

INSTRUCCIÓN TECNICA SOLICITUD CERTIFICADOS WIN-ACME

USO INTERNO

Elaborado por		CTU - ACS	
Versión	V 1.0	Fecha aprobación	02/2026

 	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

ÍNDICE

ÍNDICE	2
1. Control de Versiones	3
2. Objeto del Documento	3
3. ALCANCE	3
4. REFERENCIAS	3
5. DEFINICIONES	4
6. PROCESO DE SOLICITUD	4
6.1. Protocolo ACME	4
6.2. Configuración ACME en el cliente	4
6.3. Registro	5
6.4. Solicitud de certificado	5
6.5. Renovación de certificado	6
6.6. Revocación de certificado	6
6.7. Listado / Revisión de certificados	6
7. RESPONSABILIDADES	7
7.1. RESPONSABILIDADES SOLICITANTE	7
7.2. RESPONSABILIDADES CTU	7
8. HERRAMIENTAS	7
9. REGISTROS	7

 	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

1. Control de Versiones

Título:	INSTRUCCIÓN TÉCNICA SOLICITUD CERTIFICADOS ACME			
Tipo de documento:	Instrucción Técnica			
Nombre del Fichero:	CER-SCS-IT02-SOLICITUD ACME-WNDOWS.v1.0			
Clasificación:	Uso Interno			
Estado:	APROBADO			
Autor:	CTU - ACS			
Versión:	1.0	Fecha:	02/2026	

Control de cambios

Redactor	Fecha	Descripción de los cambios
FJM y MS	02/2026	Elaboración del documento
Jefe ACS	02/2026	Aprobación del documento

2. Objeto del Documento

El objeto del presente documento es describir el procedimiento de configuración, solicitud y explotación de un certificado de servidor SSL, de modo que se automatice su renovación.

3. ALCANCE

Este procedimiento afecta a todo el personal y a los colaboradores externos que prestan servicio en la UNED, administrando sistemas TIC.

4. REFERENCIAS

- Política de Seguridad
- Normativas de Seguridad y procedimientos de gestión, en especial los procedimientos de criptografía.

 	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

5. DEFINICIONES

N/A

6. PROCESO DE SOLICITUD

6.1. Protocolo ACME

El protocolo ACME nos va a permitir automatizar la emisión de certificados y poder delegar su solicitud, renovación, revocación en los clientes.

Para configurar ACME en el entorno del servicio de certificados, hay dos puntos claves implicados:

- Servicio de Certificados de HARICA (servidor), que permita delegar la gestión de determinados nombres/dominios a los clientes
- Cliente ACME, que es el software necesario instalar en donde se vaya a hacer uso de los certificados finales, y con el que se gestionará el/los certificados que han sido delegados.

Si se quiere ampliar información se pueden visitar las siguientes URL's de interés:

- Enlaces de Harica cuando se realiza la búsqueda en su web por el literal ACME
<https://guides.harica.gr/docs/Guides/Server-Certificate/ACME-Instructions/>
- Servicio de certificados de RedIRIS
<https://www.rediris.es/tcs/doc/hcm/#hcm-acme>

6.2. Configuración ACME en el cliente

Para poder comunicarnos con el servidor de HARICA necesitamos un cliente ACME, los hay para diversos sistemas operativos, vamos a usar 2 para los ejemplos, pero cualquiera de los disponibles es válido.

- CERTBOT: Para sistemas Linux <https://certbot.eff.org/>
- Win-ACME: Para sistemas Windows <https://www.win-acme.com/>

Ambos programas funcionan desde línea de comandos.

Asimismo, hay que realizar la solicitud de alta del sistema a certificar, para ello mandamos un correo a admin.caroot@csi.uned.es, indicando el nombre principal que debe llevar el certificado y los alias, si fuera el caso.

