

Gestión de Certificados Digitales

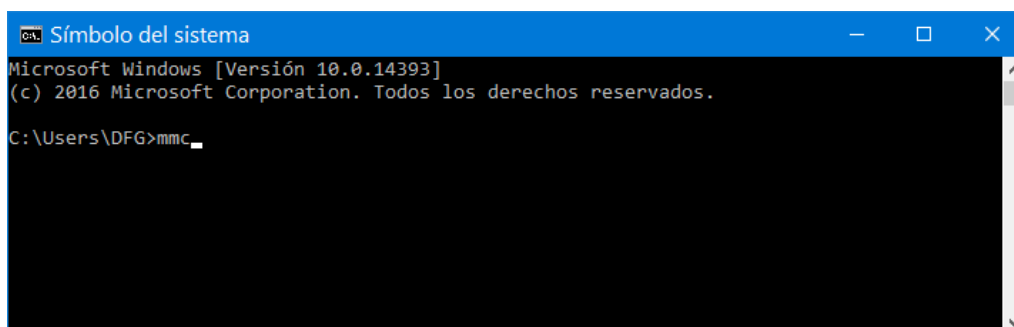
Práctica 5A

1. Objetivo

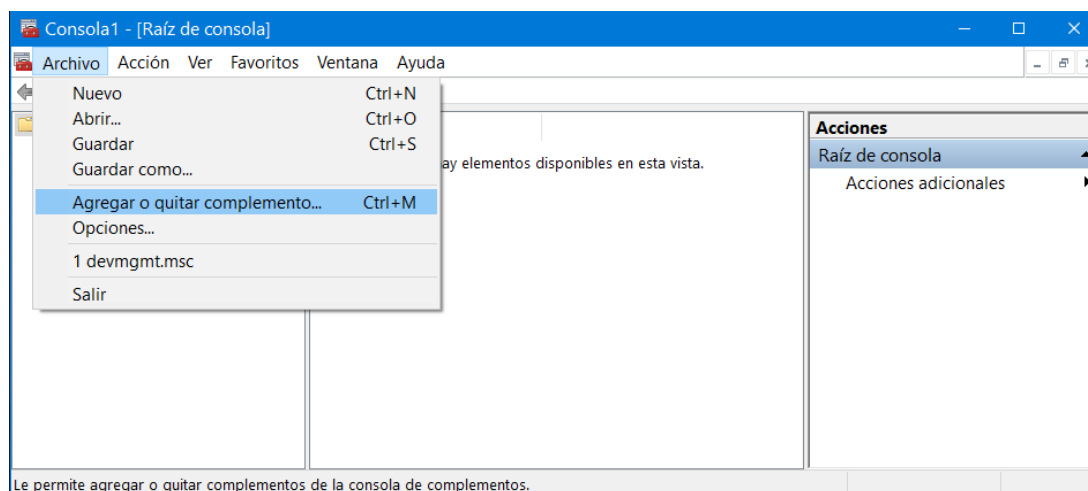
En esta práctica el alumno debe crear certificados que puedan ser instalados tanto en un servidor web como en los computadores en los que se ejecutan navegadores web. Además, cargará los certificados creados en el almacén de certificados de Windows. En una práctica posterior se utilizarán los certificados 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

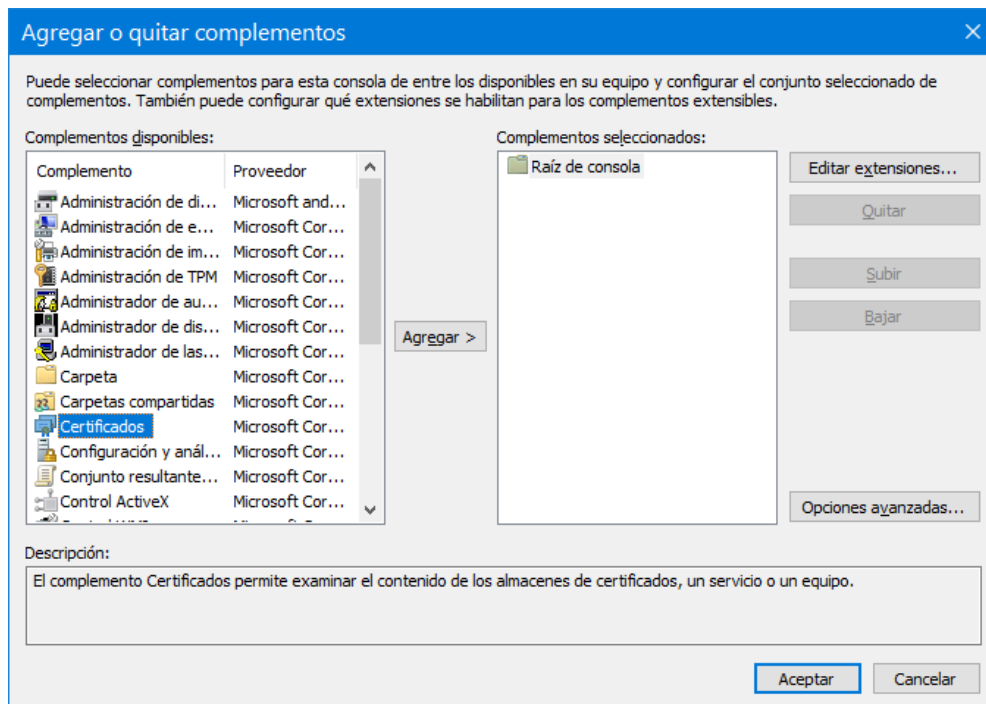
Para trabajar con certificados abrir una Microsoft Management Console. Teclear mmc en una ventana de comandos.



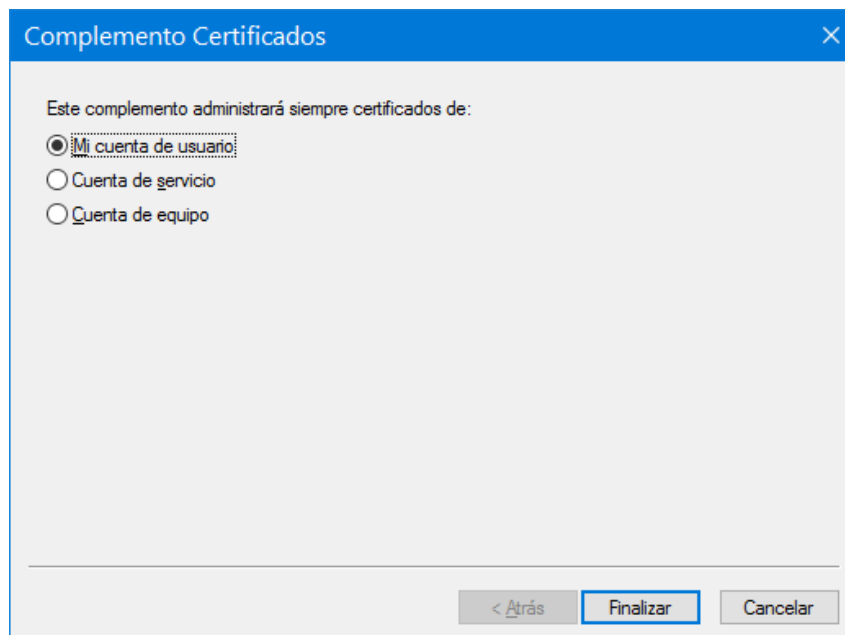
Se abre una ventana de consola y en el menú archivo seleccionar la opción de "Agregar o quitar complemento"



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

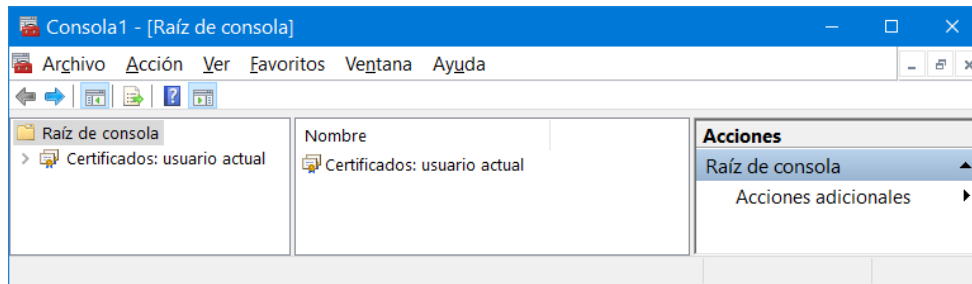


Al pulsar el botón agregar aparece un cuadro de dialogo solicitando el tipo de cuenta cuyos certificados se administrarán con el complemento seleccionado.

