



COMPROBACION DE LA CRL EN LA CLAVE PÚBLICA

1. Índice

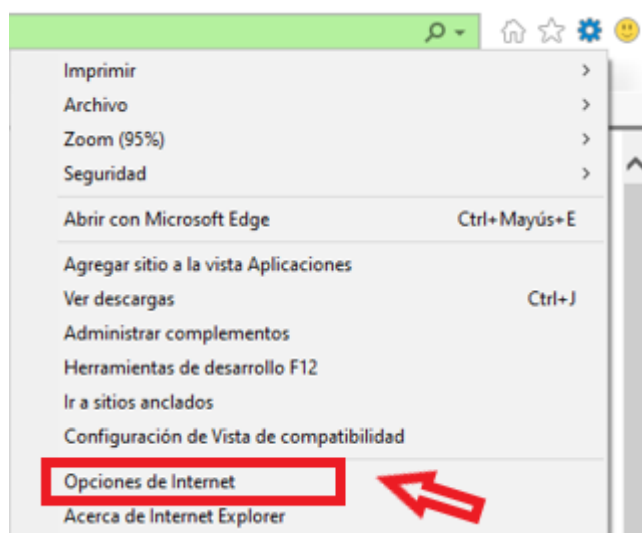
Índice	2
Objetivo del documento	3
¿Cómo descargarse la clave pública?.....	3
Comprobación de la CRL	7
Acciones a tomar cuando la CRL muestra el certificado como caducado	10

2. Objetivo del documento

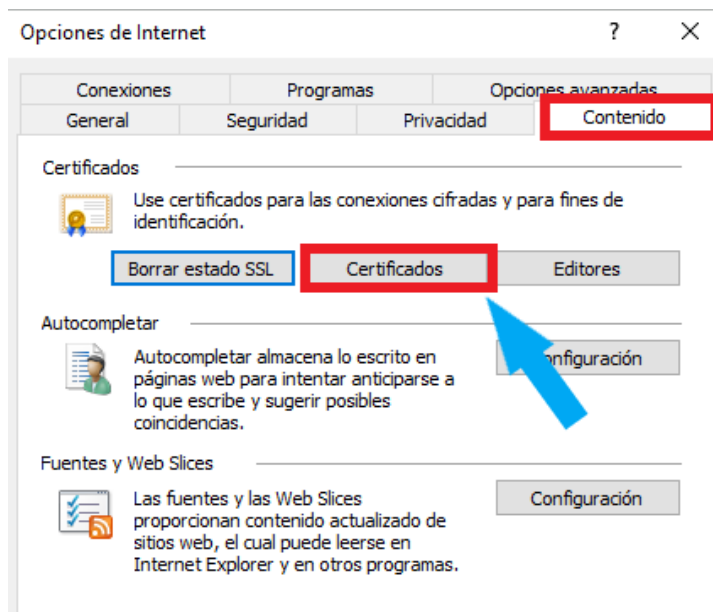
El objetivo de este documento es identificar si un certificado está revocado, comprobando que el certificado aparece en la lista de revocados, o CRL, descargándose la clave pública del propio certificado.

3. ¿Cómo descargarse la clave pública?

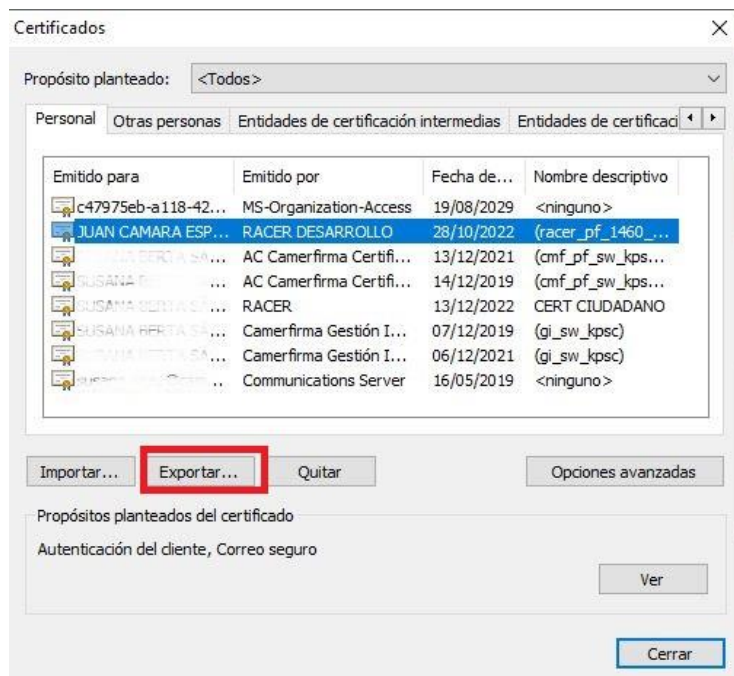
Lo primero de todo es descargarse la clave pública del certificado, para ello tenemos que ir al almacén de Windows. Desde Internet Explorer, vamos a Herramientas  y seleccionamos “Opciones de internet”



