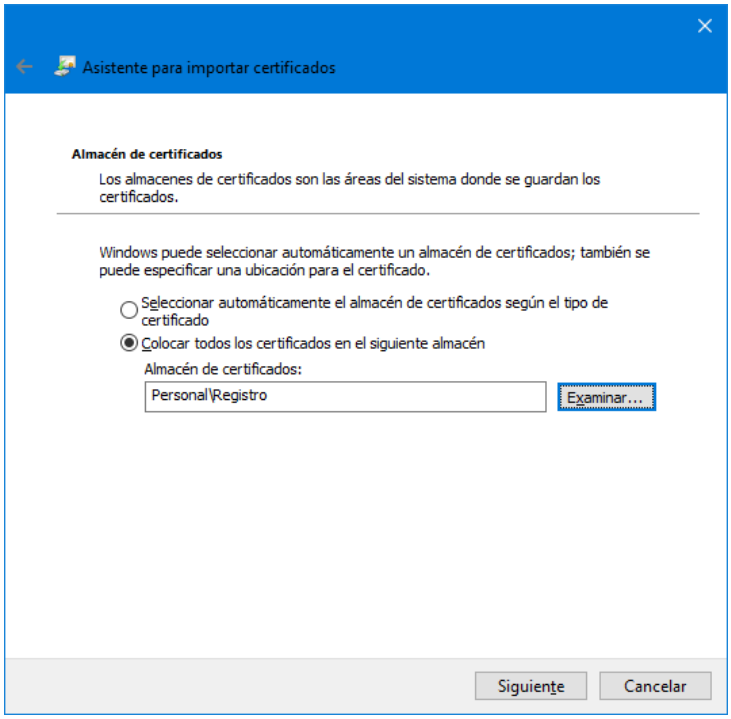
Al pulsar el botón Examinar... aparece la ventana "Seleccionar almacén de certificados".



Selecciona la opción Mostrar los almacenes físicos, despliega los almacenes físicos del almacén Personal, y selecciona el único almacén físico disponible, tal como se muestra en la figura siguiente:

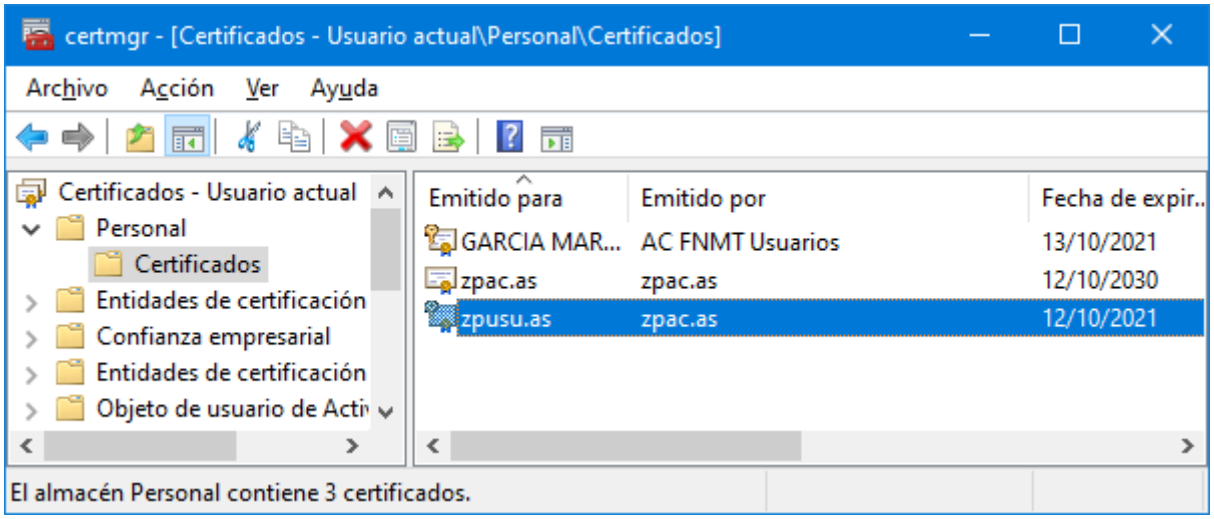


Al pulsar el botón Aceptar, el asistente de importación muestra la siguiente información:



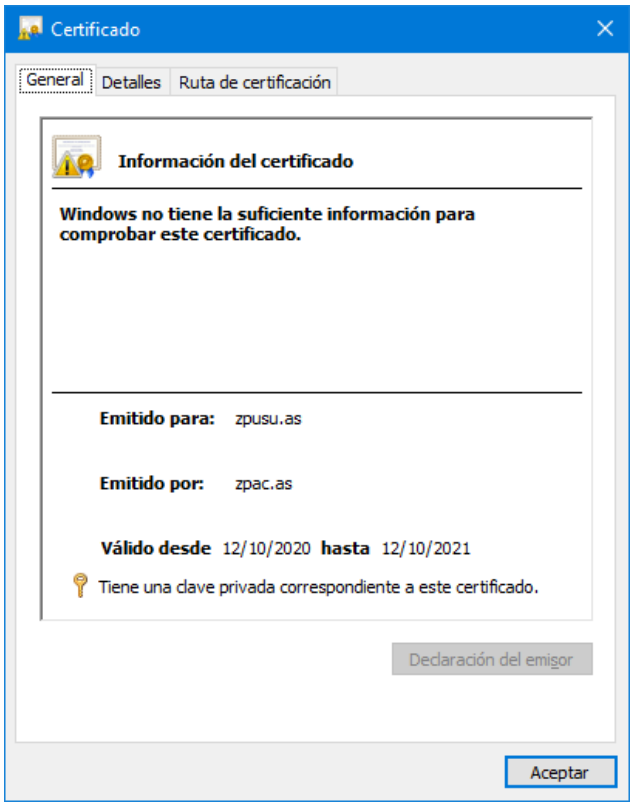
Pulsar el botón Siguiente y finalizar el proceso de importación.

Comprobar con la herramienta certmgr que el certificado ha sido importado con éxito.



Observa que el proceso de carga también ha cargado el certificado de la autoridad certificadora de zpusu.as en el almacén de certificados personales. Esto no es correcto. Elimina el certificado zpac.as.

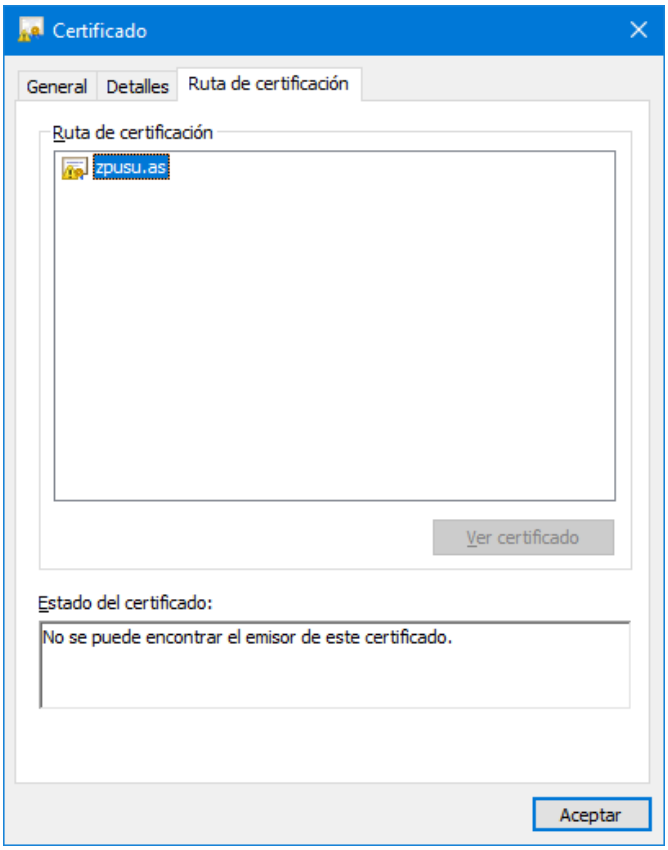
Para ver las propiedades del certificado haz doble clic sobre el certificado y aparece la ventana siguiente, que muestra la pestaña "General" con información del certificado.



Observa el mensaje que aparece en la parte inferior del cuadro de información. Se informa que hay una clave privada correspondiente al certificado.

Observa también el mensaje que hay en la parte superior del cuadro informativo, que indica que Windows no tiene la suficiente información para comprobar el certificado. El problema está relacionado con la cadena de certificados necesaria para validar el certificado de zpusu.as. Se analiza a continuación.

Comprobar la ruta de certificación y el estado de este certificado, seleccionando la pestaña “Ruta de certificación”:



Observar que no hay ruta disponible, y en relación al estado, el gestor de certificados no puede encontrar al emisor del certificado.