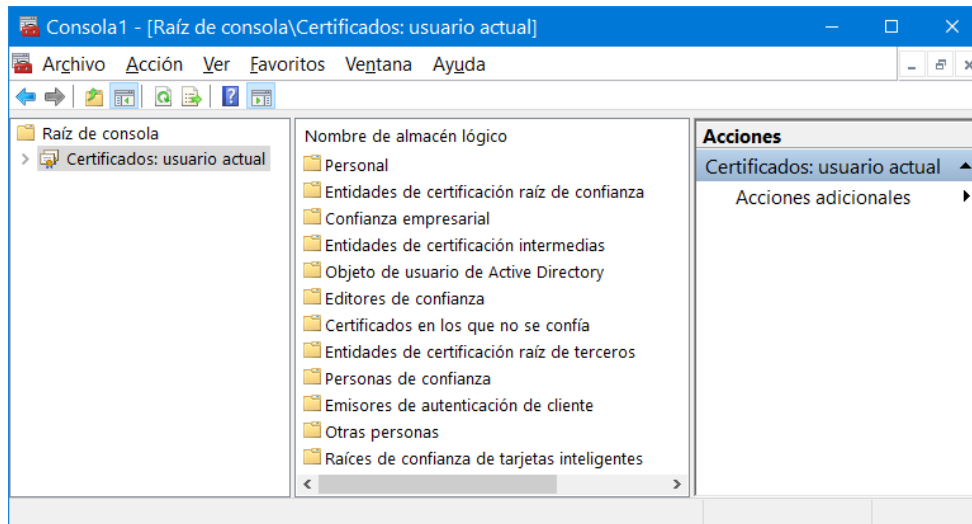


Inicialmente utilizar la cuenta del usuario. Tras pulsar el botón Finalizar en este cuadro y luego el botón Aceptar en la ventana anterior, aparece el nuevo complemento en la consola denominado "Certificados: usuario actual".

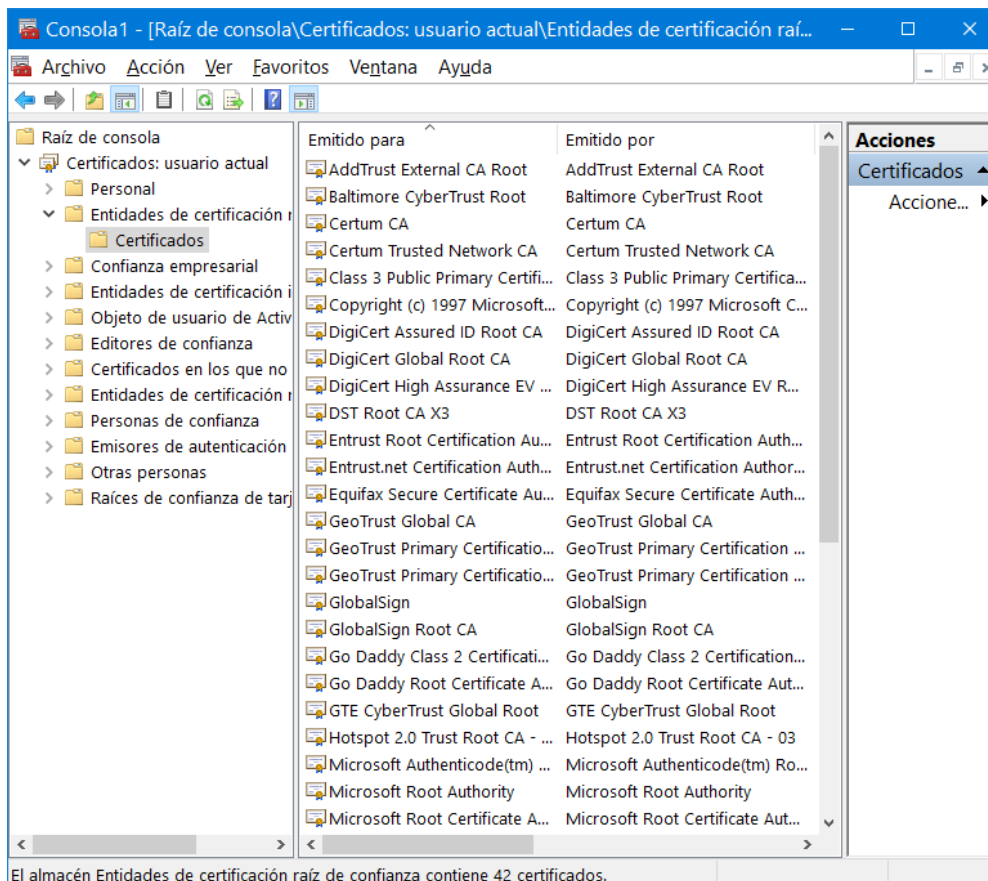
NOTA: la ventana anterior tiene tres opciones porque la ejecuta un administrador del sistema. Generalmente, un usuario sin privilegios de administración solo puede administrar los certificados de su propia cuenta de usuario.



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

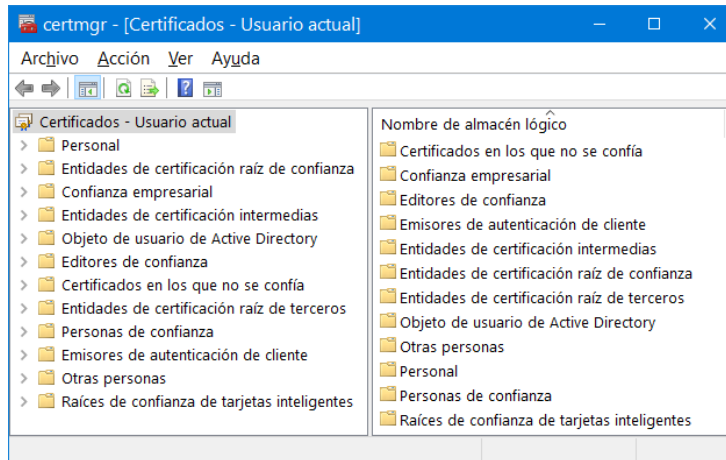


Se puede entrar en cada almacén lógico para ver los certificados que contiene. Por ejemplo dentro de "Entidades de certificación raíz de confianza\Certificados" se puede ver:

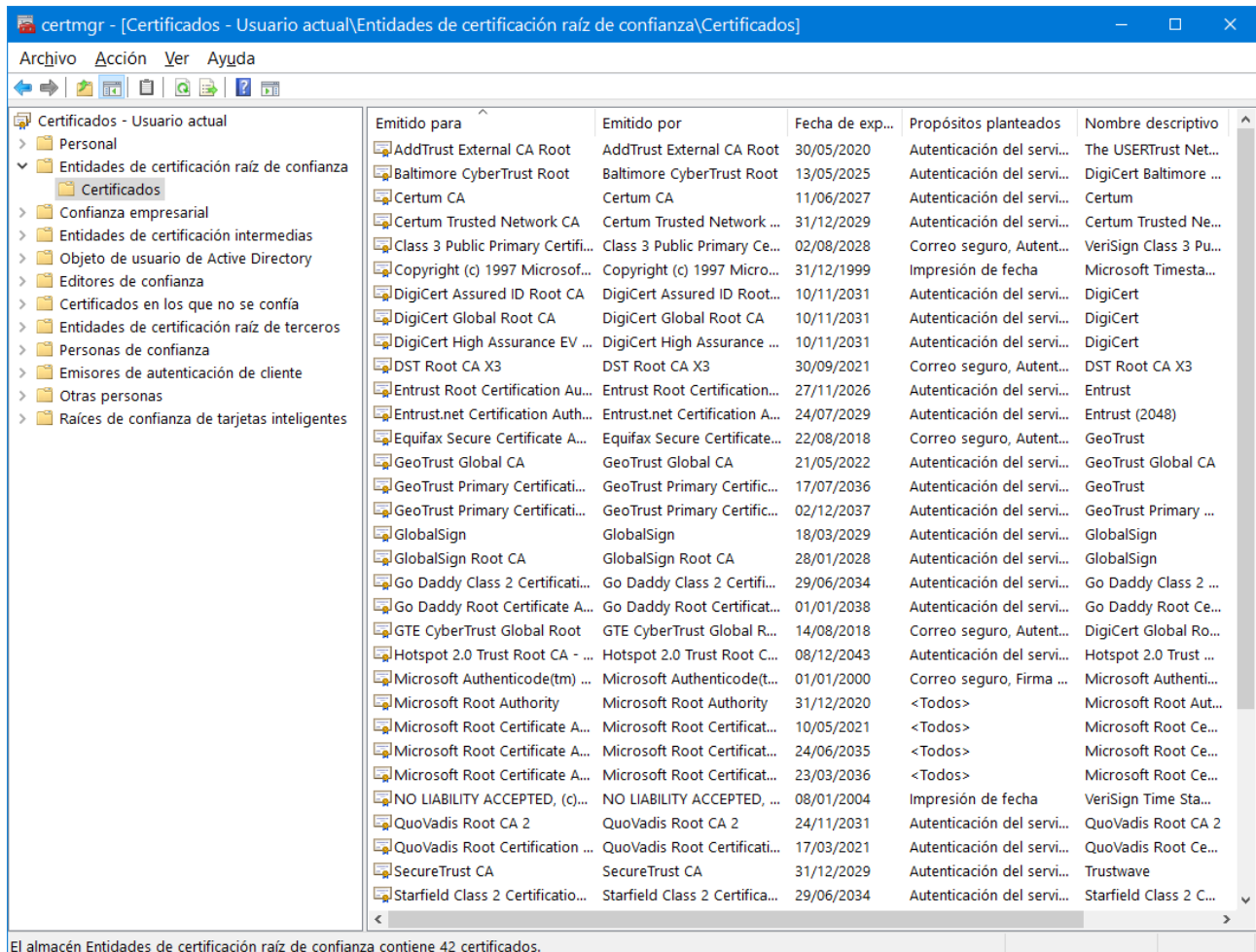


OTRA FORMA MÁS DIRECTA DE ACCEDER A LOS CERTIFICADOS:

