Práctica 3.1 HTTP HTTPS

Ramón Moreno Albert 2ª DAW semipresencial

Ejercicio 1. Encuentra 2 APIs gratuitas y realiza alguna prueba con POSTMAN (o software similar):

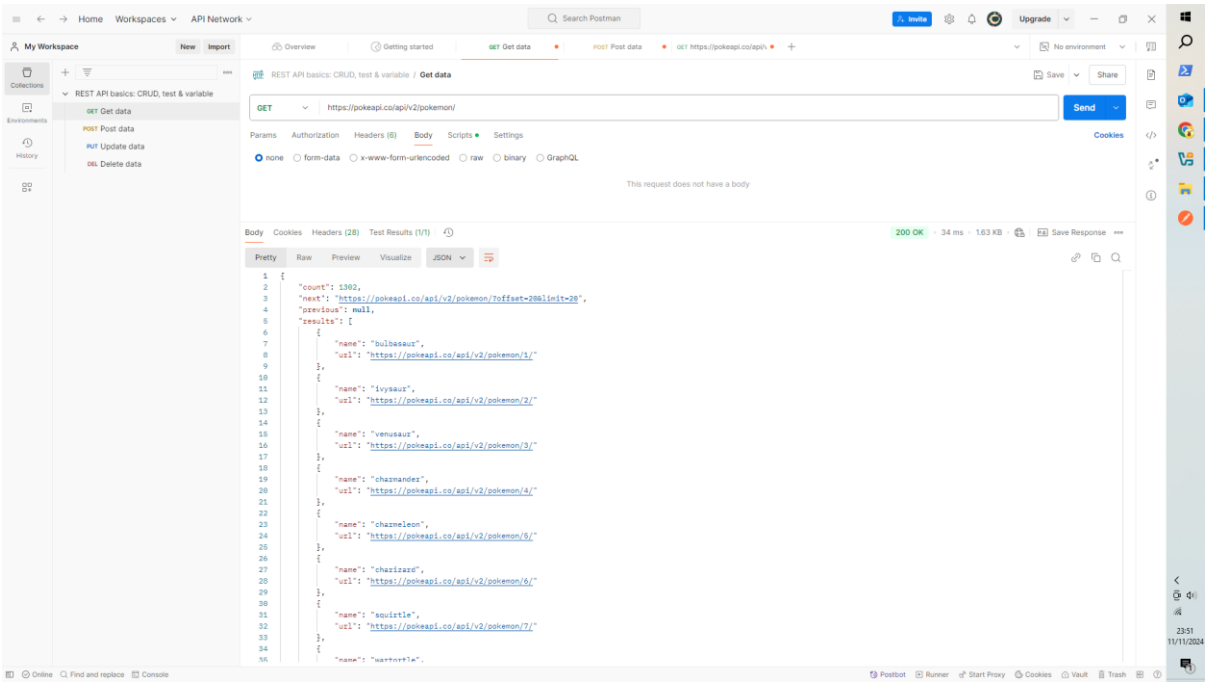
Explica brevemente qué ofrece cada API encontrada.

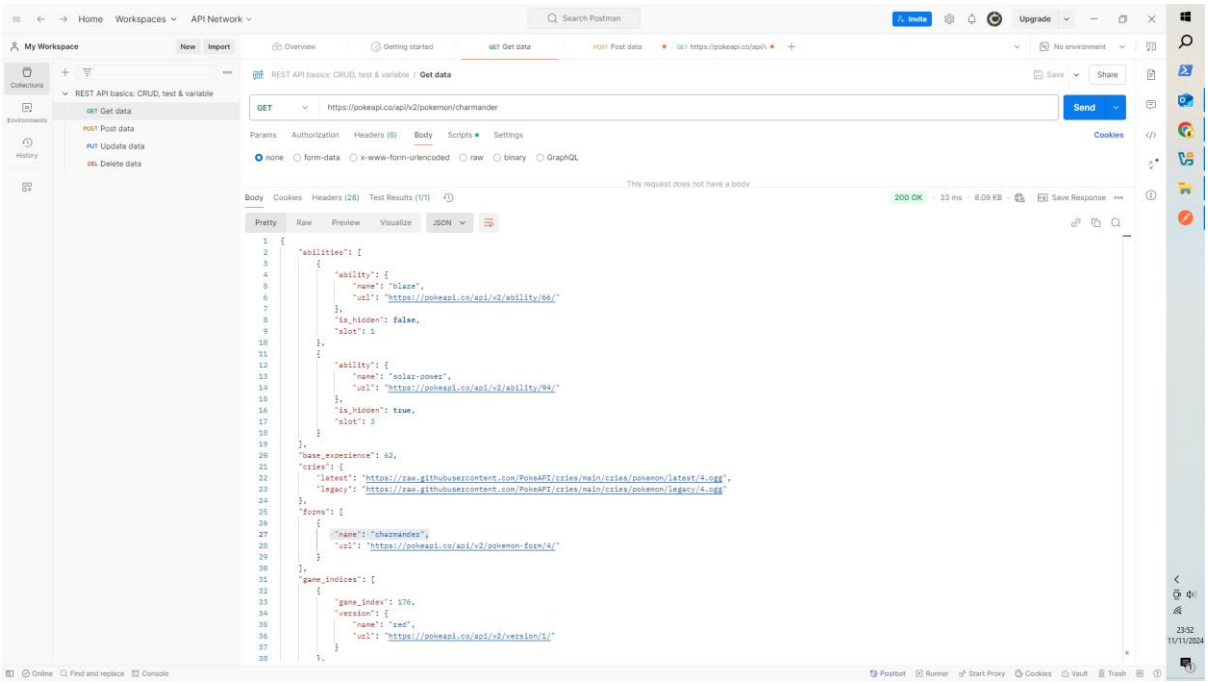
Haz capturas de pantalla de al menos 2 peticiones HTTP y explica cada una y cómo has hecho la petición.

