

INSTRUCCIÓN TECNICA SOLICITUD CERTIFICADOS ACME - CERTBOT

USO INTERNO

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

 	Título	Código	Fecha	Versión
	Procedimiento de Control de acceso físico	INF-CLA-PG	21/11/19	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 del certificado en el proveedor	5
6.4. Solicitud de certificado	6
6.5. Renovación de certificado	6
6.6. Revocación de certificado	7
6.7. Listado / Revisión de certificados	7
7. RESPONSABILIDADES	7
7.1. RESPONSABILIDADES SOLICITANTE	7
7.2. RESPONSABILIDADES CTU	7
8. HERRAMIENTAS	8
9. REGISTROS	8
10. ANEXOS	8
10.1. Ejemplo de SCRIPT para automatizar la renovación	8

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

1. CONTROL DE VERSIONES

Título:	INSTRUCCIÓN TECNICA SOLICITUD CERTIFICADOS ACME CERTBOT			
Tipo de documento:	Instrucción Técnica			
Nombre del Fichero:	CER-SCS-IT02-SOLICITUD ACME-CERTBOT.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, en sistemas Linux, utilizando el software CERTBOT.

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
	SOLICITUD CERTIFICADOS ACME - CERTBOT	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, al mismo tiempo que se realiza la solicitud al CAU, 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: ZZZZZZZZZ

Estos son necesarios para más adelante registrar una cuenta de correo con HARICA y que así podamos solicitar, descargar y manejar certificados. Se recomienda no utilizar cuentas personales, preferentemente asociadas al servicio, departamento o similares.

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.

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

6.3. Registro del certificado en el proveedor

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:

Certbot:

```
# certbot register --email XXXX@XXX.uned.es --server "https://acme-
v02.harica.gr/acme/XXXXXXXXXX/directory"* --eab-kid Aquí_pondremos_key_ID --eab-hmac-
key YYYYYYYY ** Aquí_el_valor_de_HMAC_Key
```

* 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

```
Ej: certbot register --email correo@buzon.uned.es --server "https://acme-
v02.harica.gr/acme/835666tgg-d236ggh6--4453g7-ac2523fb16266/directory" --eab-kid
677Vfg735LwmasdfaASDFTb --eab-hmac-key vw47sWGBsffcvEpFD-
r9PasfgsgSFGfgaggsuKI1asfWFQAGSAFGA
```

Una vez ejecutado te pregunta si estas de acuerdo con los términos y condiciones, le decimos Y. Luego te preguntará si quieres formar parte de las estadísticas, le decimos N. Por último, en que directorio te ha dejado el certificado.

```
# certbot register --email correo@buzon.uned.es --server "https://acme-
v02.harica.gr/acme/835666tgg-d236ggh6--4453g7-ac2523fb04566/directory" --eab-kid
677Vfg735LwmasdfaASDFTb --eab-hmac-key vw47sWGBsffcvEpFD-
r9PasfgsgSFGfgaggsuKI1asfGFSAGSAFGA
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-----
Please read the Terms of Service at: https://repo.harica.gr/documents/SA-ToU.pdf
You must agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: Y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
Account registered.
```

En estos comandos es importante poner en el campo 'email' la cuenta de correo (se recomienda utilizar una asociada al servicio evitando las personales) que queremos asociar a las solicitudes y en el campo 'account' será un alias de la cuenta.

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

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

Certbot para un solo dominio:

```
# certbot certonly --standalone --agree-tos --email XXXX@XXXX.uned.es --server "ACME URL" --domain nombredominio.uned.es --cert-name nombre (ALIAS o nombre amigable para identificarlo)
```

```
Ej: certbot certonly --standalone --agree-tos --email correo@buzon.uned.es --server "https://acme-v02.harica.gr/acme/835636tgg-d236ggh6--4453g7-textoNoValido2523fb041234/directory" --domain dominio.uned.es --cert-name alias
```

Certbot para varios dominios, los ponemos seguidos separados por coma:

```
# certbot certonly --standalone --agree-tos --email XXXX@XXXX.uned.es --server "ACME URL" --domain nombredominio.uned.es,nombre2.uned.es,nombre3.uned.es --cert-name nombre
```

```
# certbot certonly --standalone --agree-tos --email correo@buzon.uned.es --server "https://acme-v02.harica.gr/acme/835636tgg-d236ggh6--4453g7-ac2523- directory" --domain dominio.uned.es --cert-name alias
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for dominio.uned.es

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/dominio/fullchain.pem
Key is saved at: /etc/letsencrypt/live/dominio/privkey.pem
This certificate expires on 2027-01-01.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.
```

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.