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



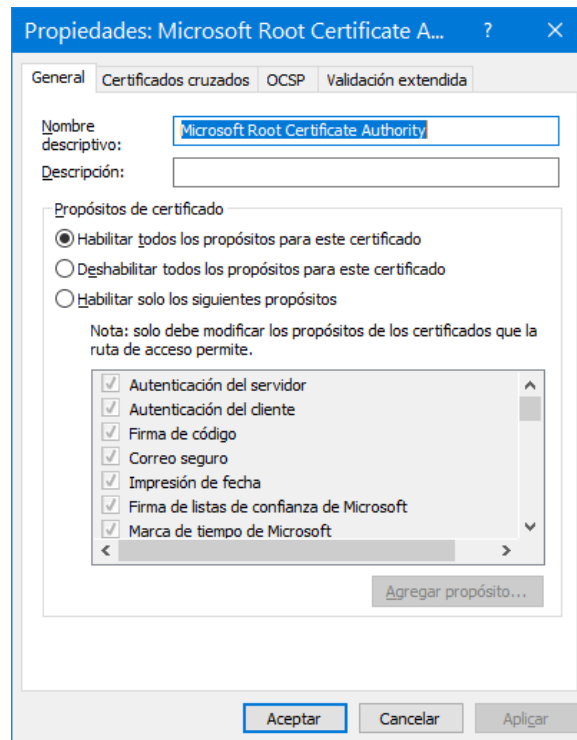
Si desplegamos el árbol de la consola (ventana de la izda) y entramos en Entidades de certificación raíz de confianza > Certificados, vemos los siguientes certificados:



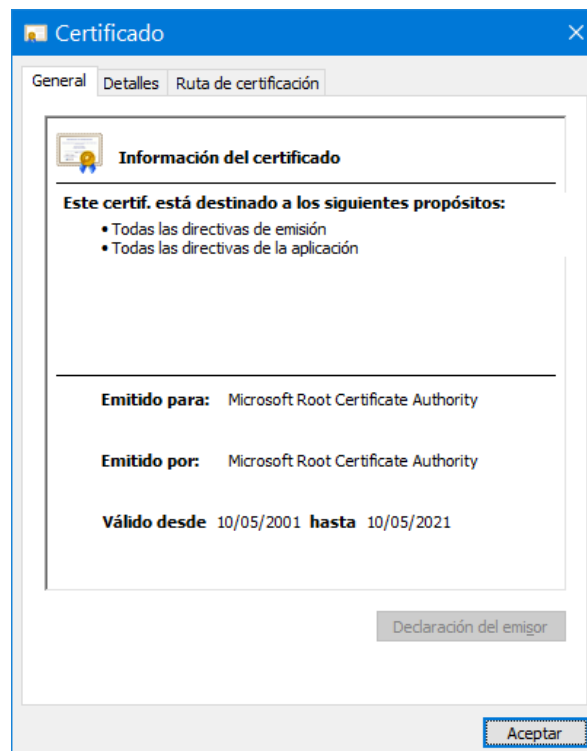
Observar que el cuarto botón por la izquierda está pulsado porque se está mostrando el árbol de la consola. Los botones a su derecha permiten cortar, copiar, eliminar, ver propiedades, y exportar la lista. Estos botones aparecen cuando está seleccionado un certificado en la ventana derecha. Estas tareas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

PROPIEDADES DE UN CERTIFICADO:

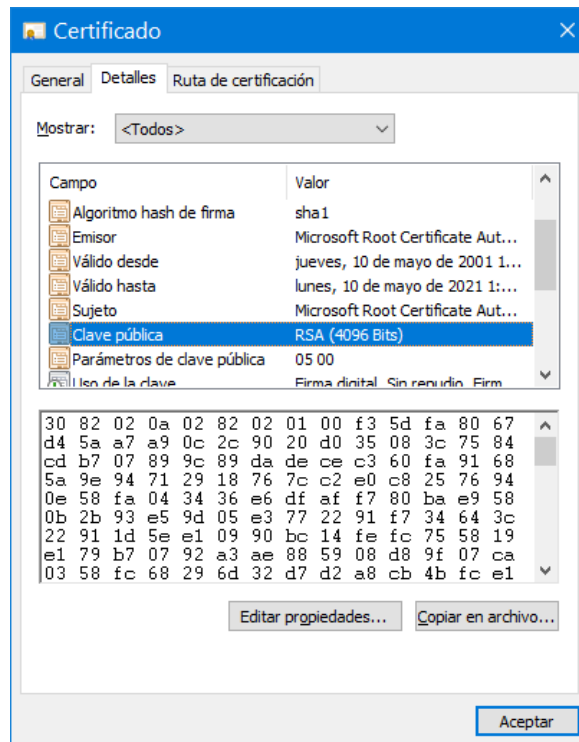
En el menú Acción elegir la opción Propiedades, o pulsar el botón derecho del ratón sobre el certificado seleccionado, o pulsar el botón Propiedades y aparece esta ventana cuando está seleccionado un certificado. Observar que este certificado está habilitado para todos los propósitos. Las otras pestañas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



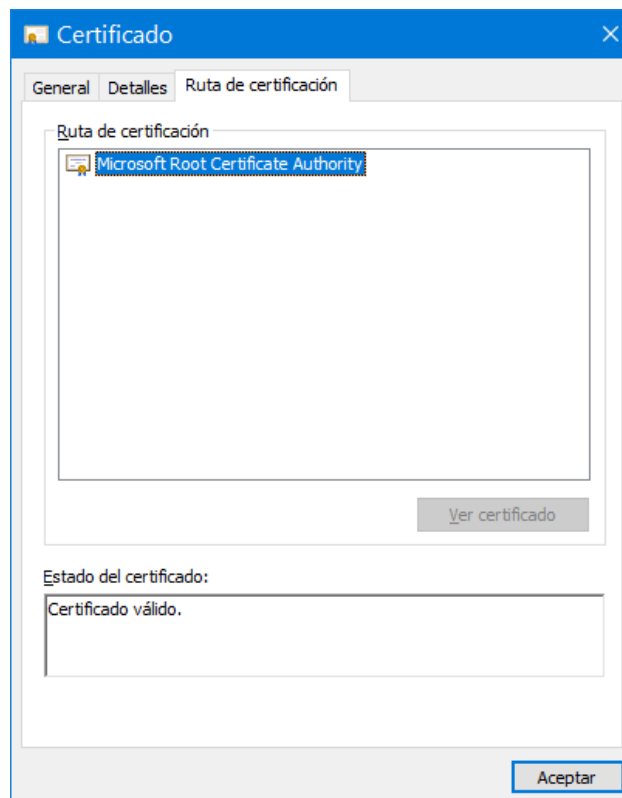
Si elegimos la opción de Abrir el certificado aparece la ventana Certificado que tiene tres pestañas. En la pestaña General se muestra la información general del certificado. Los propósitos del certificado, emitido para, emitido por y su periodo de validez. Observar que como éste es un certificado raíz,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

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 <http://www.cacert.org/>, o también, <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. En esta práctica se utilizará esta opción empleando los programas makecert.exe y pvk2pfx.exe. Estos programas están disponibles en el Campus Virtual en sus versiones de 32 y 64 bits. También puedes buscar nuevas versiones en un subdirectorio del Sistema Windows o de Visual Studio. Para trabajar cómodamente se puede copiar estos ejecutables al directorio local de trabajo.

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

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

<https://msdn.microsoft.com/library/windows/desktop/aa386968.aspx>

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 o en el registro de Windows) 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.

PARA CREAR UN CERTIFICADO RAIZ:

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

- Creación de un certificado auto-firmado
- Permitir que la clave privada generada sea exportable
- Nombre del sujeto del certificado; usar zzAC
- Tipo del certificado; usar authority
- Número de serie del certificado; usar 1
- Nombre del fichero que contendrá la clave privada generada; usar zzAC.pvk
- Nombre del fichero que contendrá el certificado; usar zzAC.cer

Para identificar inequívocamente los certificados en un futuro uso cruzado entre alumnos, es mejor utilizar como nombre del sujeto zzACnombrealumno, por ejemplo zzACalicia o zzACbenito. 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 zzAC.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 zzAC.pvk que contiene la clave privada de la autoridad certificadora.