Una de estas 2 APIs debe permitir realizar peticiones POST

Pokeapi

PokeAPI utiliza el método **GET** para obtener información sobre Pokémon, movimientos, tipos, habilidades, y más. Algunos de los endpoints más comunes son: `/pokemon/{id}`,`/pokemon/{nombre}`

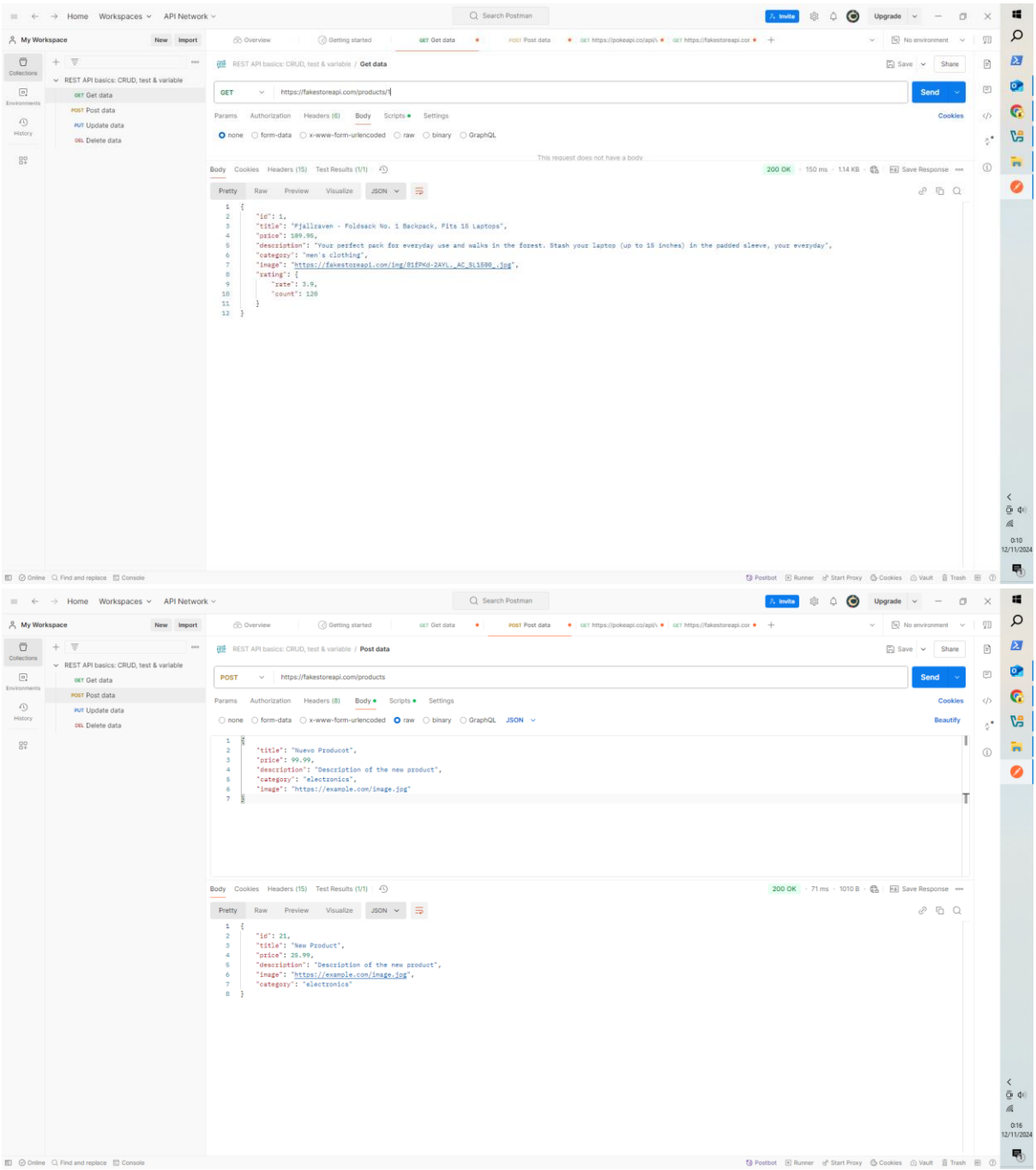



Home
Workspaces
API Network
Search Postman
Invite
Upgrade
My Workspace
New
Import
Overview
Getting started
GET Get data
POST Post data
No environment
REST API basics: CRUD, test & variable / Get data
Save
Share
Collections
Environments
History
REST API basics: CRUD, test & variable
GET Get data
POST Post data
PUT Update data
DEL Delete data
GET
https://pokeapi.co/api/v2/pokemon/charmander
Send
Params
Authorization
Headers (6)
Body
Scripts
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
This request does not have a body
Body
Cookies
Headers (28)
Test Results (1/1)
200 OK
33 ms
8.09 KB
Save Response
Pretty
Raw
Preview
Visualize
JSON
{
"abilities": [
{
"ability": {
"name": "blaze",
"url": "https://pokeapi.co/api/v2/ability/66/"
},
"is_hidden": false,
"slot": 1
},
{
"ability": {
"name": "solar-power",
"url": "https://pokeapi.co/api/v2/ability/94/"
