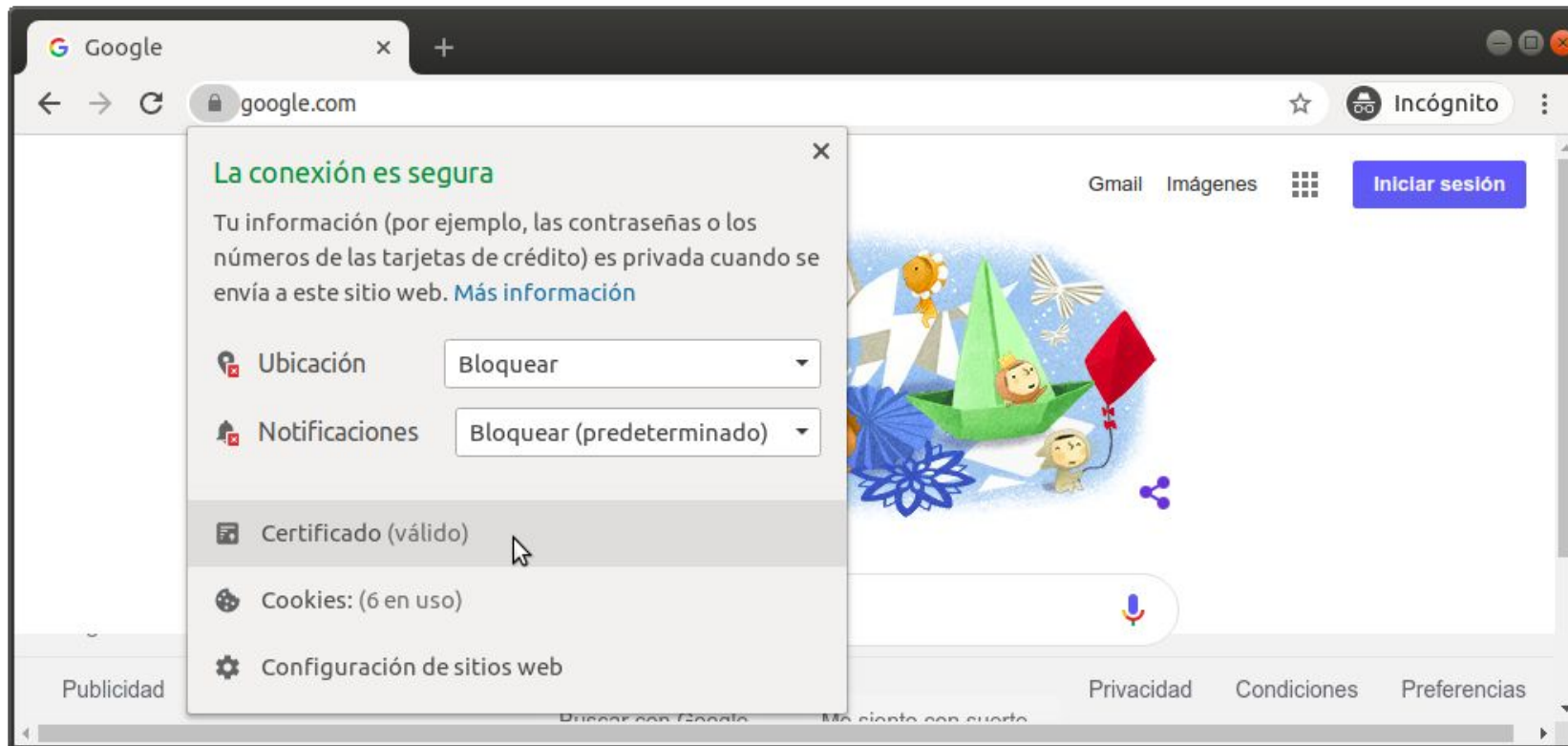


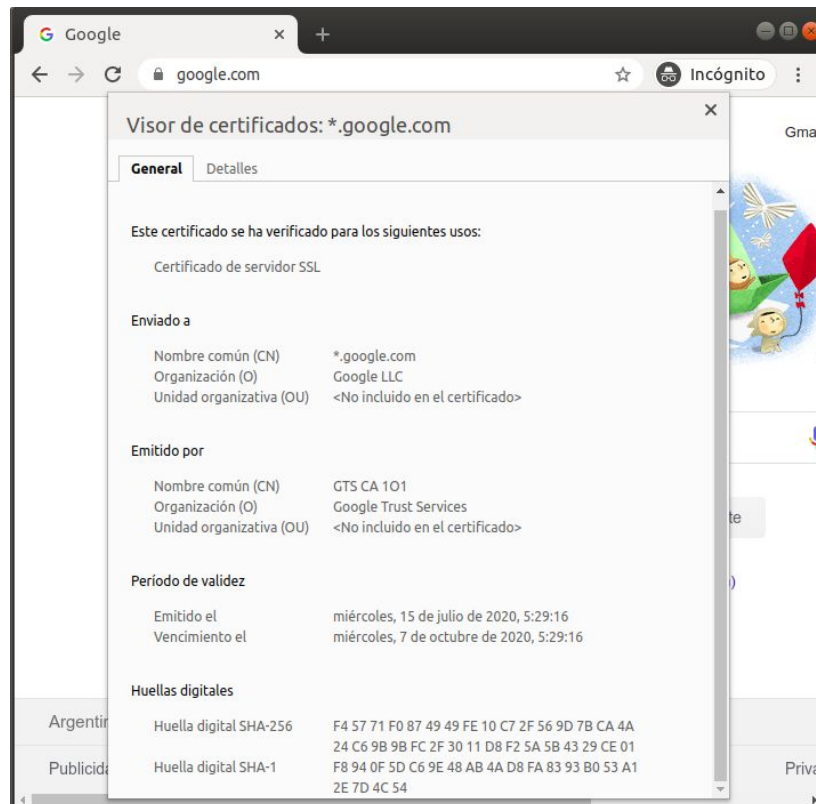
Navegando en un sitio seguro



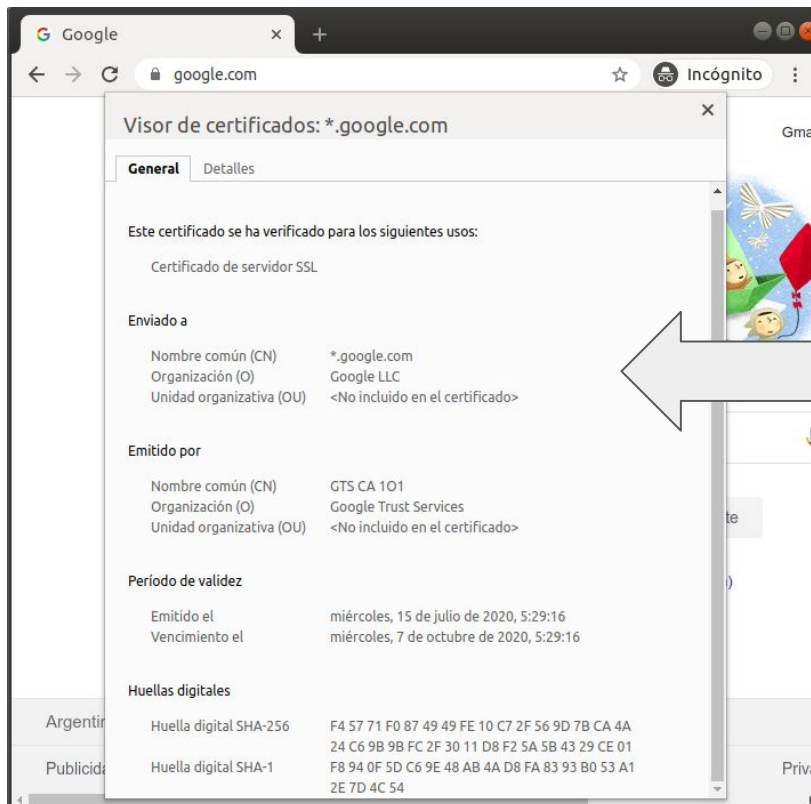
Navegando en un sitio seguro



Datos del certificado del sitio visitado

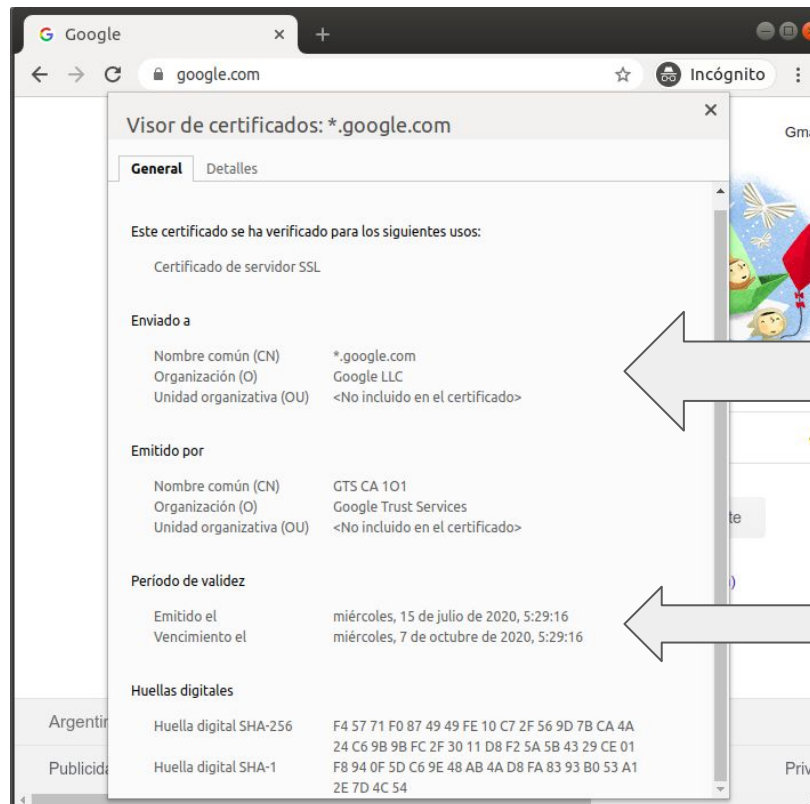


Datos del certificado del sitio visitado



Datos de la identidad del sitio para el cual fue emitido este certificado.