Certbot:

```
# certbot renew --cert-name nombre (alias que consignamos en el registro)
```

```
# certbot renew --cert-name dominio
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-----
Processing /etc/letsencrypt/renewal/dominio.conf
-----
Certificate not yet due for renewal

-----
The following certificates are not due for renewal yet:
/etc/letsencrypt/live/dominio/fullchain.pem expires on 2027-01-01 (skipped)
No renewals were attempted.
-----
```

En este ejemplo el sistema avisa de que aún no es necesario renovar, solo emitirá nuevos certificados cuando estén cerca de caducar.

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

6.6. Revocación de certificado

En caso de que ya no sea necesario hay que revocar el certificado, para ello el responsable ejecutará:

```
Certbot:
# certbot revoke --cert-name nombre
```

Asimismo, se mandará un correo avisando al CTU para que lo registrará.

6.7. Listado / Revisión de certificados

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

```
Certbot:
# certbot certificates
```

```
# certbot certificates
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-----
Found the following certs:
Certificate Name: dominio
Serial Number: 1a313ffsfgg2b4674748b2835[redacted]af
Key Type: ECDSA
Domains: dominio.uned.es
Expiry Date: 2027-01-01 12:31:48+00:00 (VALID: 364 days)
Certificate Path: /etc/letsencrypt/live/dominio/fullchain.pem
Private Key Path: /etc/letsencrypt/live/dominio/privkey.pem
-----
```

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, los alias si estos fueran necesarios y la cuenta de correo electrónico.

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.

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

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.

8. HERRAMIENTAS

- Jira como gestor de solicitudes
- Cliente ACME
- Mozilla SSL Configurator: <https://ssl-config.mozilla.org/>
Web para crear el fichero de configuración del TLS, para los sistemas: Apache, AWS ALB, AWS ELB, Caddy, Coturn, Dovecot, Exim, Go, HAProxy, Jetty, lighttpd, MySQL, nginx, Oracle HTTP, Postfix, PostgreSQL, ProFTPD, Redis, Squid, stunnel, Tomcat y Traefik.

9. REGISTROS

- Registro de solicitudes de Jira.
- Registro de los certificados emitidos.

10. ANEXOS

10.1. Ejemplo de SCRIPT para automatizar la renovación

Un ejemplo de Script a poner en el CRON y que diariamente miré a las 3 horas si es necesario renovar cuando quedan 2 días de vida del certificado:

```
#!/bin/bash

# Script: renew_if_2_days_left.sh

# Description: Chequea si el certificado SSL expira in 2 días o menos, lo renueva y manda notificación por correo.

# Variables a configurar

# En el script habría que cambiar:

# DOMAIN="tu-dominio.com"

# TO_EMAIL="destinatario@correo.com"

# FROM_EMAIL=remite@correo.com

# CERT_PATH

DOMAIN="tu-dominio.com"

CERT_PATH="/etc/.../$DOMAIN/cert.pem"

TO_EMAIL="destinatario@correo.com"

FROM_EMAIL="remite@correo.com"

LOG_FILE="/var/log/certbot-renew.log"

# Calcular días hasta la expiración
```

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

```

EXPIRY_DATE=$(openssl x509 -enddate -noout -in $CERT_PATH | cut -d= -f2)
DAYS_LEFT=$(( ( $(date -d "$EXPIRY_DATE" +%s) - $(date +%s) ) / 86400 ))

# Chequear si quedan 2 o menos días
if [ $DAYS_LEFT -le 2 ]; then
    echo "$(date): El certificado para $DOMAIN expira en $DAYS_LEFT días. Intentando renovarlo..." >> $LOG_FILE
    certbot renew --quiet >> $LOG_FILE 2>&1
    if [ $? -eq 0 ]; then
        SUBJECT="Certbot renovó el certificado exitosamente para el dominio $DOMAIN"
        BODY="El certificado SSL para $DOMAIN fue renovado exitosamente. Tenía $DAYS_LEFT días aún antes de la
caducidad."
    else
        SUBJECT="Certbot falló en la renovación del certificado de $DOMAIN"
        BODY="EL certificado SSL para el dominio $DOMAIN no pudo ser renovado. Le quedan $DAYS_LEFT días para su
caducidad. Revisar el registro de logs en $LOG_FILE."
    fi
    echo "$BODY" | mail -s "$SUBJECT" -r "$FROM_EMAIL" "$TO_EMAIL"
else
    echo "$(date): El certificado para $DOMAIN es válido para $DAYS_LEFT días más. No es necesaria su renovación." >>
$LOG_FILE
fi

```