},
"is_hidden": true,
"slot": 3
}
],
"base_experience": 62,
"cries": {
"latest": "https://raw.githubusercontent.com/PokeAPI/cries/main/cries/pokemon/latest/4.ogg",
"legacy": "https://raw.githubusercontent.com/PokeAPI/cries/main/cries/pokemon/legacy/4.ogg"
},
"forms": [
{
"name": "charmander",
"url": "https://pokeapi.co/api/v2/pokemon-form/4/"
}
],
"game_indices": [
{
"game_index": 176,
"version": {
"name": "red",
"url": "https://pokeapi.co/api/v2/version/1/"
}
},
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
23:52
11/11/2024

Proporciona datos simulados de productos de comercio electrónico. Está diseñada para ayudar a los desarrolladores a crear aplicaciones de prueba o prototipos relacionados con tiendas en línea. Ofrece información sobre productos, categorías, precios, descripciones y más, permitiendo realizar operaciones como obtener detalles de productos, categorías y realizar simulaciones de compras.

GET: Usado para obtener información sobre productos, categorías y detalles específicos de los artículos.

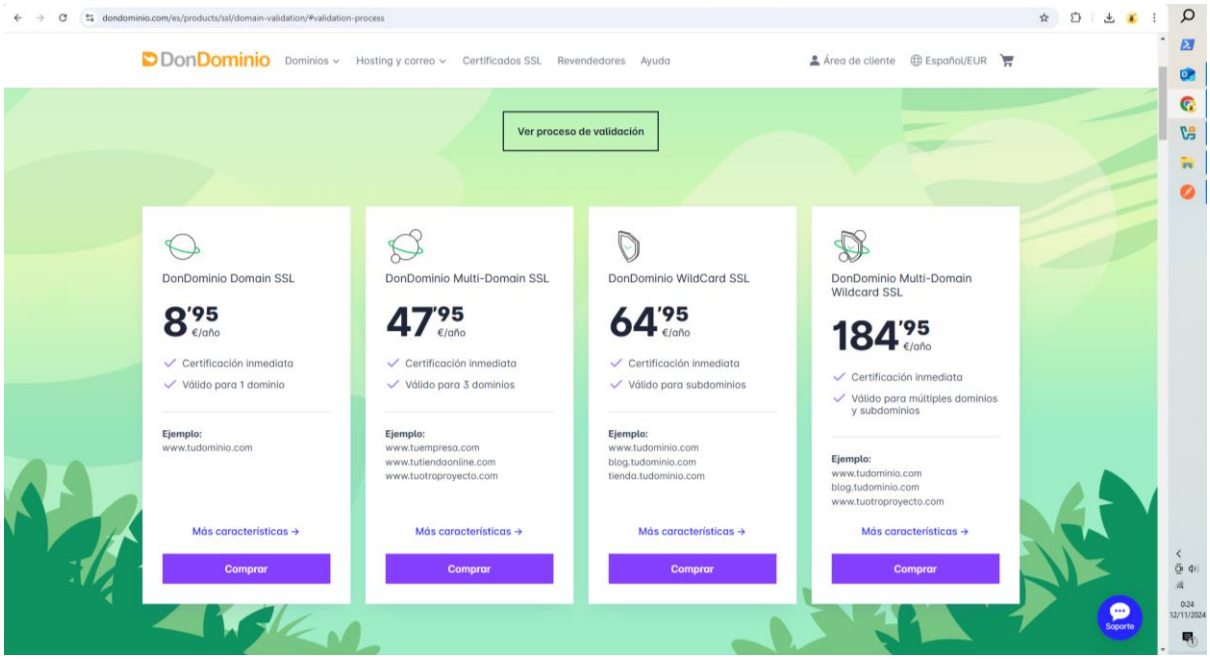
POST: Permite realizar simulaciones de creación de productos.