***.google.com** vale para diferentes sitios en el dominio **.google.com**

Datos del certificado del sitio visitado



Datos de la identidad del sitio para el cual fue emitido este certificado.
***.google.com** vale para diferentes sitios en el dominio **.google.com**

Datos sobre el período de validez del presente certificado.

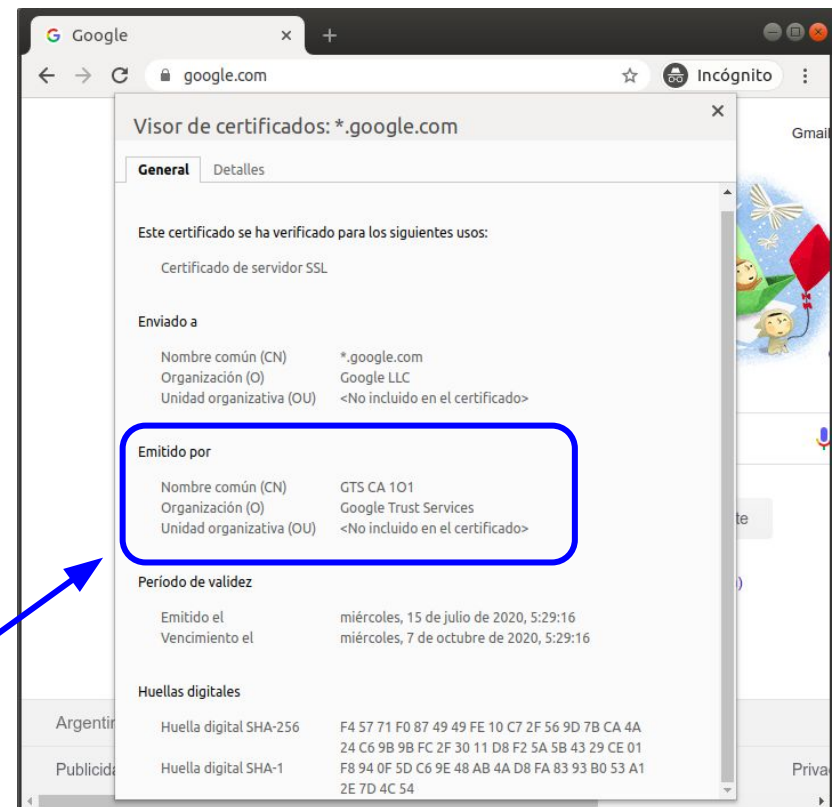
Repaso criptografía asimétrica - FIRMA DIGITAL

Los **certificados digitales**, son reconocidos como válidos, porque fueron emitido por una **Autoridad de certificación en la que confiamos**.

La **autoridad de certificación** es quien asegura que el par de claves pertenece a determinado sitio web.

Un certificado digital, está firmado por la autoridad de certificación.

Entidad en la que confiamos!!!



Algunas Autoridades de Certificación en las que Chrome confía

Por defecto nuestros los navegadores vienen con conjunto de **Autoridades de certificación en la que se confía**.