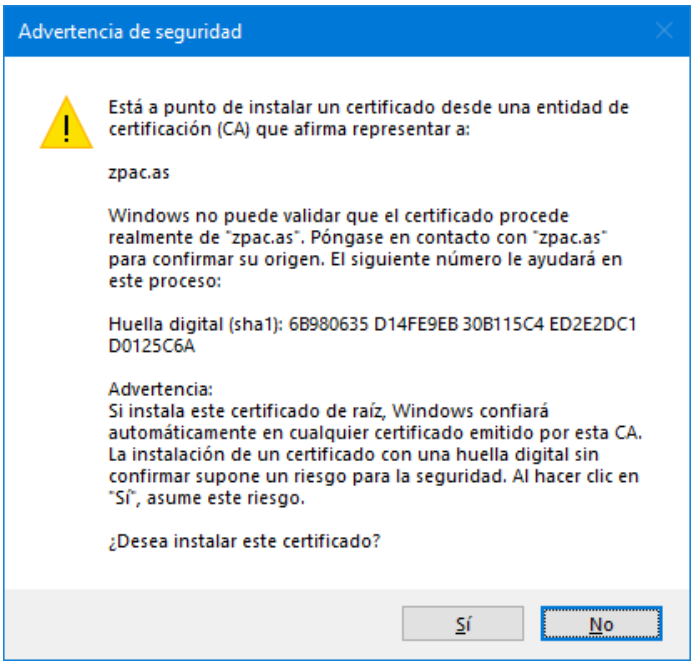
Cargar el certificado de la autoridad certificadora zpACas.cer, emisora del certificado de zpusu.as, en el almacén denominado "Entidades de certificación raíz de confianza". Para ello hacer doble clic sobre el fichero zpACas.cer y se abre la ventana siguiente:

Observar que en la parte inferior del cuadro informativo no se indica que hay una clave privada asociada al certificado, lo cual es correcto, pues estamos usando un fichero .cer.

Pulsar el botón Instalar certificado…

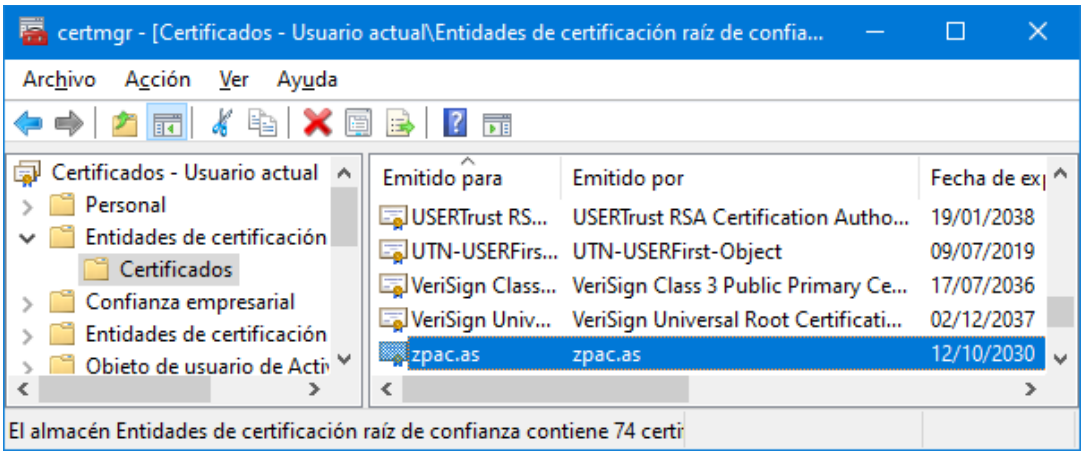
En el Asistente para importar certificados, seleccionar Usuario actual y el almacén "Entidades de certificación raíz de confianza". No elegir el almacén físico, dejando que elija el asistente.

El asistente muestra la ventana siguiente:



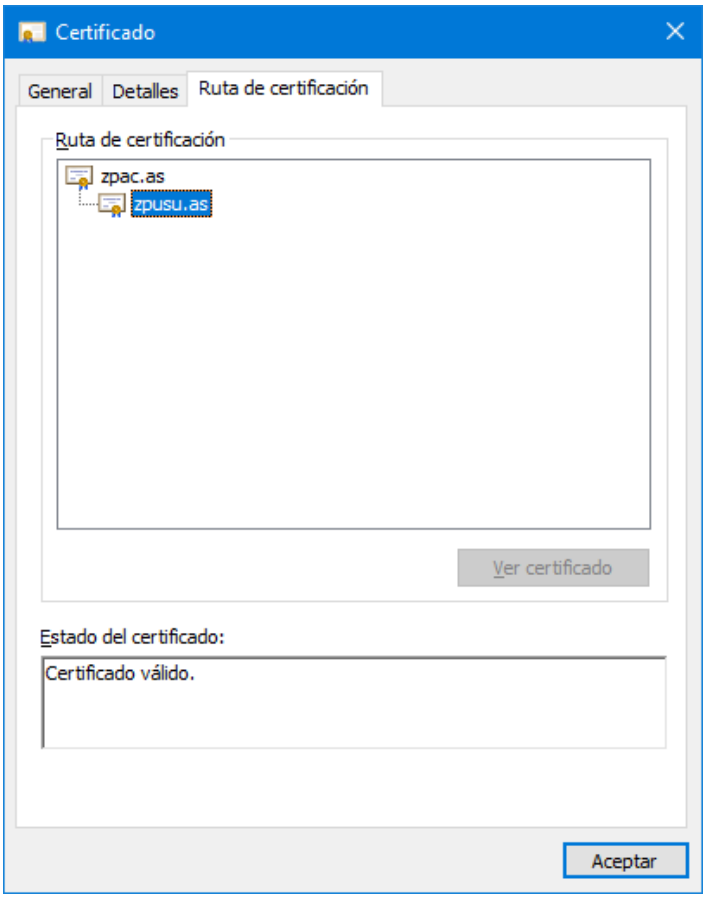
Al aceptar la instalación de un nuevo certificado raíz, creamos un nuevo anclaje de confianza y nuestro computador confiará en todos los certificados emitidos por la autoridad certificadora zpac.as.