PARA CREAR UN CERTIFICADO DE SERVIDOR:

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

- Permitir que la clave privada generada sea exportable
- Nombre del sujeto del certificado; usar zzServidor (**o mejor zzSERnombrealumno**)
- Nombre del fichero que contiene el certificado del emisor; usar zzAC.cer
- Nombre del fichero que contiene la clave privada del emisor; usar zzAC.pvk
- El tipo del clave del sujeto; usar exchange
- Nombre del fichero que contendrá la clave privada generada; usar zzSER.pvk
- Nombre del fichero que contendrá el certificado; usar zzSER.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 zzSER.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 ccCLI.bat que permita corregir cómodamente y documentar las opciones a utilizar que son, como mínimo, las siguientes:

- Permitir que la clave privada generada sea exportable
- Nombre del sujeto del certificado; usar zzCliente (**o mejor zzCLI**nombre**alumno**)
- Nombre del fichero que contiene el certificado del emisor; usar zzAC.cer
- Nombre del fichero que contiene la clave privada del emisor; usar zzAC.pvk
- El tipo del clave del sujeto; usar exchange
- Nombre del fichero que contendrá la clave privada generada; usar zzCLI.pvk
- Nombre del fichero que contendrá el certificado; usar zzCLI.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 zzCLI.cer para ver la información general y los detalles del certificado, así como la ruta de certificación (dos elementos).

CONVERSION DE LOS CERTIFICADOS:

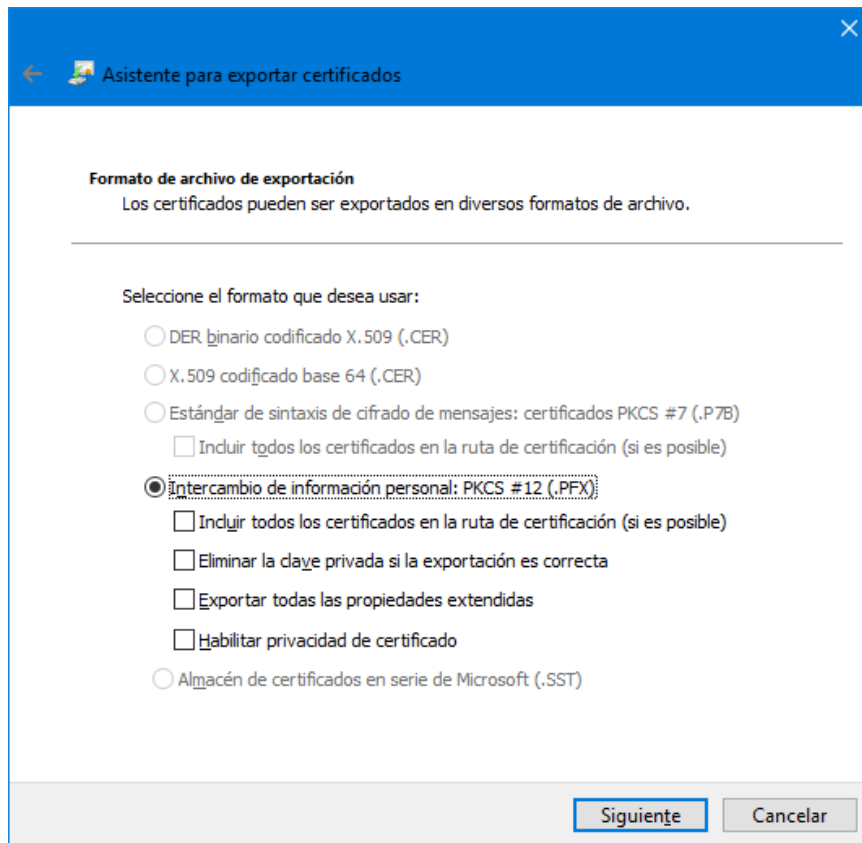
Los certificados anteriores (.cer) NO incluyen la clave privada del sujeto para el que se ha emitido el certificado. Pero en muchas ocasiones es necesario que el sujeto disponga de su pareja de claves (pública y privada) conjuntamente.

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: zzCLI.pfx y zzSER.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 zzSER_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 zzSER_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.

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**.

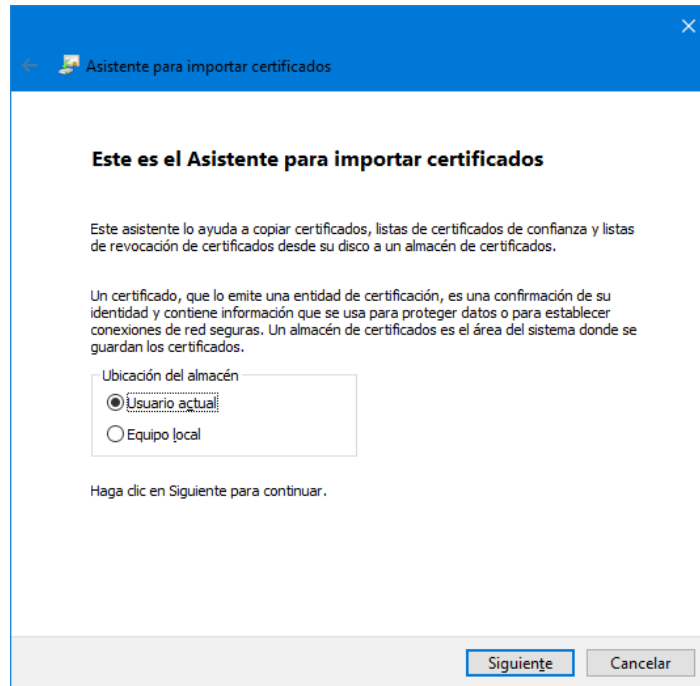
Usando las claves indicadas en el guion de esta práctica siempre existe la posibilidad de recordarlas consultando nuevamente el guion de la práctica.

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.

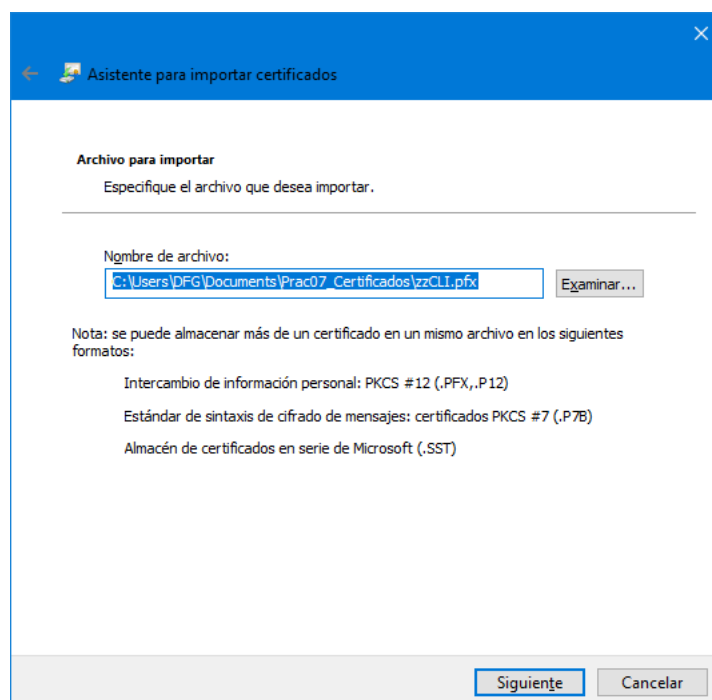
4. Cargar los certificados en el Almacén de Certificados de Windows

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 cliente y su clave privada asociada, hacer doble clic con el ratón sobre el fichero zzCLI.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 zzCLI.pfx contiene una clave privada protegida el asistente solicita la contraseña utilizada para protegerla.

Asistente para importar certificados

Protección de clave privada
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.

Contraseña:

☐ Mostrar contraseña

Opciones de importación:

☐ Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.

☐ Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.

☒ Incluir todas las propiedades extendidas.

