



Actividad 5 - Certificado HTTPS

ÍNDICE

Crear la entidad.....	3
Crear el certificado.....	4
Instalar el certificado.....	5
Crear un sitio con el nuevo certificado.....	6

Crear la entidad.

Descarga mkcert desde [Github](#)

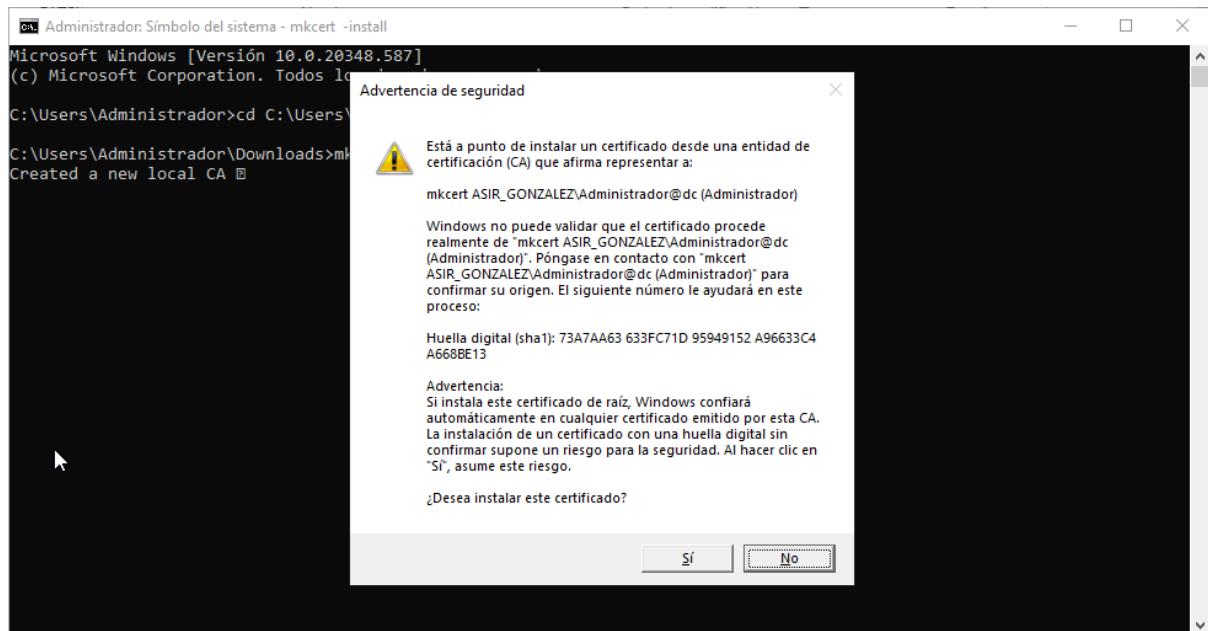
The screenshot shows the 'Assets' section of a GitHub repository for 'mkcert'. It lists nine items:

File	Size	Last Updated
mkcert-v1.4.4-darwin-amd64	5.06 MB	Apr 26, 2022
mkcert-v1.4.4-darwin-arm64	4.93 MB	Apr 26, 2022
mkcert-v1.4.4-linux-amd64	4.57 MB	Apr 26, 2022
mkcert-v1.4.4-linux-arm	4.54 MB	Apr 26, 2022
mkcert-v1.4.4-linux-arm64	4.42 MB	Apr 26, 2022
mkcert-v1.4.4-windows-amd64.exe	4.67 MB	Apr 26, 2022
mkcert-v1.4.4-windows-arm64.exe	4.43 MB	Apr 26, 2022
Source code (zip)		Apr 26, 2022
Source code (tar.gz)		Apr 26, 2022

Ve a la carpeta contenedora y abre un terminal.

Escribe:

```
mkcert -install
```



Si abres la utilidad certmgr, podrás ver que se ha añadido una nueva entidad.

The screenshot shows the Windows Certificates Management (certmgr) window. The left pane displays a tree view of certificates under 'Certificados - Usuario actual'. The right pane is a grid showing detailed information for each certificate, including issuer, expiration date, and purpose. A new certificate, 'mkcert ASIR_GONZALEZ\Administr...', has been added and is highlighted in blue.

Emitido para	Emitido por	Fecha de expir...	Propósitos plantea...	Nombre descriptivo
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02/08/2028	Autenticación del c...	VeriSign Class 3 Pu...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Impresión de fecha	Microsoft Timesta...
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Autenticación del c...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Autenticación del c...	DigiCert Global Roo...
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Autenticación del c...	DigiCert Global Roo...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01/01/2000	Correo seguro, Fir...	Microsoft Authenti...
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<Todos>	Microsoft ECC Prod...
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	27/02/2043	<Todos>	Microsoft ECC TS R...
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<Todos>	Microsoft Root Aut...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/05/2021	<Todos>	Microsoft Root Cert...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<Todos>	Microsoft Root Cert...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	22/03/2036	<Todos>	Microsoft Root Cert...
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	22/10/2039	<Todos>	Microsoft Time Sta...
mkcert ASIR_GONZALEZ\Adminis...	mkcert ASIR_GONZALEZ\Administr...	19/11/2035	<Todos>	<Ninguno>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	08/01/2004	Impresión de fecha	VeriSign Time Stam...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15/03/2032	Firma de código	<Ninguno>
Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Impresión de fecha	Thawte Timestampi...

Crear el certificado.

Para crear el certificado basta con que escribas en la misma terminal de antes:

```
mkcert -pkcs12 localhost
```

o bien, el nombre de dominio que uses, por ejemplo

```
mkcert -pkcs12 web.local
```

```
C:\Users\Administrador\Downloads>mkcert -pkcs12 localhost
Created a new certificate valid for the following names ⓘ
- "localhost"

The PKCS#12 bundle is at "./localhost.p12" ⓘ

The legacy PKCS#12 encryption password is the often hardcoded default "changeit" ⓘ
It will expire on 19 February 2028 ⓘ
```

La contraseña será “changeit”.