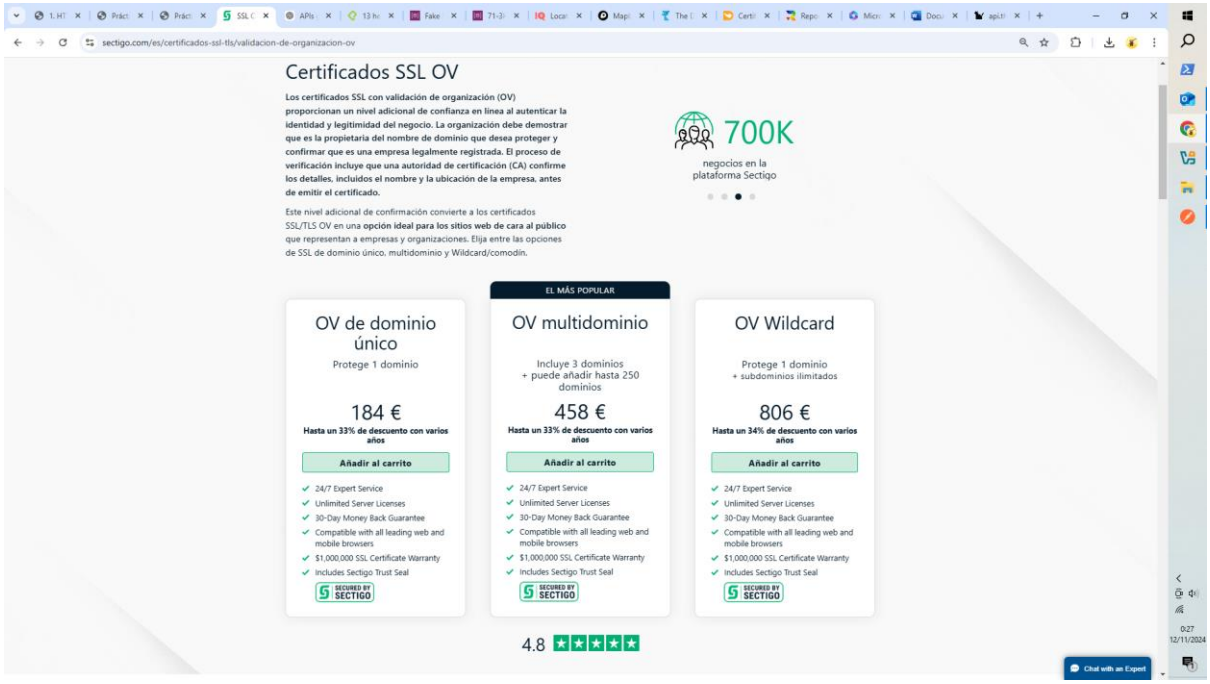
Ejercicio 3. HTTPS, niveles de validación:

Encuentra alguna empresa que emita certificaciones en los distintos niveles que hemos visto, pon información sobre los precios que ofrecen para cada nivel:

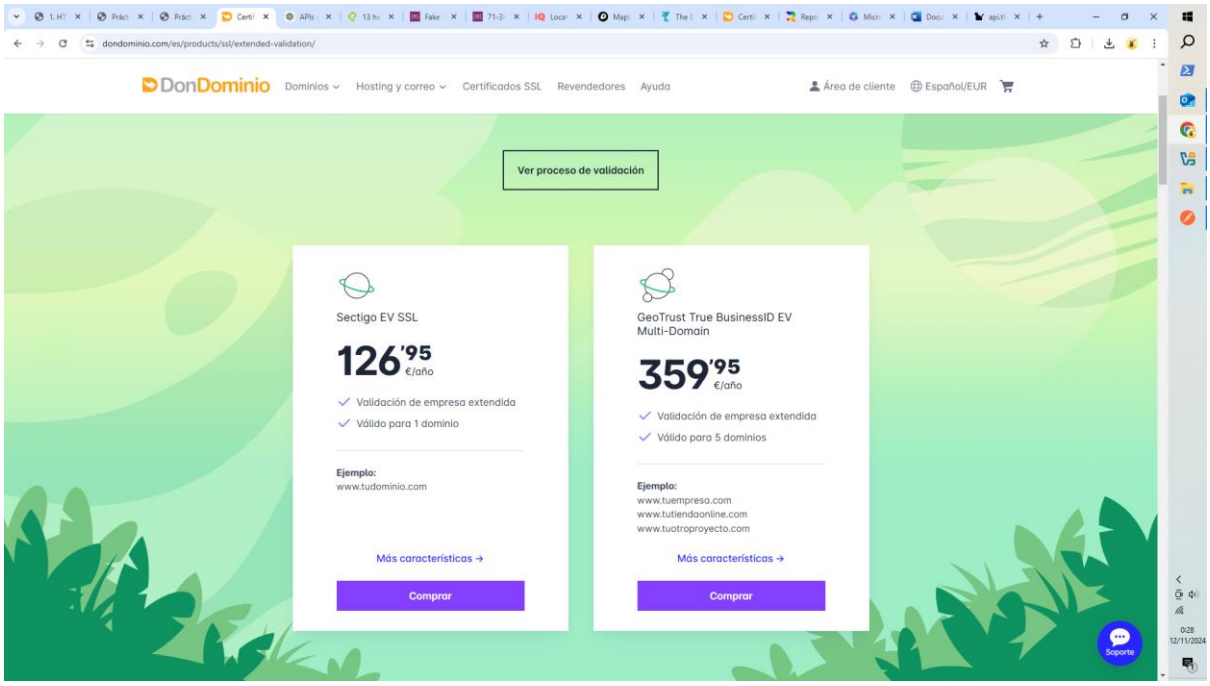
Validación de Dominio (Domain Validation - DV)



Validación de Organización (Organization Validation - OV)



Validación Extendida (Extended Validation - EV)



Nota: el objetivo no es encontrar una empresa que ofrezca los tres niveles (si la encuentras genial), sino encontrar información de los precios que hay en el mercado de los distintos certificados según el nivel.