La cuenta del servicio nos enviará un correo con un enlace donde podremos visualizar los siguientes datos:

- Server URL: <https://acme-v02.harica.gr/acme/XXXXXXXXXX/directory>
- Key ID: YYYYYY (es lo mismo que Account ID en otros sistemas)
- HMAC Key: ZZZZZZZZ

Estos son necesarios para más adelante registrar una cuenta de correo con HARICA y que así podamos solicitar, descargar y manejar certificados.

	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

Además necesitaremos tener el dominio en el DNS creado para que una vez instalado poder utilizarlo, por lo que si se trata de un nuevo servidor lo primero es pedir el alta en DNS.

6.3. Registro

Una vez tenemos los datos, para darnos de alta en el servidor que gestiona los certificados tenemos que registrar una cuenta de correo, que irá asociada a los datos que nos han proporcionado en el paso anterior, de forma que en adelante esa cuenta de correo nos asocie al dominio que queremos certificar. Una vez hacemos este paso luego los siguientes comandos no requieren usar ningún tipo de autenticación, únicamente la cuenta de correo que hemos asociado.

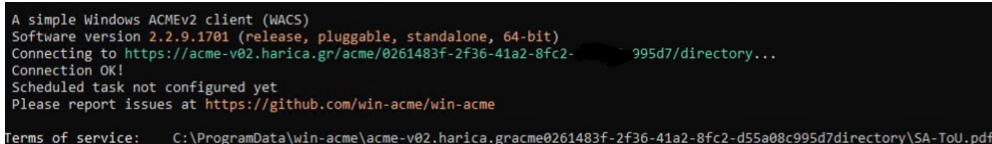
Para el registro ejecutamos desde línea de comandos:

WinACME. Para crear el comando se recomienda apoyarse en el block de notas:

```
> wacs.exe --register --baseuri "SERVER URL se conservan las comillas" --accepttos --emailaddress XXXX@XXXX.uned.es --eab-key-identifier "Key ID sin comillas" --eab-key " sin comillas" --account nombre_cuenta
```

* eab-key-identifier= No son las Xs, hay que escribir el Key-ID

** eab-key = No son las Ys, hay que escribir el HMAC Key



```
A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.harica.gr/acme/0261483f-2f36-41a2-8fc2-d55a08c995d7/directory...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme
Terms of service: C:\ProgramData\win-acme\acme-v02.harica.gr\acme\0261483f-2f36-41a2-8fc2-d55a08c995d7\directory\SA-ToU.pdf
```

En estos comandos es importante poner en el campo 'email' la cuenta de correo que queremos asociar a las solicitudes y en el campo 'account' será un alias de la cuenta.

6.4. Solicitud de certificado

Una vez estamos registrados en HARICA se puede lanzar la petición para que nos hagan llegar el certificado. Hay que especificar el nombre del dominio y la cuenta de correo. Para poder tener un fácil manejo se recomienda ponerle un nombre fácil de recordar

WinACME para un solo dominio:

```
> wacs.exe --source manual --commonname nombredominio.uned.es --host nombredominio.uned.es --friendlyname (nombre, por lo general se pondrá el FQDN y sin comillas) --baseuri "ACME URL" --accepttos --emailaddress XXXX@XXXX.uned.es --account nombre_cuenta
```

Para varios dominios los escribimos los nombres separados por comas y entre comillas en hosts, además incluiremos --san:

```
wacs.exe --source manual --commonname nombredominio1.uned.es --host "nombredominio1.uned.es,nombredominio2.uned.es,alias.uned.es" --friendlyname nombredominio1.uned.es --baseuri "ACME URL" --accepttos --emailaddress XXXX@uned.es --account nombre_cuenta --san
```

El comando de arriba deberá dejar el certificado en el almacén por defecto, pero es posible configurar el directorio en el archivo Settings.json.