Posteriormente tendríamos que irnos a la pestaña “Contenido” y seleccionamos “Certificados”



Nos aparece una ventana como esta, en la que aparecen todos los certificados instalados en el almacén de Windows. Para exportar la clave pública, nos ponemos encima del certificado seleccionado y damos a “Exportar”



A continuación, tendríamos que seguir el asistente para exportar certificados:

←  Asistente para exportar certificados

✕

Este es el Asistente para exportar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde un almacén de certificados a su disco.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Haga clic en Siguiente para continuar.

Siguiente

Cancelar

Seleccionamos “No exportar la clave privada” y damos a “Siguiente”:

←  Asistente para exportar certificados

✕

Exportar la clave privada

Puede elegir la exportación de la clave privada con el certificado.

Las claves privadas se protegen con contraseñas. Si desea exportar la clave privada con el certificado, debe escribir una contraseña en una página posterior.

¿Desea exportar la clave privada con el certificado?

☐ Exportar la clave privada

☒ No exportar la clave privada

Nota: la clave privada asociada está marcada como no exportable. Solamente puede exportarse el certificado.

Siguiente

Cancelar

En la siguiente pantalla seleccionamos el formato a usar. En este caso seleccionamos “DER binario codificado X.509 (.CER)”, aunque también nos valdría si seleccionamos “X.509 codificado base 64 (.CER)”. Seguimos con el asistente.

← Asistente para exportar certificados

×

Formato de archivo de exportación

Los certificados pueden ser exportados en diversos formatos de archivo.

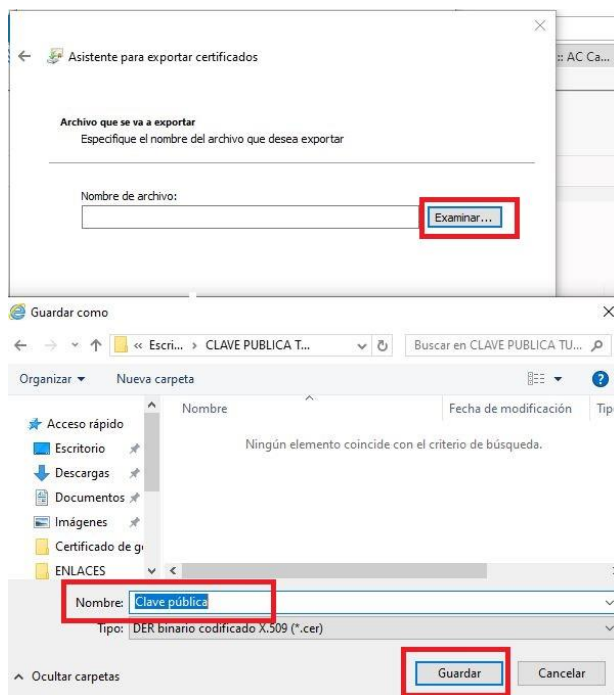
Seleccione el formato que desea usar:

- ☒ DER binario codificado X.509 (.CER)
- ☐ X.509 codificado base 64 (.CER)
- ☐ Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
- ☐ Incluir todos los certificados en la ruta de certificación (si es posible)
- ☐ Intercambio de información personal: PKCS #12 (.PFX)
- ☐ Incluir todos los certificados en la ruta de certificación (si es posible)
- ☐ Eliminar la clave privada si la exportación es correcta
- ☐ Exportar todas las propiedades extendidas
- ☐ Habilitar privacidad de certificado
- ☐ Almacén de certificados en serie de Microsoft (.SST)

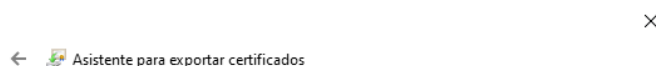
Siguiente

Cancelar

En la siguiente ventana tenemos que guardar el fichero exportado, para ello, pinchamos en el botón “Examinar”, localizamos la ubicación donde queremos guardarlo y le ponemos un nombre. A continuación, damos a “Guardar”