Comprueba con certmgr que se ha importado correctamente y que aparece al final de todos los certificados (para eso lo llamamos zp..., z para que aparezca al final y sea fácilmente localizable y p porque se generó con powershell). Puede que tengas que pulsar el botón actualizar (flecha giratoria a la derecha) para que aparezca el nuevo certificado instalado.



No es sencillo ver donde almacena Windows estos certificados, pues no está oficialmente documentado. Se supone que residen en algún directorio del sistema de archivos del SO.

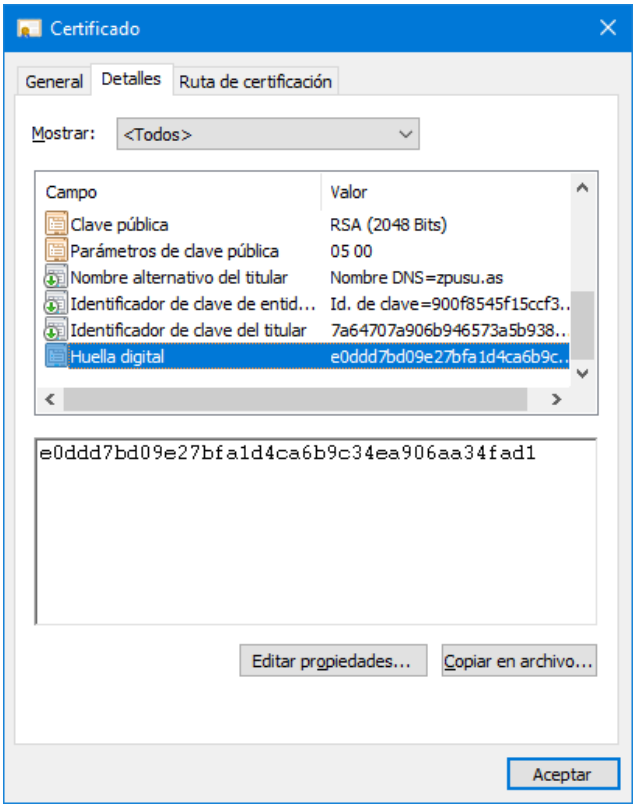
Ahora, en la herramienta certmgr abre la carpeta de certificados personales, pulsa en zpusu.as y selecciona la pestaña "Ruta de certificación". Aparece la siguiente ventana.



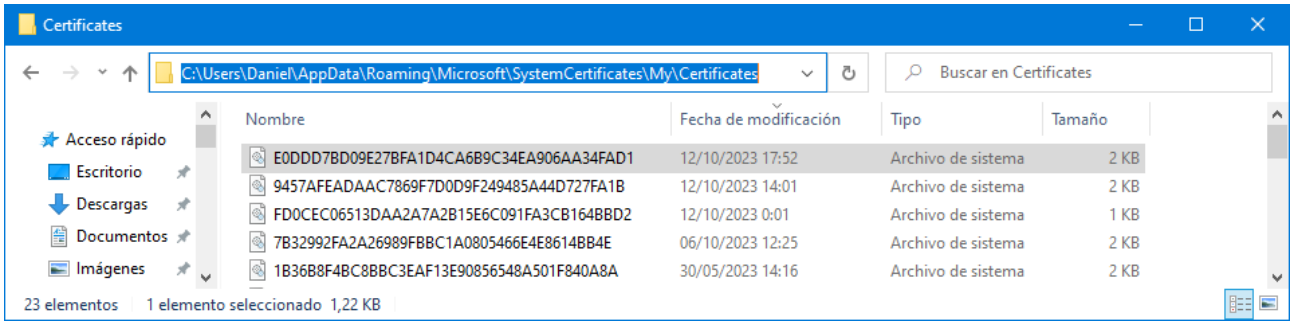
Comprueba como ahora el certificado tiene una ruta de certificación definida y el sistema considera que el certificado es válido.

