¿Qué pasa con la seguridad cuando se transmite información?

Hay algunas preguntas que podemos hacernos:

- ¿Estamos seguros que quien nos envía un mensaje es quien dice ser?
- Si alguien logra interceptar una comunicación ¿puede ver el contenido del mensaje?
- Si alguien accede al contenido del mensaje ¿puede modificarlo sin que el que lo reciba se dé cuenta?

¿Qué pasa con la seguridad cuando se transmite información?

Hay distintos mecanismos para proteger la información y garantizar:

- Autenticidad
- Confidencialidad
- Integridad

Depende de lo que queramos garantizar qué mecanismos vamos a usar!

Un ejemplo de intercambio de Información Seguro

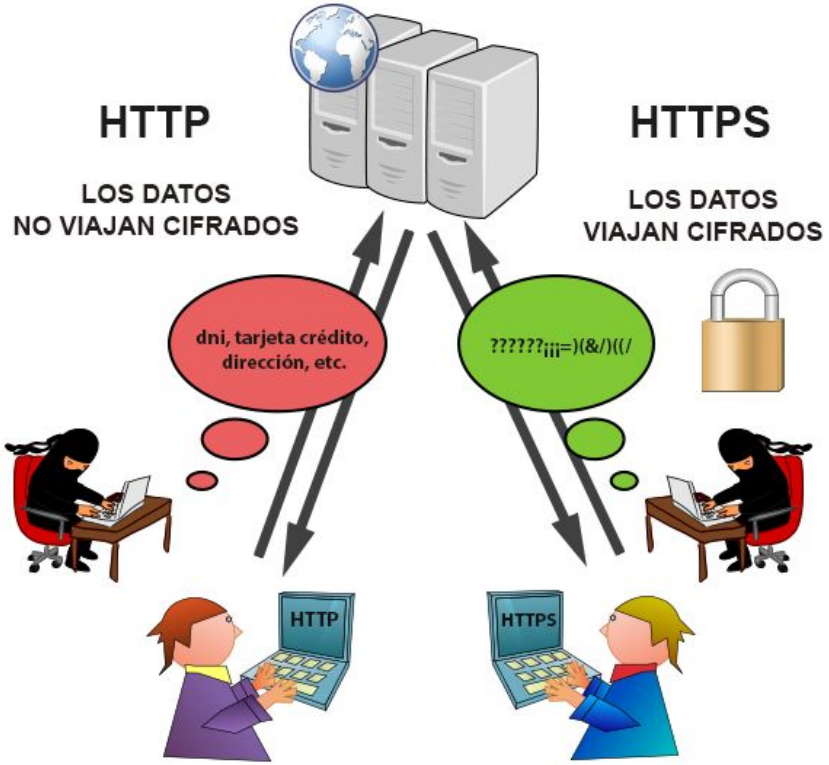
Pensemos en un servicio de mensajería de paquetes que usa un protocolo para proteger la comunicación.
El protocolo sería:

- Se usa una caja con candado para guardar los mensajes a enviar. Existe una única llave.
- Inicialmente el receptor debe hacer llegar al emisor el candado que éste debe utilizar.
- Para transmitir un mensaje secreto, el emisor guarda el mensaje en la caja y la cierra con el candado que el receptor le dio.
- El receptor recibe la caja, y luego de abrir el candado con la llave que **solo él posee** puede acceder al mensaje.

Navegando en sitios seguros

Cuando navegamos en Internet, los protocolos de comunicación más usados son HTTP y HTTPS.

Estos protocolos son los que utilizan los navegadores para conectarse a páginas web.



Navegando en sitios seguros - HTTPS

A diferencia de **HTTP**, el protocolo de navegación **HTTPS** provee un canal de comunicación seguro entre el cliente y el servidor.

La seguridad que ofrece **HTTPs** implica que:

- La información viaja de manera cifrada de extremo a extremo.
- El cliente puede verificar la autenticidad del sitio visitado.
- Opcionalmente el servidor puede requerir autenticación del cliente.