¿Qué es Let 's Encrypt? busca información ya que es algo muy utilizado hoy en día.

Let's Encrypt es una autoridad certificadora gratuita y de código abierto que ayuda a que los sitios web usen HTTPS, mejorando la seguridad y privacidad en la web. Fue creada en 2015 con el objetivo de hacer más fácil para todos los sitios web usar cifrado. Ofrece certificados SSL/TLS de forma gratuita, lo que permite conexiones seguras

Ejercicio 4.

Analiza los certificados de 2 sitios webs1:

Indica el período de validez del certificado.

Comprueba la cadena de certificados con la herramienta que te he enseñado en la teoría.

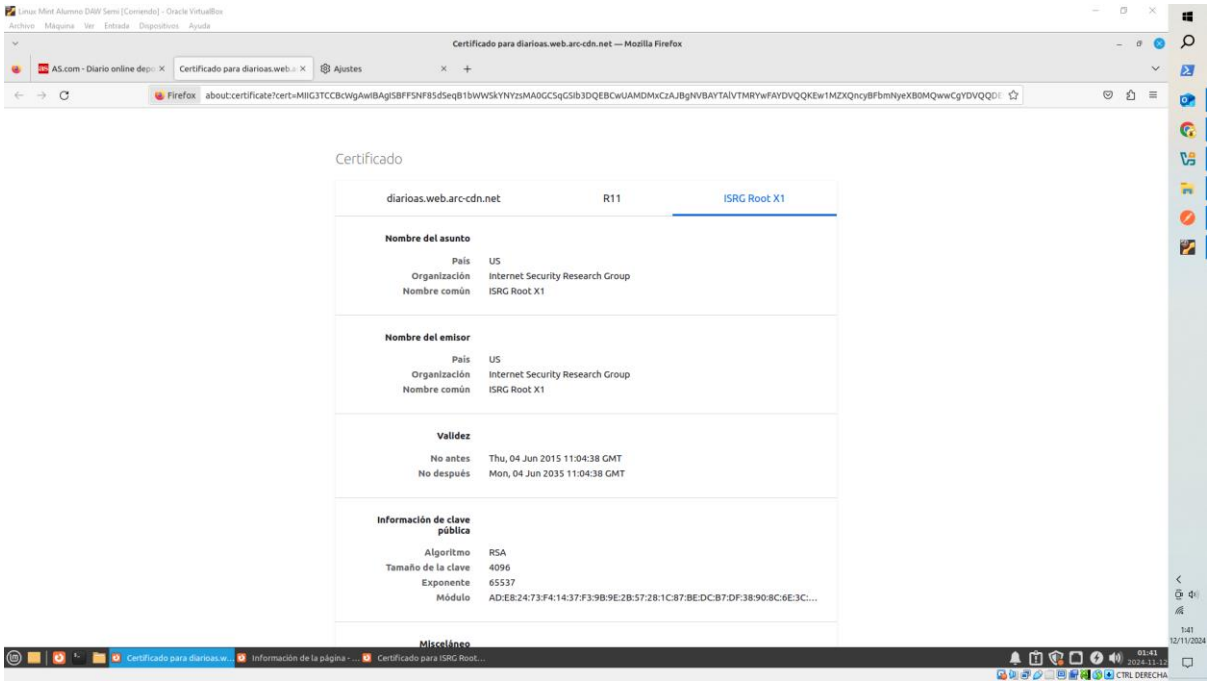
Indica cuál es el CA intermediaria (si la tuviera), el root CA y el certificado del servidor web.

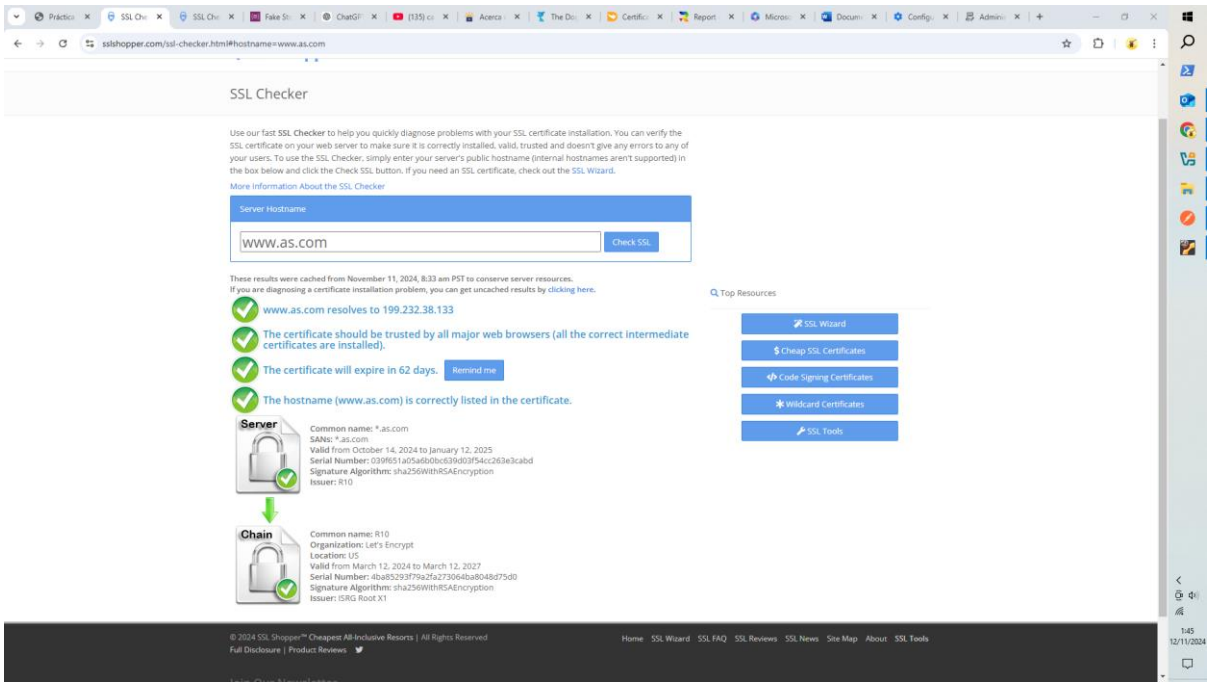
Comprueba si esas CAs tanto la intermediaria como el root CA están añadidas a los listados del navegador o del sistema operativo...