ALMACENAMIENTO DE LOS CERTIFICADOS EN EL SISTEMA OPERATIVO

Con la herramienta certmgr muestra el campo del certificado de zpusu.as denominado Huella digital, tal como se muestra en la figura siguiente:



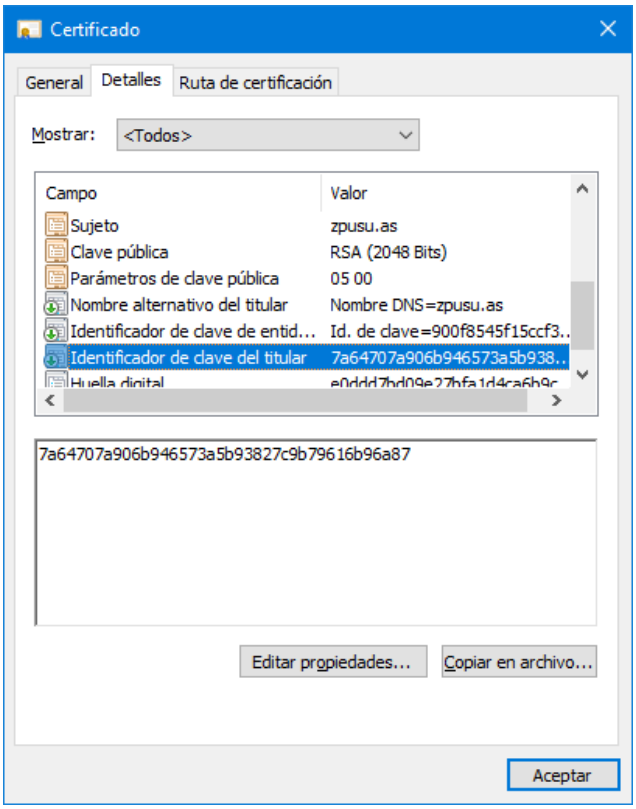
Comprobar que el certificado ha sido almacenado en el directorio y fichero que se pueden ver en la ventana siguiente (adaptar la ruta al computador utilizado):



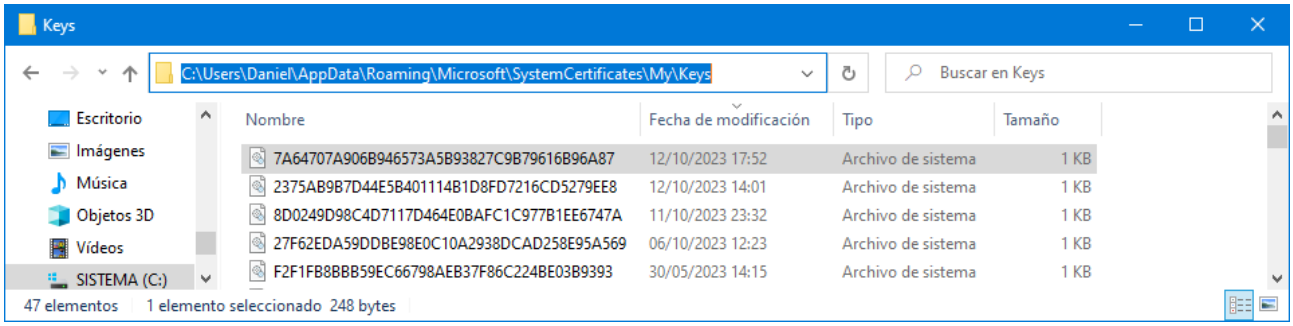
Para llegar a ese directorio debes permitir que el explorador de Windows muestre los archivos, carpetas y unidades ocultos. Para ello, en una ventana del explorador de archivos, selecciona la pestaña Vista para que se despliegue su cinta de opciones y marca la casilla □ Elementos ocultos Mostar u ocultar.

Comprueba que la huella digital del certificado coincide con el nombre del fichero en el que se almacena el certificado.

Con la herramienta certmgr muestra el campo del certificado de zpusu.as denominado Identificador de clave del titular, tal como se muestra en la figura siguiente:



Comprueba que se ha creado una clave privada en el directorio predeterminado para contener las claves del usuario justo al mismo tiempo, y que el Identificador de clave del titular coincide con el nombre del fichero en el que se almacena la clave, tal como se muestra en la ventana siguiente.



No hay documentación sobre los mecanismos que usa el SO para almacenar las claves. No obstante, observar la coincidencia de fechas, horas y minutos en la creación de los ficheros con la de importación del certificado.