Nosotros podríamos agregar o borrar alguna **autoridad de certificación**, pero no es algo que se suela hacer.

org-E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.	▼
org-Entrust, Inc.	▼
org-Entrust.net	▼
org-FNMT-RCM	▼
org-GeoTrust Inc.	▼
org-GlobalSign	^
GlobalSign	⋮
GlobalSign	⋮
GlobalSign	⋮
GlobalSign	⋮
org-GlobalSign nv-sa	▼
org-GoDaddy.com, Inc.	▼
org-Government Root Certification Authority	▼
org-GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.	▼
org-Hellenic Academic and Research Institutions Cert. Authority	▼
org-Hongkong Post	▼




Problemas cuando usamos HTTPs

Cuando accedemos a un sitio HTTPs, se pueden presentar distintos problemas que no permiten al navegador asegurar la identidad del sitio visitado.

Cuando ocurre alguna de estas situaciones, el navegador alerta al usuario. Es importante que el usuario entienda que el problema es que **no se puede asegurar la identidad del sitio visitado**.

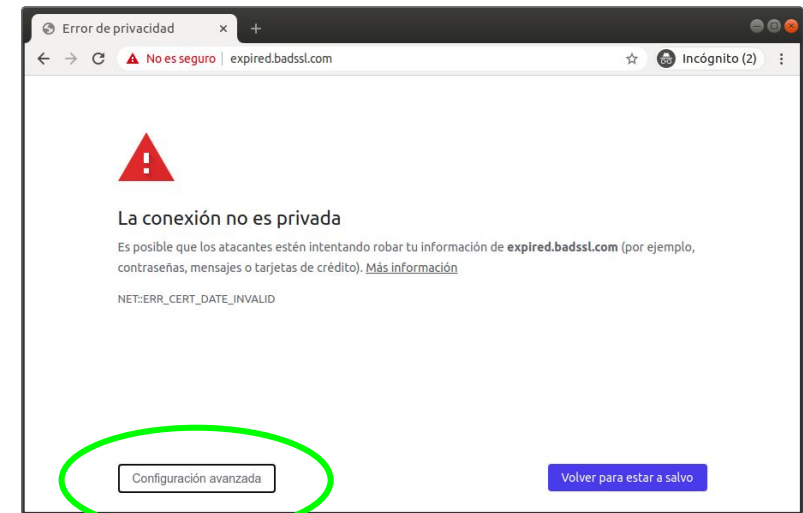
Estos problemas pueden deberse tanto a errores en la configuración del sitio como así también a ataques de phishing contra los usuarios.



Problemas cuando usamos HTTPs

En caso que no se trate de un phishing, algunas situaciones en las que podemos ver este tipo de alertas es cuando:

- El certificado está vencido.
- No coincide la URL del sitio visitado con la identidad del certificado presentado por el sitio web.
- El certificado está autofirmado.
- El certificado está firmado por una CA en la que no se confía.
- Cuidado con la fecha/hora del sistema!!



Certificado expirado - <https://expired.badssl.com/>

Este servidor no ha podido demostrar que es **expired.badssl.com**; su certificado de seguridad caducó hace 1.953 días. Este problema puede deberse a una configuración incorrecta o a que un atacante ha interceptado la conexión. La fecha que consta en el reloj de tu ordenador actualmente es el domingo, 16 de agosto de 2020. ¿Es correcto? Si no lo es, corrige el reloj del sistema y, a continuación, actualiza esta página.

[Acceder a expired.badssl.com \(sitio no seguro\)](#)

Ocultar configuración avanzada

Volver para estar a salvo

Visor de certificados: *.badssl.com

General	
Enviado a	
Nombre común (CN)	*.badssl.com
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	Domain Control Validated
Emitido por	
Nombre común (CN)	COMODO RSA Domain Validation Secure S
Organización (O)	COMODO CA Limited
Unidad organizativa (OU)	<No incluido en el certificado>
Período de validez	
Emitido el	miércoles, 8 de abril de 2015, 21:00:00
Vencimiento el	domingo, 12 de abril de 2015, 20:59:59

No coincide la identidad del sitio con la del certificado - <https://wrong.host.badssl.com/>

Este servidor no ha podido probar que su dominio es **wrong.host.badssl.com**, su certificado de seguridad procede de ***.badssl.com**. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a wrong.host.badssl.com \(sitio no seguro\)](#)