Siguiente Cancelar

Si se han seguido las indicaciones de la práctica la clave será **conclipfx**. 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:

Asistente para importar certificados

Almacén de certificados
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

☐ Seleccionar automáticamente el almacén de certificados según el tipo de certificado

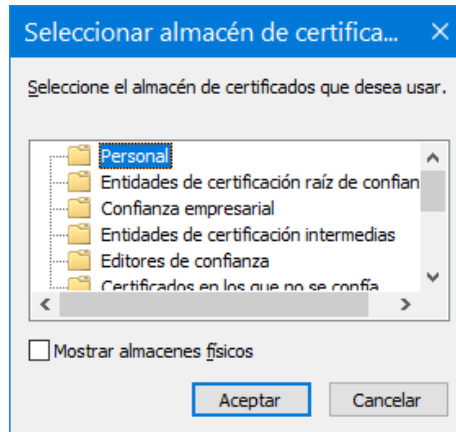
☒ Colocar todos los certificados en el siguiente almacén

Almacén de certificados:

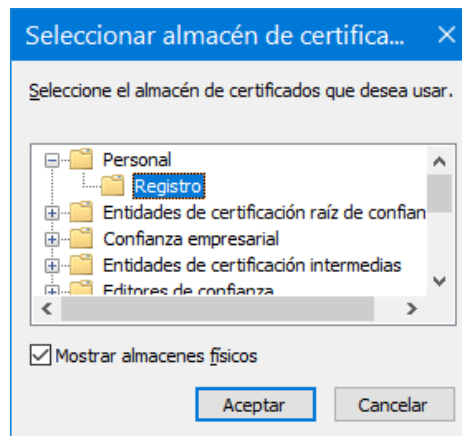
Examinar...

Siguiente Cancelar

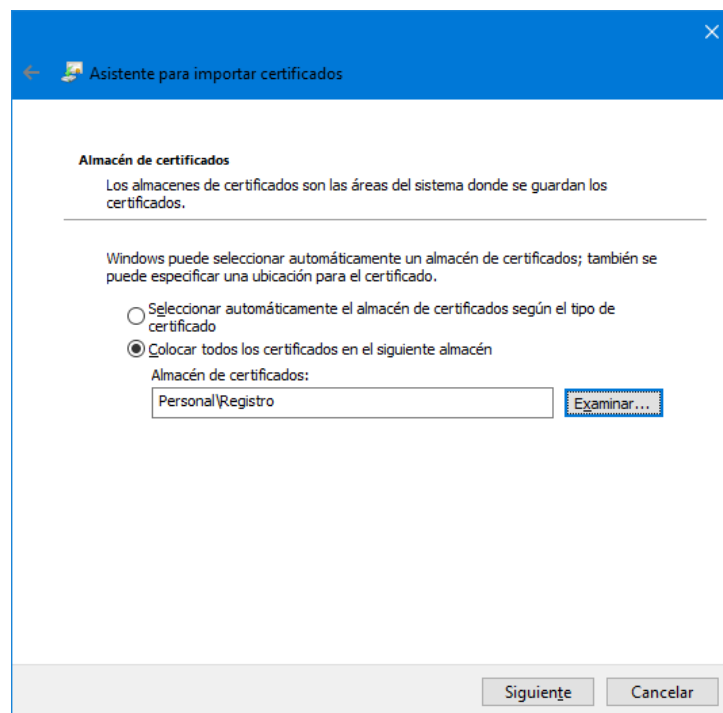
Al pulsar el botón Examinar... aparece la ventana "Seleccionar almacén de certificados".



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:

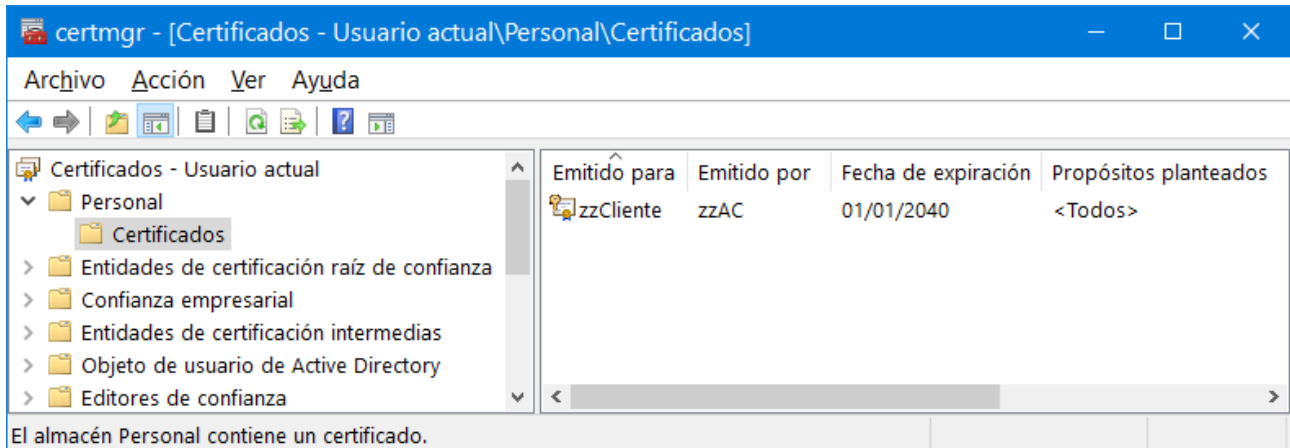


Al pulsar el botón Aceptar, el asistente de importación muestra la siguiente información:

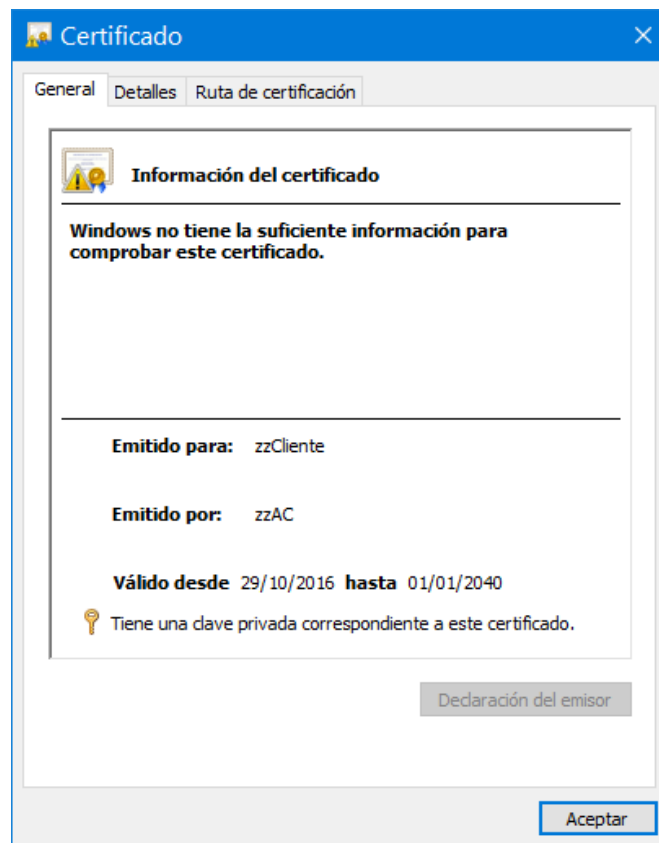


Pulsar el botón Siguiente y finalizar el proceso de importación.

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



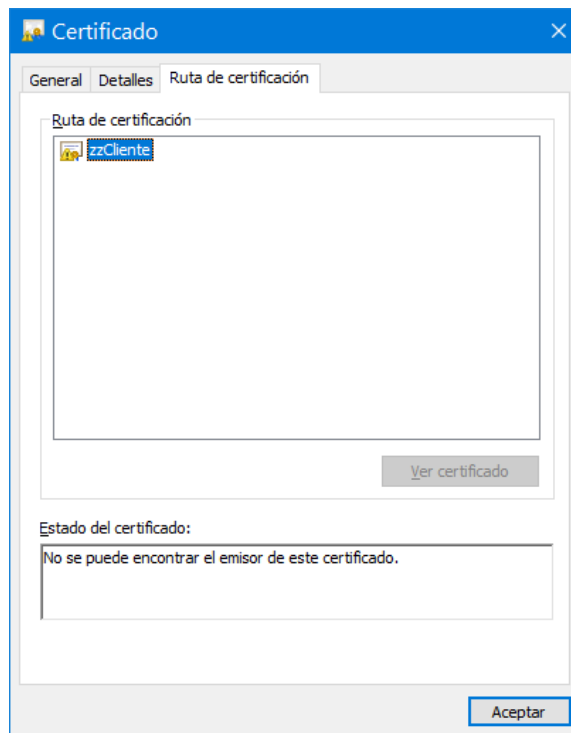
Para ver las propiedades del certificado haz doble clic sobre el certificado y aparece la ventana siguiente, que muestra la pestaña “General” con información del certificado.