En la ventana de la herramienta certmgr eliminar el certificado. Comprobar que también desaparece el fichero correspondiente del directorio en el que se almacenan los certificados. **Pero la clave privada RSA asociada al certificado no se elimina automáticamente de los directorios correspondientes.** Si no deseamos retener las claves privadas en el sistema hay que borrar sus ficheros manualmente.

Generalmente, el usuario debe despreocuparse del almacenamiento de las claves privadas asociadas a los certificados, permitiendo que el sistema operativo gestione su almacenamiento.

Pero entonces, la seguridad de las claves privadas de cada usuario, depende de la seguridad del sistema de ficheros y de la contraseña del usuario para el acceso al sistema operativo.

6. Volcar el contenido de un certificado con la herramienta certutil.exe

La herramienta certutil.exe está disponible en C:\Windows\System32\ por lo que se podrá utilizar directamente en cualquier consola sin importar el directorio desde el que se utilice.

Puede ser útil para volcar la información detallada que contiene un certificado (.cer) o un fichero de intercambio de información personal (.pfx).

A los comandos que soporta los denomina verbos.

Abre una consola y colócate en el directorio en el que están los certificados generados.

Para obtener ayuda sobre certutil teclear:

>certutil -?

>certutil -comando -?

https://docs.microsoft.com/es-es/windows-server/administration/windows-commands/certutil

Para ver el contenido de un certificado (.cer) usar:

>certutil -dump zpACas.cer

Observa la cantidad de información proporcionada sobre el certificado. Se puede ampliar un poco la información que proporciona usando la opción verbose (-v):

>certutil -v -dump zpACas.cer

Para ver el contenido de un fichero de intercambio (.pfx) usar:

>certutil -v -dump zpUSUas.pfx

El programa solicita la contraseña para abrir el fichero.

Con los ficheros .pfx el programa certutil.exe vuelca muy poca información cuando no se usa la opción -v.

También se puede usar certutil para volcar la información del almacén de certificados del usuario:

>certutil -user -store My

La opción -user indica que se use el almacén de claves y los certificados de HKEY_CURRENT_USER.

Uso de certutil para verificar un almacén de certificados y su contenedor de claves asociado:

>certutil -user -verifystore My

7. Anexo: Creación de certificados con el programa MakeCert

El programa makecert permite crear certificados y claves privadas para una autoridad certificadora y con ellos crear certificados para servidores y clientes, y en general para usuarios.

Microsoft, aunque mantiene la herramienta makecert, recomienda que se use el cmdlet New-SelfSignedCertificate del entorno PowerShell. En este anexo se explica la creación de certificados con makecert como una alternativa a New-SelfSignedCertificate.

La ayuda sobre el programa makecert.exe está integrada en la ayuda de Visual Studio. En la pestaña de índice o en la de contenido buscar Makecert.exe.

La ayuda en Internet sobre makecert.exe está disponible en:

https://docs.microsoft.com/es-es/windows/win32/seccrypto/makecert

El propio programa makecert proporciona ayuda así:

makecert -? Muestra la ayuda de las opciones básicas

makecert -! Muestra la ayuda de las opciones extendidas

El programa makecert puede crear un certificado directamente en uno de los almacenes lógicos del sistema operativo (físicamente residen en directorios del sistema operativo) y/o crearlo en un fichero. En esta práctica se recomienda crear los certificados exclusivamente en ficheros. Posteriormente se importa el certificado en un almacén lógico desde el fichero.

El programa makecert necesita claves para generar los certificados, que pueden estar en el almacén de claves del sistema operativo o en ficheros. Si no hay claves disponibles, makecert puede crear automáticamente las claves y guardarlas en el almacén de claves del SO y/o en ficheros. En esta práctica se recomienda permitir la creación automática de claves y guardarlas exclusivamente en ficheros.

Hay que crear tres certificados:

1) Un certificado auto-firmado que correspondería al certificado raíz de una Autoridad Certificadora.

2) Un certificado de servidor que debe ser firmado usando la clave privada asociada al certificado de la Autoridad Certificadora.

3) Un certificado de cliente que debe ser firmado usando la clave privada asociada al certificado de la Autoridad Certificadora.