Ocultar configuración avanzada

Volver para estar a salvo

Visor de certificados: *.badssl.com

General	
Enviado a	
Nombre común (CN)	*.badssl.com
Organización (O)	Lucas Garron Torres
Unidad organizativa (OU)	<No incluido en el certificado>
Emitido por	
Nombre común (CN)	DigiCert SHA2 Secure Server CA
Organización (O)	DigiCert Inc
Unidad organizativa (OU)	<No incluido en el certificado>
Período de validez	
Emitido el	domingo, 22 de marzo de 2020, 21:00:00
Vencimiento el	martes, 17 de mayo de 2022, 9:00:00

Certificado autofirmado - <https://self-signed.badssl.com/>

The screenshot shows a web browser window with a security warning. The address bar displays "No es seguro" (Not secure) and the URL "self-signed.badssl.com". The main content area contains a message explaining that the server cannot prove its identity and that the system does not trust the security certificate. Below this message is a link to "Acceder a self-signed.badssl.com (sitio no seguro)". At the bottom of the page, there are two buttons: "Ocultar configuración avanzada" (Hide advanced settings) and "Volver para estar a salvo" (Go back to be safe).

Este servidor no ha podido probar que su dominio es **self-signed.badssl.com**, el sistema operativo de tu ordenador no confía en su certificado de seguridad. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a self-signed.badssl.com \(sitio no seguro\)](#)

Ocultar configuración avanzada

Volver para estar a salvo

Visor de certificados: *.badssl.com

General Detalles

Enviado a

Nombre común (CN)	*.badssl.com
Organización (O)	BadSSL
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

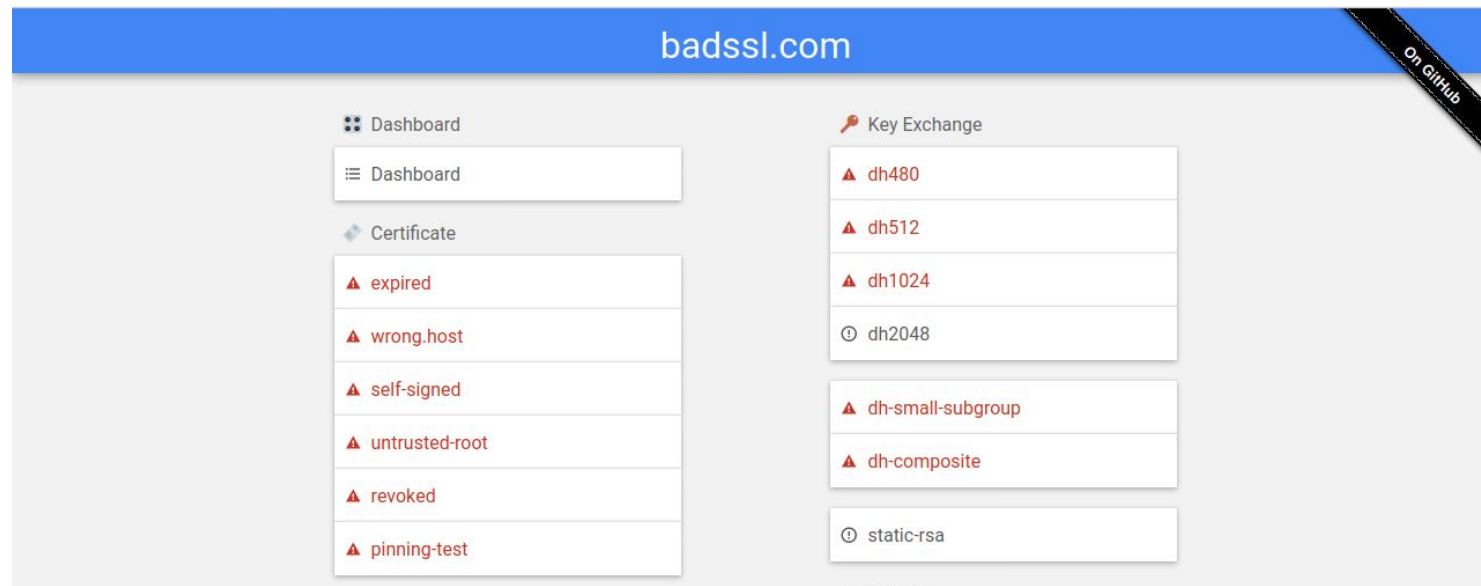
Nombre común (CN)	*.badssl.com
Organización (O)	BadSSL
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	miércoles, 9 de octubre de 2019, 20:41:52
Vencimiento el	viernes, 8 de octubre de 2021, 20:41:52

Otros problemas con certificados

Este sitio nos permite ver ejemplos de otros posibles problemas con certificados donde el navegador nos mostrará una alerta.



<https://badssl.com/>