DiarioAs

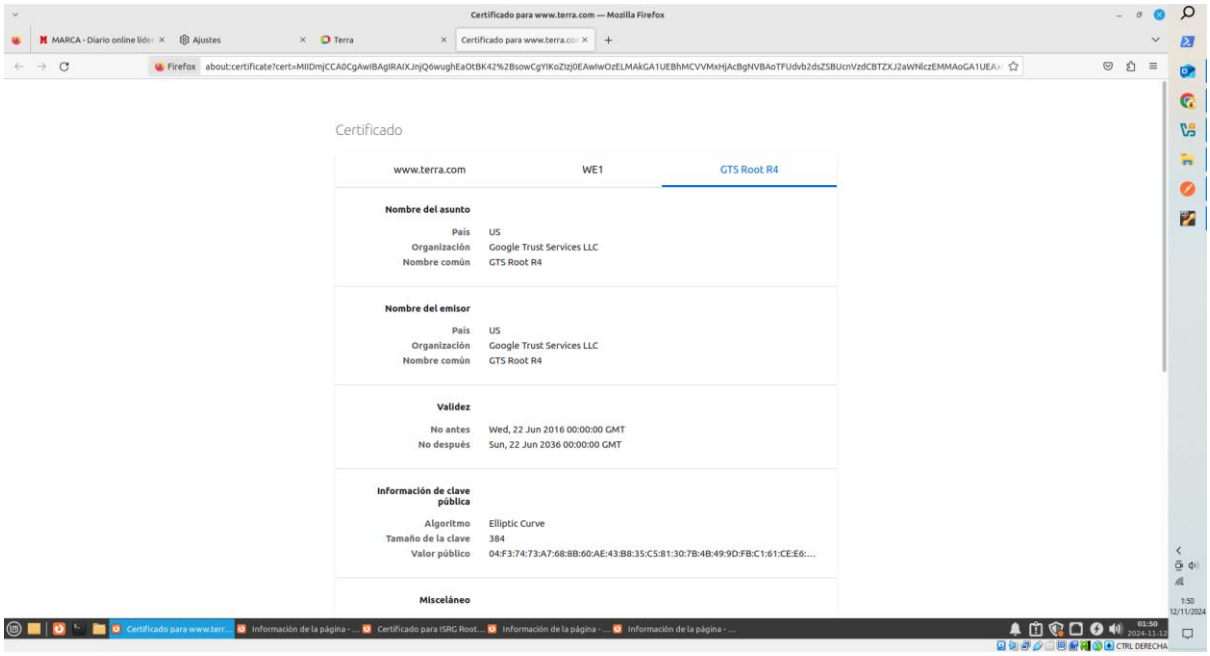
www.as.com

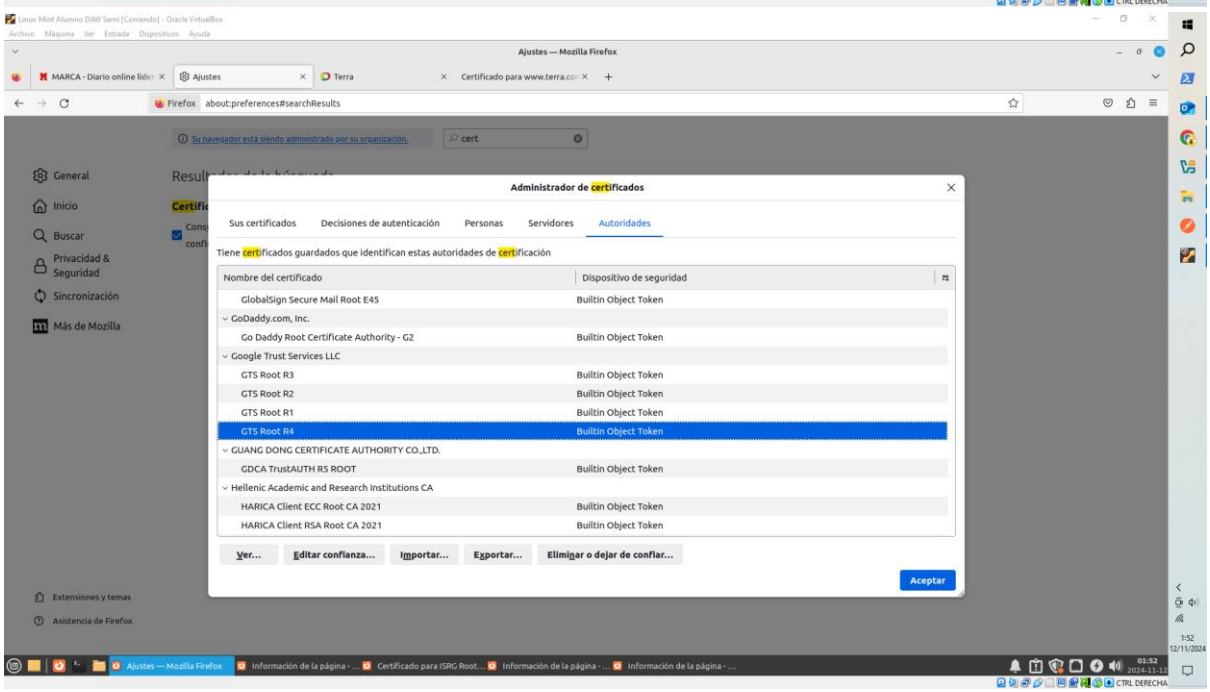
Se aprecia en las siguientes imágenes que el navegador contiene el certificado de diario AS

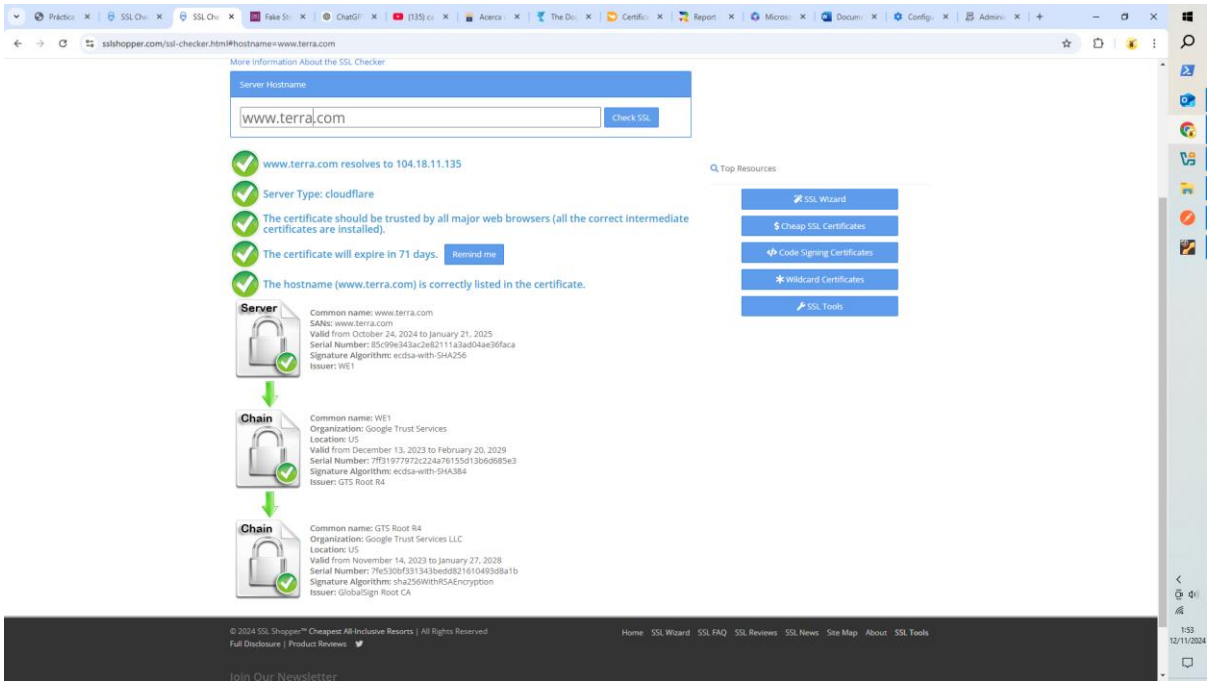

Certificado para diarioas.web.arc-cdn.net — Mozilla Firefox
Certificado
diarioas.web.arc-cdn.net
R11
ISRG Root X1
Nombre del asunto
País US
Organización Internet Security Research Group
Nombre común ISRG Root X1
Nombre del emisor
País US
Organización Internet Security Research Group
Nombre común ISRG Root X1
Validez
No antes Thu, 04 Jun 2015 11:04:38 GMT
No después Mon, 04 Jun 2035 11:04:38 GMT
Información de clave pública
Algoritmo RSA
Tamaño de la clave 4096
Exponente 65537
Módulo AD:E8:24:73:F4:14:37:F3:9B:9E:2B:57:28:1C:87:BE:DC:B7:DF:38:90:8C:6E:3C:...
Miscelánea