NOTA: Los prefijos de los nombres de las entidades y de los ficheros, como zmAC.as, tienen esta racionalidad:
z → Para que los certificados aparezcan al final de los almacenes y sean fácilmente localizables
m → Para indicar que se han generado con makecert, o p para indicar generados con powershell

PARA CREAR UN CERTIFICADO RAIZ:

Se recomienda crear la orden en un archivo zmACas.bat que permita corregir cómodamente y documentar las opciones a utilizar que son, como mínimo, las siguientes:

- Nombre del sujeto del certificado; usar -n "CN=zmAC.as"
- Creación de un certificado auto-firmado; usar -r
- Permitir que la clave privada generada sea exportable; usar -pe
- Tipo del certificado; usar -cy authority
- Número de serie del certificado; usar -# 1
- Longitud de la clave del sujeto; usar -len 2048
- Algoritmo de resumen para firmar el certificado; usar -a sha256
- Nombre del fichero que contendrá la clave privada generada; usar -sv "zmACas.pvk"
- Nombre del fichero que contendrá el certificado; usar zmACas.cer

Para identificar inequívocamente los certificados en un futuro uso cruzado entre alumnos, es mejor utilizar como nombre del sujeto zmACnombrealumno, por ejemplo zmACalicia o zmACbenito. Esto también se puede aplicar a los nombres de los ficheros.

Al ejecutar makecert se pide una contraseña para proteger la clave privada de la autoridad certificadora que se crea automáticamente y que se debe almacenar en un fichero. Usar **conac**. A continuación, makecert pide esta contraseña para generar el fichero con la clave privada.

Hacer doble clic sobre el fichero zmACas.cer para ver la información general y los detalles del certificado, así como la ruta de certificación (un solo elemento).

Observar que en el directorio aparece el fichero zmACas.pvk que contiene la clave privada de la autoridad certificadora.

PARA CREAR UN CERTIFICADO DE SERVIDOR:

Se recomienda crear la orden en un archivo zmSERas.bat que permita corregir cómodamente y documentar las opciones a utilizar que son, como mínimo, las siguientes:

- Nombre del sujeto del certificado; usar -n "CN=zmSER.as" (o mejor zmSERnombrealumno)
- Permitir que la clave privada generada sea exportable; usar -pe
- Tipo del certificado; usar -cy end
- Nombre del fichero que contiene el certificado del emisor; usar -ic "zmACas.cer"
- Nombre del fichero que contiene la clave privada del emisor; usar -iv "zmACas.pvk"
- El tipo del clave del sujeto; usar -sky Exchange
- Longitud de la clave del sujeto; usar -len 2048
- Algoritmo de resumen para firmar el certificado; usar -a sha256
- Nombre del fichero que contendrá la clave privada generada; usar -sv "zmSERas.pvk"
- Nombre del fichero que contendrá el certificado; usar zmSERas.cer

Al ejecutar makecert se pide una contraseña para proteger la clave privada del servidor que debe crear automáticamente y que se debe almacenar en un fichero. Usar por ejemplo **conser**. A continuación makecert pide esta contraseña para generar el fichero con la clave privada.

Finalmente, makecert pide la contraseña de la clave privada del emisor del certificado (la autoridad certificadora) para firmar el certificado. Esta contraseña es **conac**.

Hacer doble clic sobre el fichero zmSERas.cer para ver la información general y los detalles del certificado, así como la ruta de certificación (dos elementos).

PARA CREAR UN CERTIFICADO DE CLIENTE:

Se recomienda crear la orden en un archivo zmCLIas.bat que permita corregir cómodamente y documentar las opciones a utilizar que son, como mínimo, las siguientes:

- Nombre del sujeto del certificado; usar -n "CN=zmCLI.as" (o mejor zmCLInombrealumno)
- Permitir que la clave privada generada sea exportable; usar -pe
- Tipo del certificado; usar -cy end
- Nombre del fichero que contiene el certificado del emisor; usar -ic "zmACas.cer"
- Nombre del fichero que contiene la clave privada del emisor; usar -iv "zmACas.pvk"
- El tipo del clave del sujeto; usar -sky Exchange
- Longitud de la clave del sujeto; usar -len 2048
- Algoritmo de resumen para firmar el certificado; usar -a sha256
- Nombre del fichero que contendrá la clave privada generada; usar -sv "zmCLIas.pvk"
- Nombre del fichero que contendrá el certificado; usar zmCLIas.cer

Al ejecutar makecert se pide una contraseña para proteger la clave privada del cliente que debe crear automáticamente y que se debe almacenar en un fichero. Usar por ejemplo **concli**. Posteriormente makecert pide esta contraseña para generar el fichero con la clave privada.

Finalmente, makecert pide la contraseña de la clave privada del emisor del certificado (la autoridad certificadora) para firmar el certificado. Esta contraseña es **conac**.

Hacer doble clic sobre el fichero zmCLIas.cer para ver la información general y los detalles del certificado, así como la ruta de certificación (dos elementos).