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

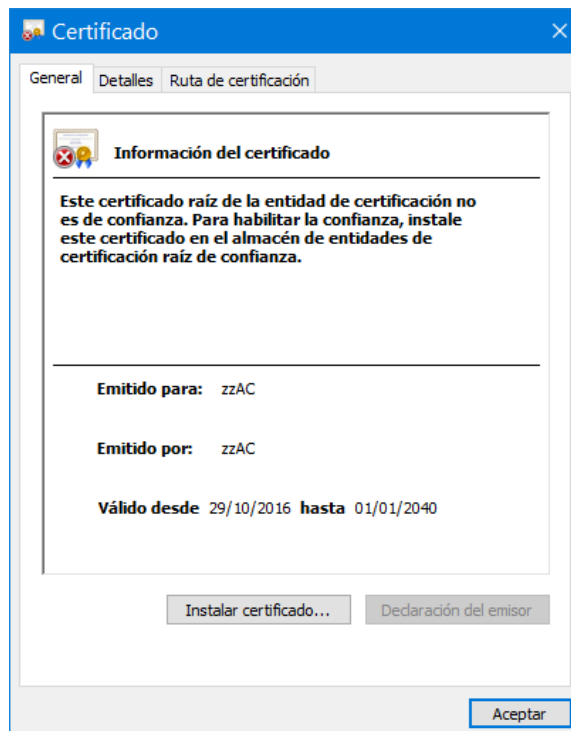
Observa también el mensaje que hay en la parte superior del cuadro informativo, que indica que Windows no tiene la suficiente información para comprobar el certificado. El problema está relacionado con la cadena de certificados necesaria para validar el certificado de zzCliente. Se analiza a continuación.

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 zzAC.cer, emisora del certificado de zzCliente, en el almacén denominado "Entidades de certificación raíz de confianza". Para ello hacer doble clic sobre el fichero zzAC.cer y se abre la ventana siguiente:

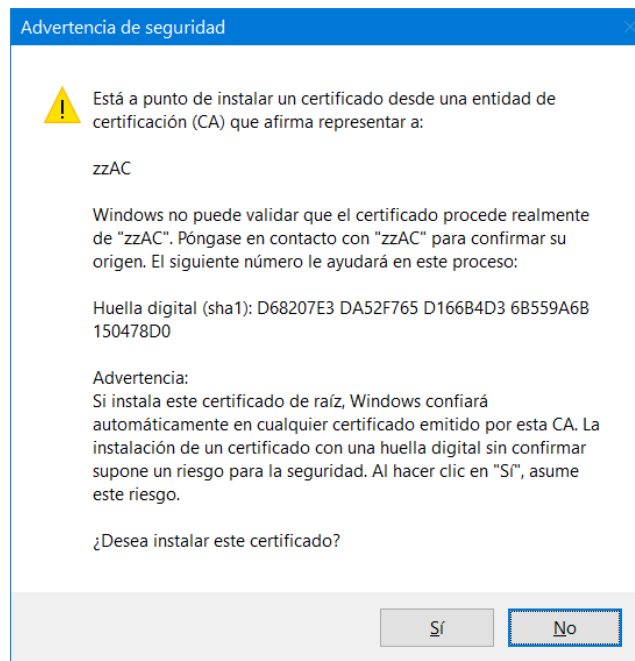


Observar que en la parte inferior del cuadro informativo no se indica que hay una clave privada asociada al certificado, lo cual es correcto, pues estamos usando un fichero .cer.

Pulsar el botón Instalar certificado...

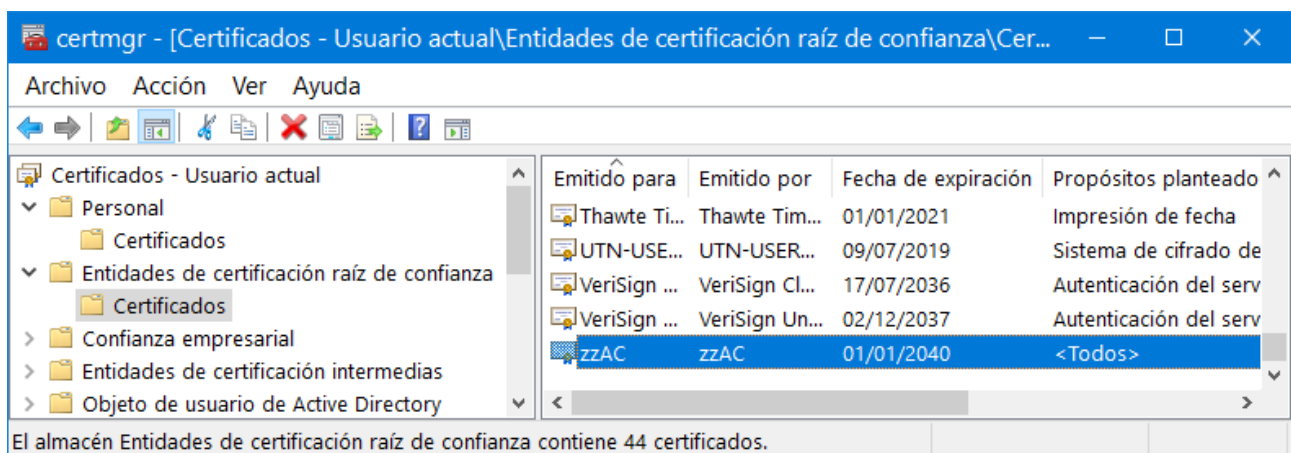
En el Asistente para importar certificados, seleccionar Usuario actual y el almacén “Entidades de certificación raíz de confianza”. No elegir el almacén físico, dejando que elija el asistente.

El asistente muestra la ventana siguiente:



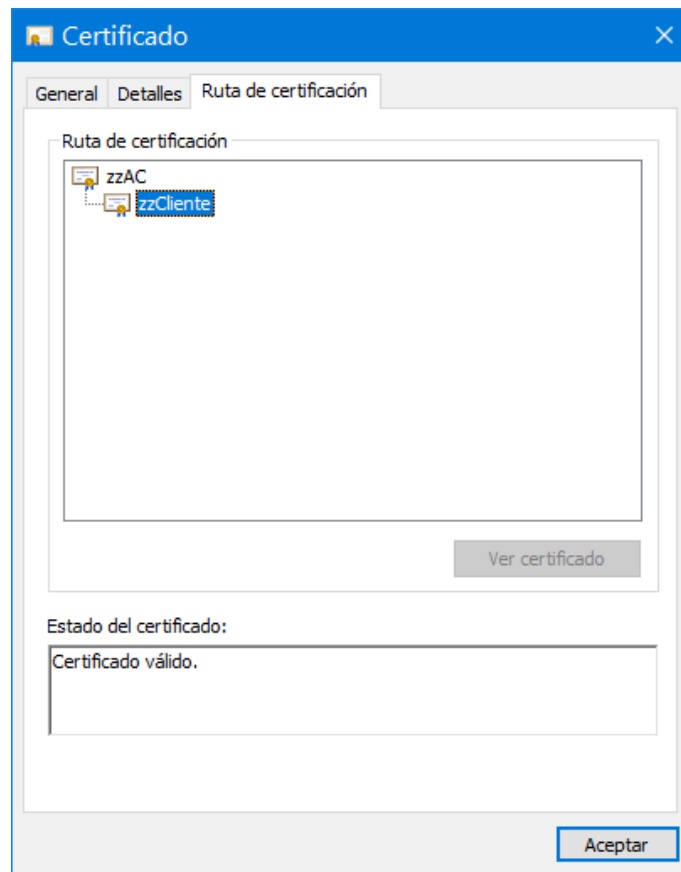
Al aceptar la instalación de un nuevo certificado raíz, creamos un nuevo anclaje de confianza y nuestro computador confiará en todos los certificados emitidos por la autoridad certificadora zzAC.

Comprueba con certmgr que se ha importado correctamente y que aparece al final de todos los certificados (**para eso lo llamamos zz..., para que aparezca al final y sea fácilmente localizable**). 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 el Registro del SO.

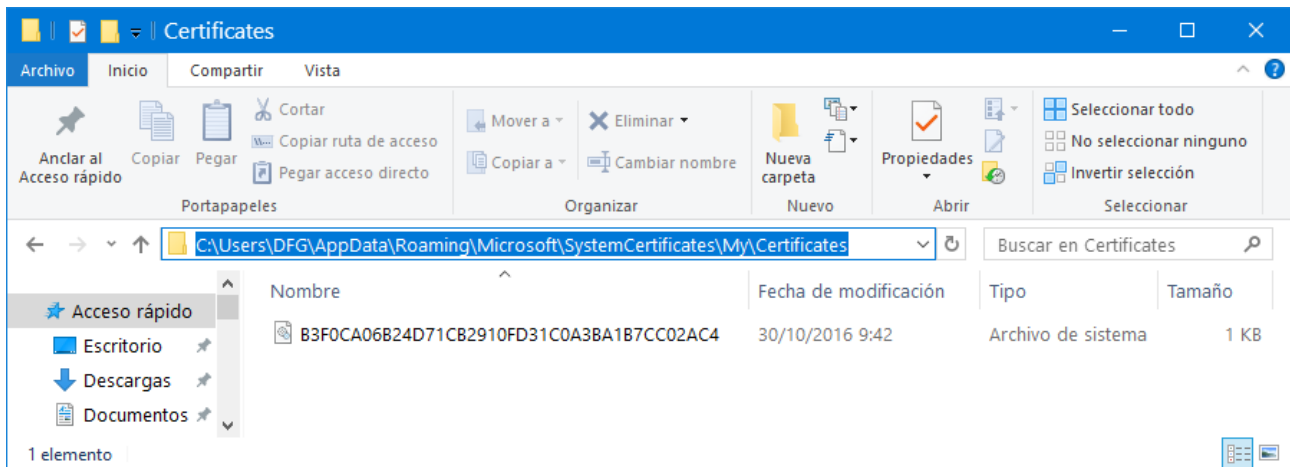
Ahora, en la herramienta certmgr abre la carpeta de certificados personales, pulsa en zzCliente y selecciona la pestaña "Ruta de certificación". Aparece la siguiente ventana.