Seguimos con el asistente y en la siguiente ventana que nos aparece, tendríamos que dar a “Finalizar”:

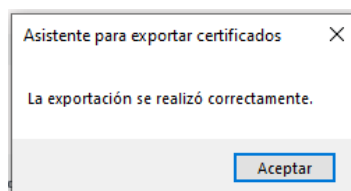
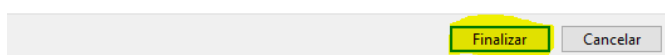


Finalización del Asistente para exportar certificados

El Asistente para exportar certificados se completó correctamente.

Especifiqué la siguiente configuración:

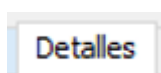
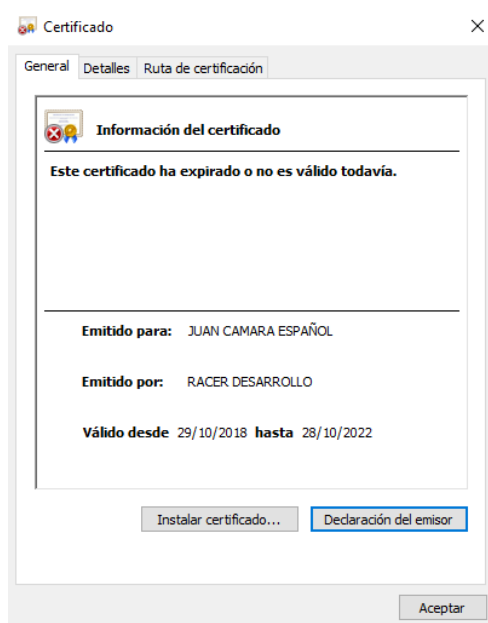
Nombre de archivo	C:\Users\susanar\Desktop\C
Exportar claves	No
Incluir todos los certificados en la ruta de certificación	No
Formato de archivo	DER binario codificado X.509 (



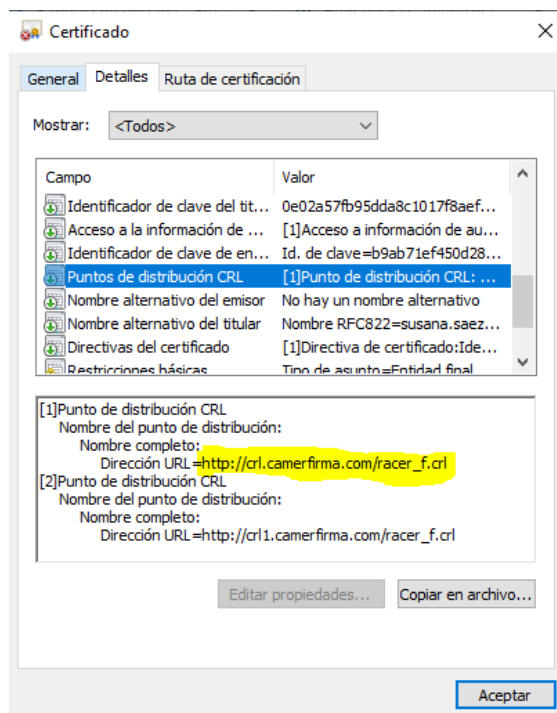
Ya tendríamos exportada la clave pública.

4. Comprobación de la CRL

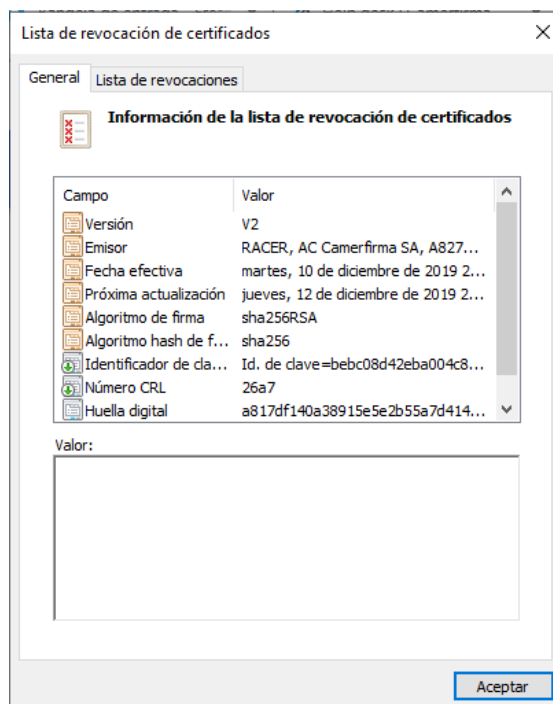
Una vez que tenemos la clave pública del certificado (se le habrá generado un archivo con extensión .cer o .crt) si la ejecutamos para ver los detalles del certificado, nos aparecerá así:



Tenemos que pinchar en la pestaña **Detalles** para poder ver todos los campos del certificado. Tenemos que localizar el Campo “Puntos de distribución CRL” y copiar la primera dirección URL (en este ejemplo sería la que está seleccionada)



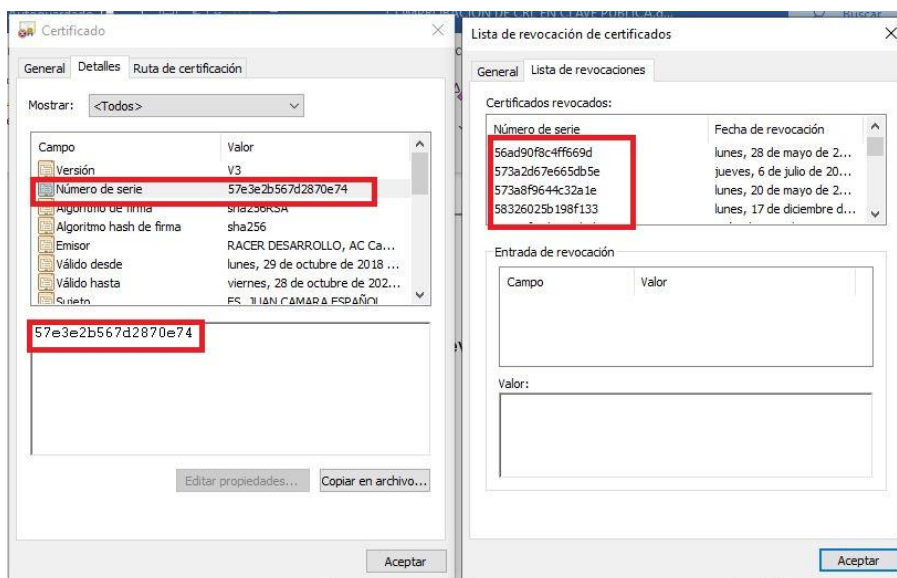
Pegamos dicha dirección URL en un navegador cualquiera y se descarga la “Lista de revocación de certificados”. Un fichero como el siguiente:



Nos vamos a la pestaña “Lista de revocaciones” y comparamos con el campo “Número de serie” de la clave pública. Si dicho número de serie **no** aparece en la Lista de revocaciones es que el certificado **no** está revocado.

Si el número de serie, **si** aparece en la Lista de revocaciones es que el certificado se encuentra revocado.

El orden de la lista de revocación es haxadecimal, es decir, primero irían los números del 0 al 9 y posteriormente las letras (a, b, c, etc).



5. Acciones a tomar cuando la CRL muestra el certificado como caducado.

Si el número de serie de la clave pública del certificado aparece en la lista de revocaciones, y por tanto, muestra el certificado como revocado, hay que contemplar dos escenarios:

1.- Si al validar el certificado, se sigue mostrando como revocado, tendría que hacer una nueva solicitud, o si lo prefiere, puede ponerse en contacto con el departamento de soporte de Camerfirma.

Para validar el certificado, lo puede hacer de dos maneras:

- (a) A través de Valide Red Sara (<https://valide.redsara.es/valide/validarFirma/ejecutar.html>),
- (b) o bien a través del aplicativo de validación en nuestra web: www.camerfirma.com → Certificados digitales → Utilidades → Validación de certificados → Acceso al servicio de Consulta (plataforma STATUS), (https://secure.camerfirma.com/solicitudes_status/estado_certificado.php)

2.- Si una vez validado el certificado, en Valide o en nuestro aplicativo, aparece como correcto, debe abrirnos una consulta a través de nuestra herramienta de gestión de

incidencias (<https://camerfirma.freshdesk.com/support/tickets/new>) o bien mandar un correo a soporteusuarios@camerfirma.com, explicando toda la casuística, para que lo podamos revisar.