sslshopper.com/ssl-checker.html#hostname=www.as.com
SSL Checker
Use our fast SSL Checker to help you quickly diagnose problems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users. To use the SSL Checker, simply enter your server's public hostname (internal hostnames aren't supported) in the box below and click the Check SSL button. If you need an SSL certificate, check out the SSL Wizard.
More Information About the SSL Checker
Server Hostname
www.as.com
Check SSL
These results were cached from November 11, 2024, 8:33 am PST to conserve server resources.
If you are diagnosing a certificate installation problem, you can get uncached results by clicking here.
www.as.com resolves to 199.232.38.133
The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
The certificate will expire in 62 days.
Remind me
The hostname (www.as.com) is correctly listed in the certificate.
Server
Common name: *.as.com
SANs: *.as.com
Valid from October 14, 2024 to January 12, 2025
Serial Number: 039f651a05a6b0bc639d03f54cc263e3cabd
Signature Algorithm: sha256WithRSAEncryption
Issuer: R10
Chain
Common name: R10
Organization: Let's Encrypt
Location: US
Valid from March 12, 2024 to March 12, 2027
Serial Number: dba85293f79a2fa2739648a8048d75d0
Signature Algorithm: sha256WithRSAEncryption
Issuer: ISRG Root X1
Top Resources
SSL Wizard
Cheap SSL Certificates
Code Signing Certificates
Wildcard Certificates
SSL Tools
Home SSL Wizard SSL FAQ SSL Reviews SSL News Site Map About SSL Tools

Se aprecia en las siguientes imágenes que el navegador tiene el certificado de terra.com


Certificado para www.terra.com — Mozilla Firefox
Certificado
www.terra.com
WE1
GTS Root R4
Nombre del asunto
País US
Organización Google Trust Services LLC
Nombre común GTS Root R4
Nombre del emisor
País US
Organización Google Trust Services LLC
Nombre común GTS Root R4
Validez
No antes Wed, 22 Jun 2016 00:00:00 GMT
No después Sun, 22 Jun 2036 00:00:00 GMT
Información de clave pública
Algoritmo Elliptic Curve
Tamaño de la clave 384
Valor público 04:F3:74:73:A7:68:8B:60:AE:43:B8:35:C5:81:30:7B:4B:49:9D:FB:C1:61:CE:E6:...
Misceláneo


Ajustes — Mozilla Firefox
about:preferences#searchResults
Su navegador está siendo administrado por su organización.
cert
General
Inicio
Buscar
Privacidad & Seguridad
Sincronización
Más de Mozilla
Administrador de certificados
Sus certificados
Decisiones de autenticación
Personas
Servidores
Autoridades
Tiene certificados guardados que identifican estas autoridades de certificación
Nombre del certificado
Dispositivo de seguridad
GlobalSign Secure Mail Root E45 Builtin Object Token
GoDaddy.com, Inc.
Go Daddy Root Certificate Authority - G2 Builtin Object Token
Google Trust Services LLC
GTS Root R3 Builtin Object Token
GTS Root R2 Builtin Object Token
GTS Root R1 Builtin Object Token
GTS Root R4 Builtin Object Token
GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.
GDCA TrustAUTH R5 ROOT Builtin Object Token
Hellenic Academic and Research Institutions CA
HARICA Client ECC Root CA 2021 Builtin Object Token
HARICA Client RSA Root CA 2021 Builtin Object Token
Ver...
Editar confianza...
Importar...
Exportar...
Eliminar o dejar de confiar...
Aceptar
Extensiones y temas
Asistencia de Firefox


sslshopper.com/ssl-checker.html#hostname=www.terra.com
More Information About the SSL Checker
Server Hostname
www.terra.com
Check SSL
www.terra.com resolves to 104.18.11.135
Server Type: cloudflare
The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
The certificate will expire in 71 days.
Remind me
The hostname (www.terra.com) is correctly listed in the certificate.
Server
Common name: www.terra.com
SANs: www.terra.com
Valid from October 24, 2024 to January 21, 2025
Serial Number: 85c99e343ac2e82111a3ad04ae36faca
Signature Algorithm: ecdsa-with-SHA256
Issuer: WE1
Chain
Common name: WE1
Organization: Google Trust Services
Location: US
Valid from December 13, 2023 to February 20, 2029
Serial Number: 7ff3197797 2c224a76155d13b6d685e3
Signature Algorithm: ecdsa-with-SHA384
Issuer: GTS Root R4
Chain
Common name: GTS Root R4
Organization: Google Trust Services LLC
Location: US
Valid from November 14, 2023 to January 27, 2028
Serial Number: 7fe530bf331343bedd821610493d8a1b
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign Root CA
Top Resources
SSL Wizard
$ Cheap SSL Certificates
Code Signing Certificates
Wildcard Certificates
SSL Tools
© 2024 SSL Shopper™ Cheapest All-Inclusive Resorts | All Rights Reserved
Full Disclosure | Product Reviews
Home SSL Wizard SSL FAQ SSL Reviews SSL News Site Map About SSL Tools
Join Our Newsletter