Instalar el certificado.

En la carpeta donde ejecutaste mkcert, se habrá generado un archivo, hazle doble click

▼ hoy (2)

localhost.p12	19/11/2025 9:26	Personal Informati...	4 KB
mkcert.exe	19/11/2025 9:02	Aplicación	4.782 KB

Sigue el asistente.

Elige "Equipo local"

Este es el Asistente para importar certificados

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

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.

Ubicación del almacén

- Usuario actual
 Equipo local

Haga clic en Siguiente para continuar.

Escribe la contraseña anterior.

Escriba la contraseña para la clave privada.

Contraseña:

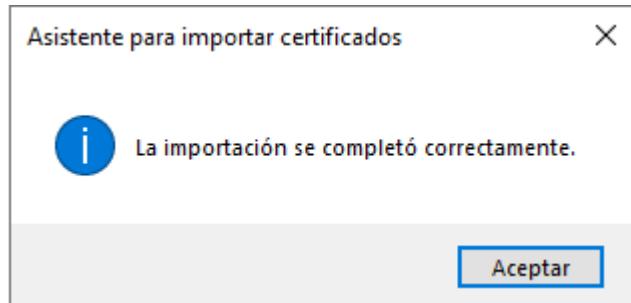
changeit

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.
- Proteger la clave privada mediante security(Non-exportable) basada en virtualizado
- Incluir todas las propiedades extendidas.

Si todo está bien, te saldrá el siguiente mensaje:



Ahora ve al panel de IIS y comprueba que puedas ver el certificado.

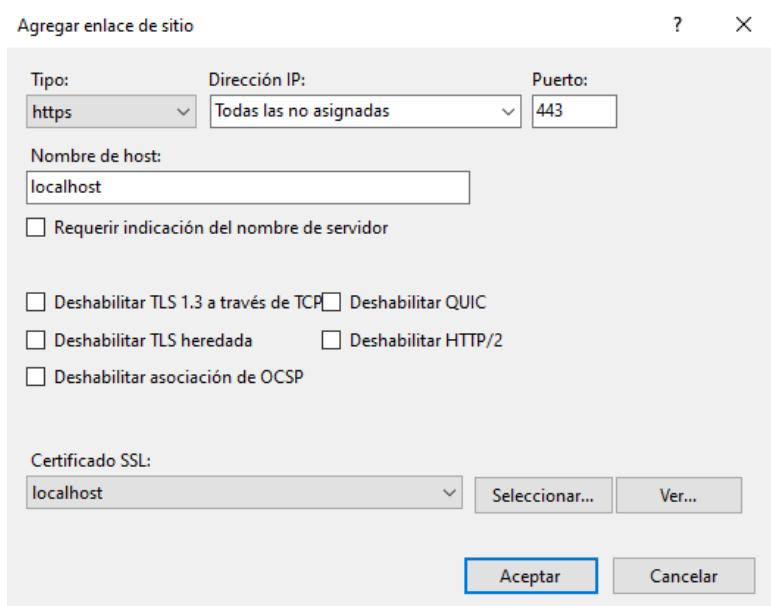
The screenshot shows the 'Certificados de servidor' (Server Certificates) section in the IIS Manager. It displays a table with one certificate entry:

Filtro:	Ir	Mostrar todo	Agrupar por:	Sin agrupar
Nombre		Emitido para	Emitido por	Fec
		localhost	mkcert ASIR_GONZALEZ\Ad...	19/

Crear un sitio con el nuevo certificado.

Crea o modifica un sitio en IIS y añade el certificado,

Si eliges añadir el certificado a una web existente, añade un nuevo enlace.



Opcionalmente, puedes marcar la opción de “Requerir SSL”, para obligar al usuario a que use https

Esta página permite modificar la configuración

Requerir SSL

Certificados de cliente:

- Omitir
- Aceptar
- Requerir



Comprobación: si accedes al sitio web desde el propio servidores verás que puedes acceder correctamente, y no tendrás el aviso de no seguro, ya que contamos con la entidad

The screenshot shows a browser window with the address bar displaying `https://localhost`. The main content area shows the standard "Welcome" page from IIS, which includes text in English, Japanese, and Portuguese. Overlaid on this is a "Visor de certificados: localhost" (Certificate Viewer) dialog box. The dialog box has tabs for "General" and "Detalles", with "General" selected. The "General" tab displays the following information:

Emitido para	
Nombre común	localhost
Organización (O)	mkcert development certificate
Unidad organizativa (UO)	ASIR_GONZALEZ\Administrador@dc (Administrador)

The "Detalles" tab displays the following information:

Emitido por	
Nombre común	mkcert ASIR_GONZALEZ\Administrador@dc (Administrador)
Organización (O)	mkcert development CA
Unidad organizativa (UO)	ASIR_GONZALEZ\Administrador@dc (Administrador)

Below these, under "Período de validez", it shows:

Emitido el	miércoles, 19 de noviembre de 2025, 9:26:35
Fecha de expiración	sábado, 19 de febrero de 2028, 9:26:35

At the bottom, it shows "Huellas digitales de SHA-256" with two rows of hexidecimal values:

Certificado	f9352c682023b93f6eab20ab8894fa2516b88e19e9f93ddc470be9 34a8b6161c
Clave pública	3c2984f1a5cb426fb4e045d34dd835216479e84fc178ebc903351 71ef58663d

En cambio, si lo haces desde una máquina que no tenga la entidad instalado, te dirá que no es seguro