CONVERSION DE LOS CERTIFICADOS:

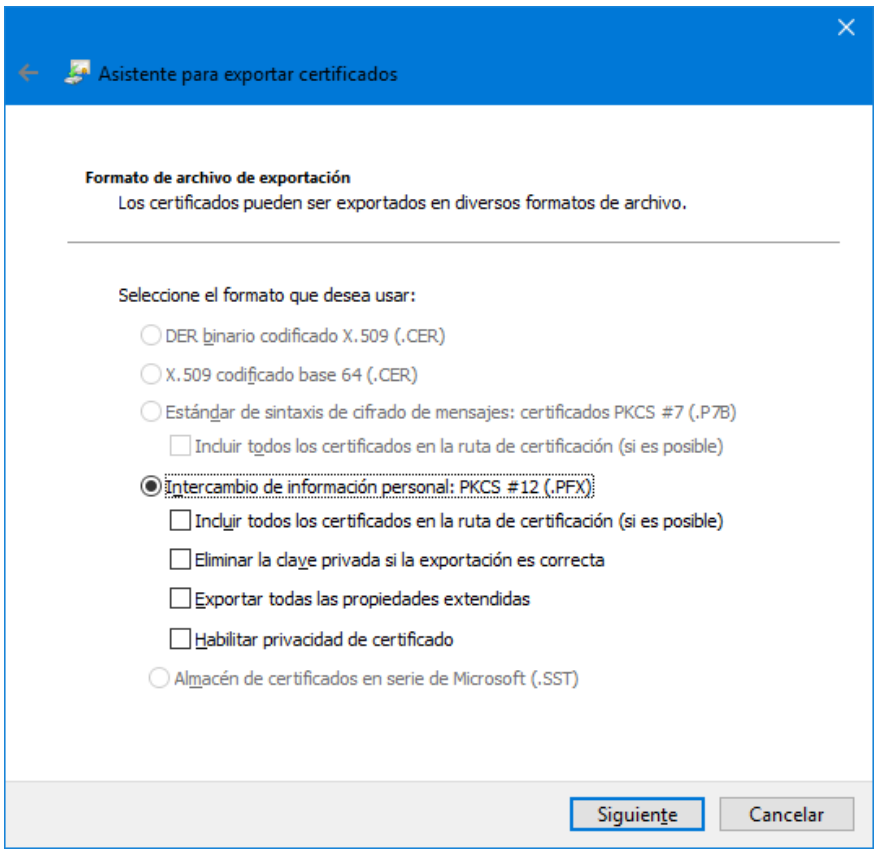
Los certificados anteriores (.cer) NO incluyen la clave privada del sujeto para el que se ha emitido el certificado. Pero en muchas ocasiones es necesario que el sujeto disponga de su pareja de claves (pública y privada) conjuntamente.

Para ello se puede usar el programa pvk2pfx.exe que añade la clave privada (.pvk) al certificado (.cer) generando un nuevo certificado del tipo PFX (.pfx) que implementa el estándar PKCS#12 (*Personal Information Exchange Syntax Standard*). Observar que denominar como certificado a un fichero PFX que incluye una clave privada es inadecuado, aunque habitual.

Como nombres de estos nuevos certificados a crear se sugiere utilizar: zmCLIas.pfx y zmSERas.pfx. NO generar un .pfx para la Autoridad Certificadora.

Para disponer de ayuda, ejecutar el programa sin argumentos, y así aparece en la consola la ayuda con las opciones para los argumentos. Si no se proporcionan los argumentos suficientes se abre el asistente de exportación de certificados. **Ejecutar pvk2pfx pasándole solo 2 argumentos:** el fichero con la clave privada (.pvk) y el fichero con el certificado correspondiente (.cer).

Al crear los certificados .pfx se muestra un cuadro de diálogo que permite optar por exportar la clave privada o no exportarla. Seleccionar que se desea exportarla. El siguiente cuadro de diálogo permite elegir tres opciones para el archivo final .PFX.



Si no seleccionamos opciones tendremos el certificado más simple posible. Denominarlo zmSERas_Simple.pfx por ejemplo.

Si seleccionamos las opciones primera y tercera se incluye en el archivo todos los certificados que permiten validar el certificado del servidor. Denominarlo zmSERas_Completo.pfx.

Al utilizar el certificado "simple" para configurar un servidor se pueden obtener mensajes de aviso indicando que falta información. Con el "completo" no deberían aparecer avisos, y por ello se recomienda usar el completo.

Al optar por exportar la clave privada al archivo PFX será necesario proporcionar una contraseña para proteger el acceso al fichero PFX. Se recomienda usar: para el servidor **conserpfx** y para el cliente **conclipfx**.

Usando las contraseñas indicadas en el guion de esta práctica siempre existe la posibilidad de recordarlas consultando nuevamente el guion de la práctica.

Al hacer doble clic sobre un fichero (.pfx) NO se abre el visor de certificados, sino que se abre el asistente de importación de certificados, ya que este formato está orientado a la transferencia de información de un computador a otro.