 	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

Alternativamente, en especial si lo ejecutamos en un servidor distinto a donde esta el IIS, podremos dejarlo en fichero PFX, para ello añadimos los comandos: --pfxfilepath, --pfxfilename, --store pfxfile y --pfxpassword.

```
wacs.exe --source manual --commonname servidor.uned.es --host servidor.uned.es --friendlyname
servidor.uned.es --baseuri "https://acme-v02.harica.gr/acme/0261443f-2f36-42a2-8fc2-
000000000000/directory" --accepttos --emailaddress cuenta@csi.uned.es --account "nombre que le dimos
sin comillas" --store pfxfile --pfxfilepath D:\ --pfxfilename nombre_fichero
```

Una vez ejecutado nos informará de las acciones ejecutadas:

```
A simple Windows ACMEv2 client (WACS)
Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.harica.gr/acme/0261483f-2f36-41a2-8fc2-88c995d7/directory...
Connection OK!
Scheduled task looks healthy
Please report issues at https://github.com/win-acme/win-acme
Running in mode: Unattended
Source generated using plugin Manual: calificaciones-des.a.uned.es
Using account calificaciones-des.a
Overwriting previously created renewal

Plugin Manual generated source calificaciones-des.a.uned.es with 1 identifiers
Plugin Single created 1 order
Renewing calificaciones-des.a.uned.es
Using cache for calificaciones-des.a.uned.es. To get a new certificate within 1 days, run with --nocache.
Store with PfxFile...
Copying certificate to the pfx folder D:\calificaciones-des.a.uned.es.pfx
Scheduled task looks healthy
Next renewal due after 2026/3/26
Certificate calificaciones-des.a.uned.es created
```

WinACME para varios nombres de dominio:

```
> wacs.exe --source manual --commonname nombredominio.uned.es --host
nombredominio.uned.es,nombre2.uned.es,nombre3.uned.es --friendlyname ""nombre, por lo general se
pondrá el FQDN principal sin comillas" --baseuri "ACME URL" --accepttos --emailaddress
XXXX@XXXX.uned.es --account nombre_cuenta
```

6.5. Renovación de certificado

El certificado que nos bajemos tendrá 1 año de validez, a partir del 15 de marzo de 2026 será de 200 días, el mismo día de 2027 bajará a 100 días. La renovación la podemos hacer de forma autónoma con el cliente ACME.

WinACME:

```
> wacs.exe --renew --baseuri "ACME URL"
```

6.6. Revocación de certificado

En caso de que ya no sea necesario hay que revocar el certificado.

WinACME:

```
> wacs.exe --revoke --baseuri "ACME URL"
```

6.7. Listado / Revisión de certificados

Para revisar que todo está dado de alta de forma correcta.

WinACME:

```
> wacs.exe --list --baseuri "ACME URL"
```

 	Título	Código	Fecha	Versión
	IT SOLICITUD CERTIFICADOS WIN-ACME	CER-SCS-IT02	02/2026	V1.0

7. RESPONSABILIDADES

7.1. RESPONSABILIDADES SOLICITANTE

Hacer el encargo al CTU de dar de alta una instancia ACME en el sistema de la CA, mandando un correo a la cuenta admin.caroot@csi.uned.es. En el correo comunicará el nombre principal del certificado y los alias si estos fueran necesarios.

Mediante el cliente ACME correspondiente registrar la instancia en el sistema ACME de la CA y descargar e instalar los certificados.

Una vez instalados deberán realizar la prueba de SSL Labs, se ha de conseguir como mínimo la calificación A, en la dirección: [https:// www.ssllabs.com/ssltest](https://www.ssllabs.com/ssltest)

Comunicar al CTU en caso de que cambie el responsable o la cuenta de correo asociadas a un certificado.

7.2. RESPONSABILIDADES CTU

El CTU será el encargado de dar de alta el ACME correspondiente a uno o varios nombres de dominio configurando la instancia en la CA.

Una vez dada de alta la instancia proporcionará los datos al solicitante desde pwpush.csi.uned.es.

Registrar y eliminar la instancia de los certificados revocados que hayan sido comunicados por el solicitante.

Dar soporte y asistencia técnica, así como ayudar a resolver las problemáticas.

8. HERRAMIENTAS

- Jira como gestor de solicitudes
- Cliente ACME

9. REGISTROS

- Registro de solicitudes de Jira.