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

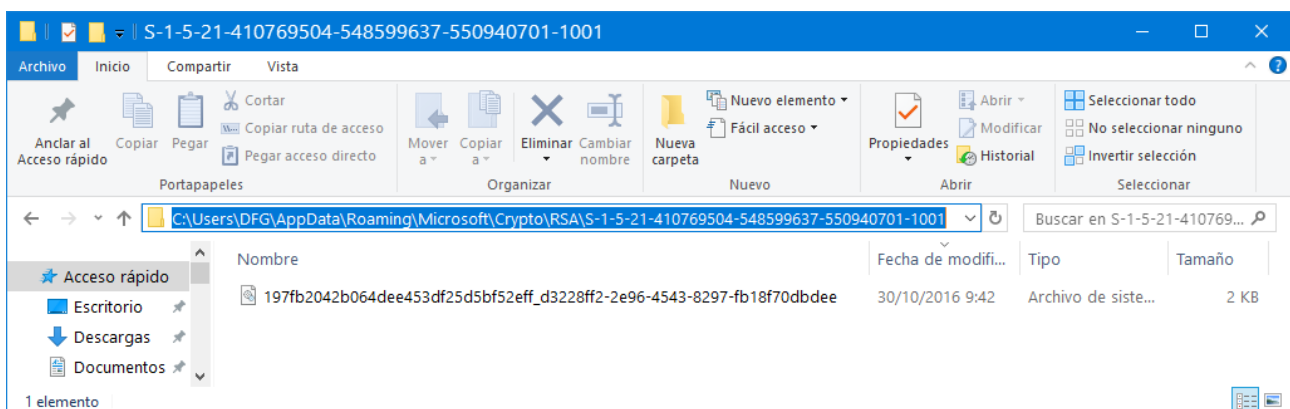
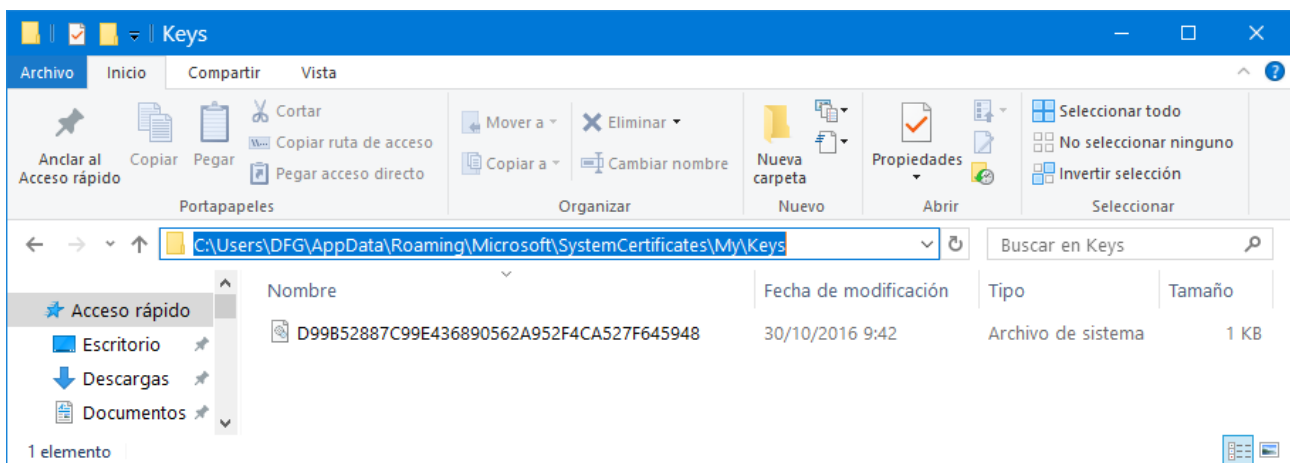
ALMACENAMIENTO DE LOS CERTIFICADOS EN EL SISTEMA OPERATIVO

Comprobar que el certificado ha sido almacenado en el directorio y fichero que se pueden ver en la ventana siguiente:



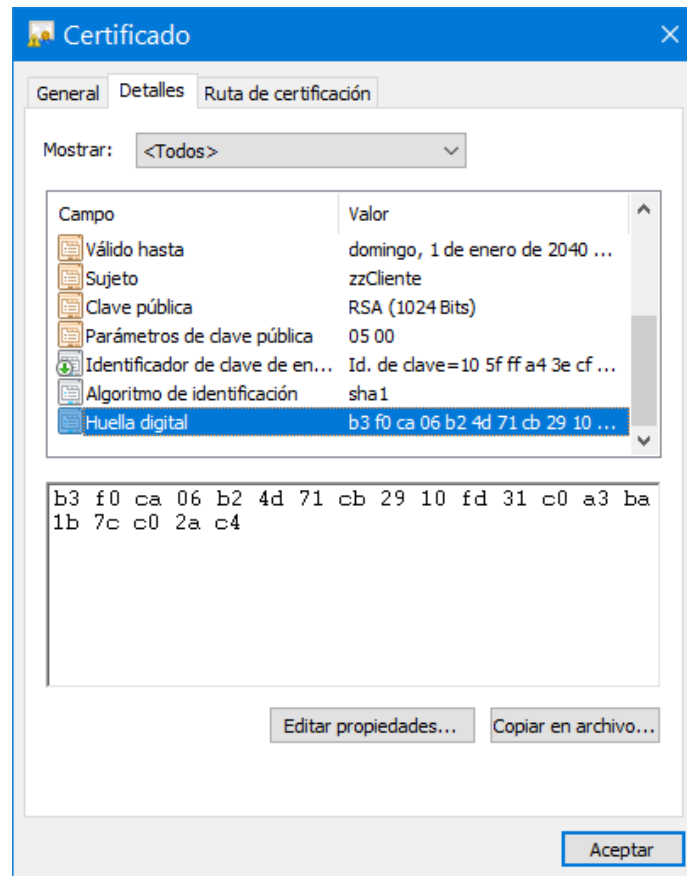
Para llegar a ese directorio debes permitir que el explorador de Windows muestre los archivos, carpetas y unidades ocultos. Para ello, en una ventana del explorador de archivos, selecciona la pestaña Vista para que se despliegue su cinta de opciones y marca la casilla ☐ Elementos ocultos Mostrar u ocultar.

También puedes comprobar que se crea una clave privada en directorios predeterminados para las claves del usuario justo al mismo tiempo, tal como se muestra en las dos ventanas siguientes.



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.

Comprobar también que el nombre del fichero en el que se almacena el certificado coincide con la propiedad denominada "Huella digital" del certificado, tal como se muestra en la ventana siguiente:



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. No las borres todavía.

Volver a importar el certificado, pero ahora permitir que el asistente seleccione automáticamente el almacén de destino, tanto el almacén lógico como el físico. Comprobar que se obtienen los mismos resultados que con la importación anterior en la que se detallaron las ubicaciones deseadas para el certificado.

Comprueba que se ha generado un nuevo fichero de claves en el directorio:

C:\Users\DFG\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-410769504-548599637-550940701-1001

Pero no se ha generado uno nuevo en el directorio:

C:\Users\DFG\AppData\Roaming\Microsoft\SystemCertificates\My\Keys

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.

5. 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 -?
```

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

```
>certutil -dump zzAC.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 zzAC.cer
```

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

```
>certutil -v -dump zzSER.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.

6. Opcional: Creación de certificados usando el entorno PowerShell

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.

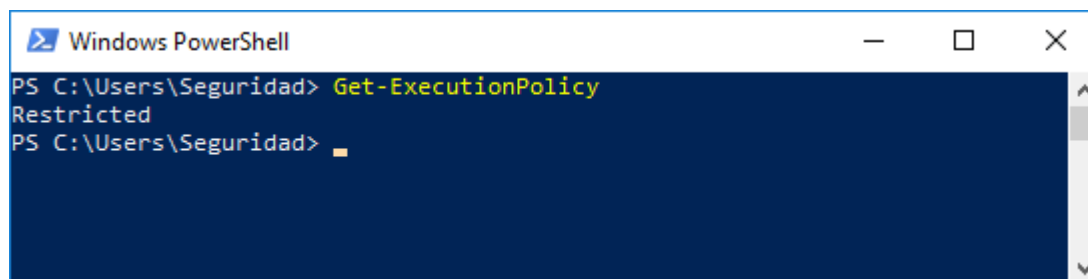
Abrir una consola de PowerShell en un sistema operativo Windows 10. Para ello pulsa el BOTÓN INICIO y al final del menú de aplicaciones mostrado aparece la carpeta de “Windows PowerShell”. En un SO de 64 bits aparece la aplicación “Windows PowerShell” de 64 bits y también la aplicación “Windows PowerShell (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.

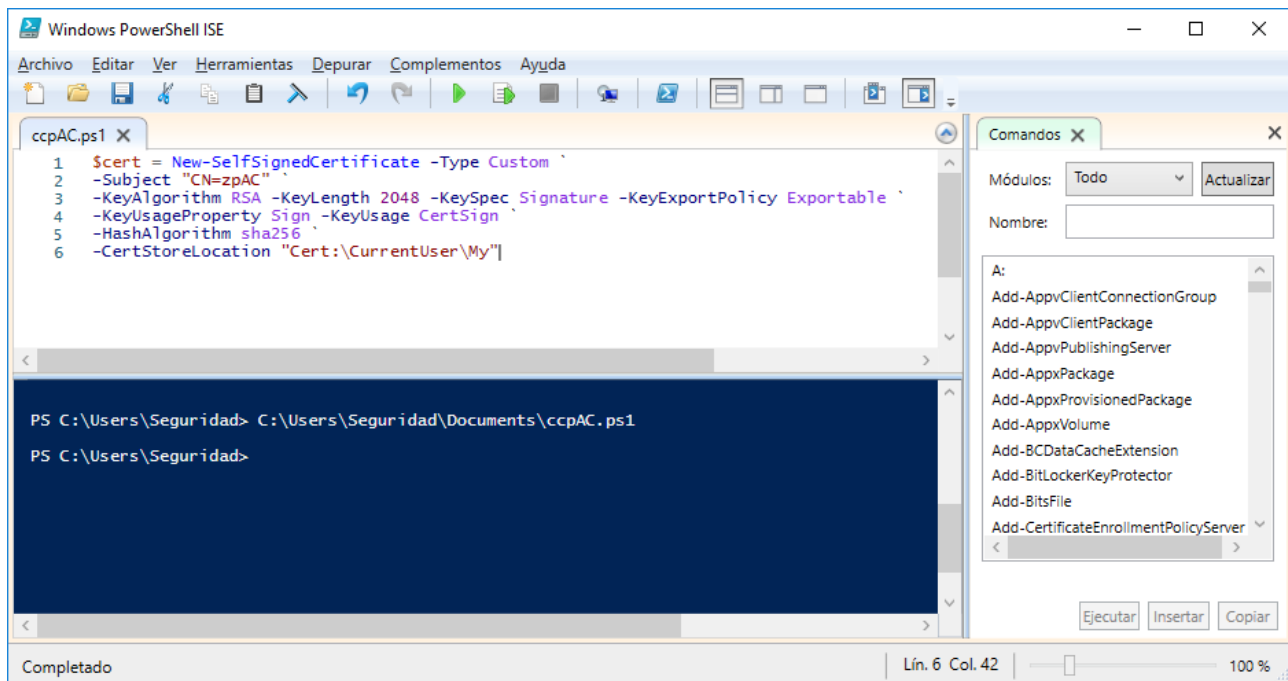
PARA GENERAR UN CERTIFICADO RAÍZ

Se puede utilizar el siguiente script:

```
$cert = New-SelfSignedCertificate -Type Custom `
-Subject "CN=zpAC" `
-KeyAlgorithm RSA -KeyLength 2048 -KeySpec Signature -KeyExportPolicy Exportable `
-KeyUsageProperty Sign -KeyUsage CertSign `
-HashAlgorithm sha256 `
-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 utilizar el carácter ` (acento invertido) como indicador de continuación de línea.
La imagen siguiente muestra la edición del script en el ISE y su ejecución:



Esta figura muestra la edición del script ccpAC.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 clave para la propiedad de "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.

-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.

-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.

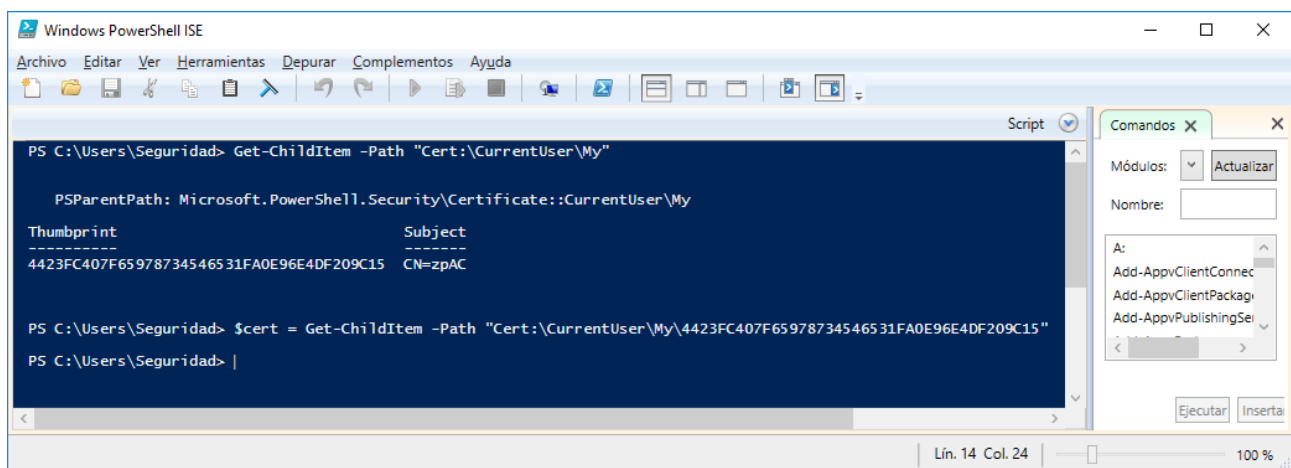
Utiliza la herramienta certmgr.msc para comprobar que el certificado emitido para zpAC está en el almacén de certificados "Personal". Este almacén NO es el apropiado para contener el certificado de una autoridad certificadora. Pero recordar que este certificado y su clave asociada se usarán para crear otros certificados, y no como raíz de confianza en el computador.

Exportar el certificado y su clave privada asociada al fichero zpAC.pfx.

Exportar solo el certificado, sin su clave privada, al fichero zpAC.cer.

PARA GENERAR UN CERTIFICADO DE USUARIO

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:



```
PS C:\Users\Seguridad> Get-ChildItem -Path "Cert:\CurrentUser\My"

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                               Subject
-----
4423FC407F65978734546531FA0E96E4DF209C15  CN=zpAC

PS C:\Users\Seguridad> $cert = Get-ChildItem -Path "Cert:\CurrentUser\My\4423FC407F65978734546531FA0E96E4DF209C15"
PS C:\Users\Seguridad> |
```

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

Ahora se puede generar un certificado de usuario con el siguiente script:

```
$cert = New-SelfSignedCertificate -Type Custom -DnsName zpUSU `
-Subject "CN=zpUSU" `
-KeyAlgorithm RSA -KeyLength 2048 -KeySpec Signature -KeyExportPolicy Exportable `
-HashAlgorithm sha256 `
-Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)" `
-CertStoreLocation "Cert:\CurrentUser\My"
```

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

```

ccpUsu.ps1
1 New-SelfSignedCertificate -Type Custom `
2 -Subject "CN=zpUSU" -DnsName "www.zpUSU.com", "www.zpUSU.es" `
3 -KeyAlgorithm RSA -KeyLength 2048 -KeySpec Signature -KeyExportPolicy Exportable `
4 -HashAlgorithm sha256 `
5 -Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)" `
6 -CertStoreLocation "Cert:\CurrentUser\My"

PS C:\Users\Seguridad> C:\Users\Seguridad\Documents\ccpUsu.ps1

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                               Subject
-----
51624CCA6F16C59A92B332C0AEB180780CBDCAD7 CN=zpUSU

PS C:\Users\Seguridad>
  
```

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=www.zpUSU.com" y "Nombre DNS=www.zpUSU.es".

-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: Especifica un array de extensiones del certificado, en forma de cadenas de caracteres. Cada cadena debe emplear uno de estos formatos:

- oid={hex}CadenaHexadecimal
- oid={text}Cadena

El valor oid identifica el objeto de la extensión y la cadena contiene una representación hexadecimal o textual del valor de la extensión.

En el script anterior oid=2.5.29.37 que representa "Enhanced Key Usage" y Cadena=1.3.6.1.5.5.7.3.2 que representa "Client Authentication".

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

Exportar el certificado y su clave privada asociada al fichero zpUSU.pfx.

El comando New-SelfSignedCertificate permite generar certificados para firmar datos usando el parámetro -KeySpec Signature, pero no permite fácilmente generar certificados para cifrar datos usando el parámetro -KeySpec KeyExchange.