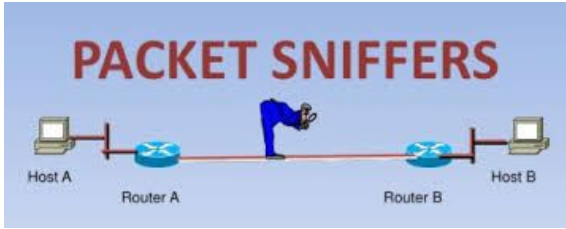
Navegando en sitios seguros - HTTPS

A diferencia de **HTTP**, el protocolo de navegación **HTTPS** provee un canal de comunicación seguro entre el cliente y el servidor.

La seguridad que ofrece **HTTPs** implica que:

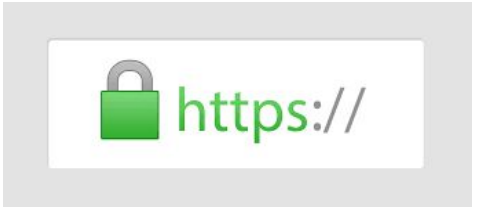
- La información viaja de manera cifrada de extremo a extremo

  Un sniffer (aplicación que permite analizar el tráfico de red con el propósito de espiar) no podrá entender los mensajes intercambiados entre el cliente y el servidor



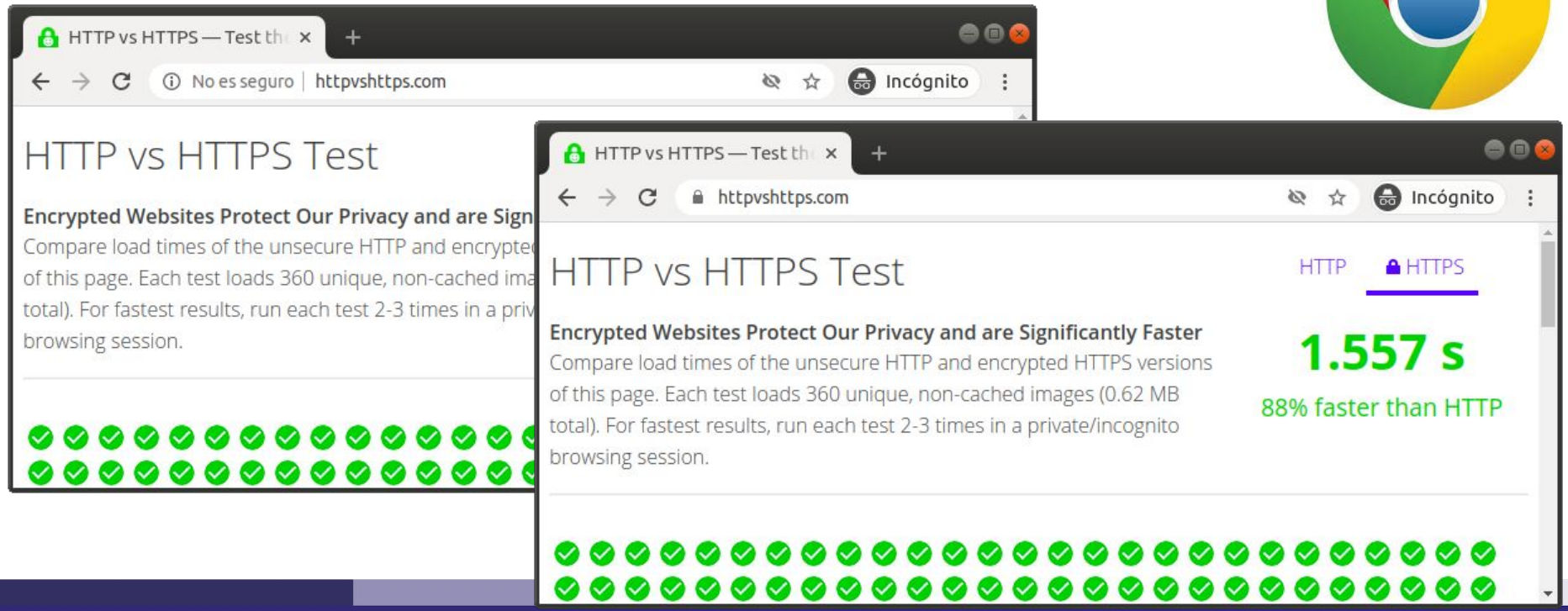
- El cliente puede verificar la autenticidad del sitio visitado

  El navegador tiene la posibilidad de utilizar la criptografía asimétrica para verificar la autenticidad del sitio visitado

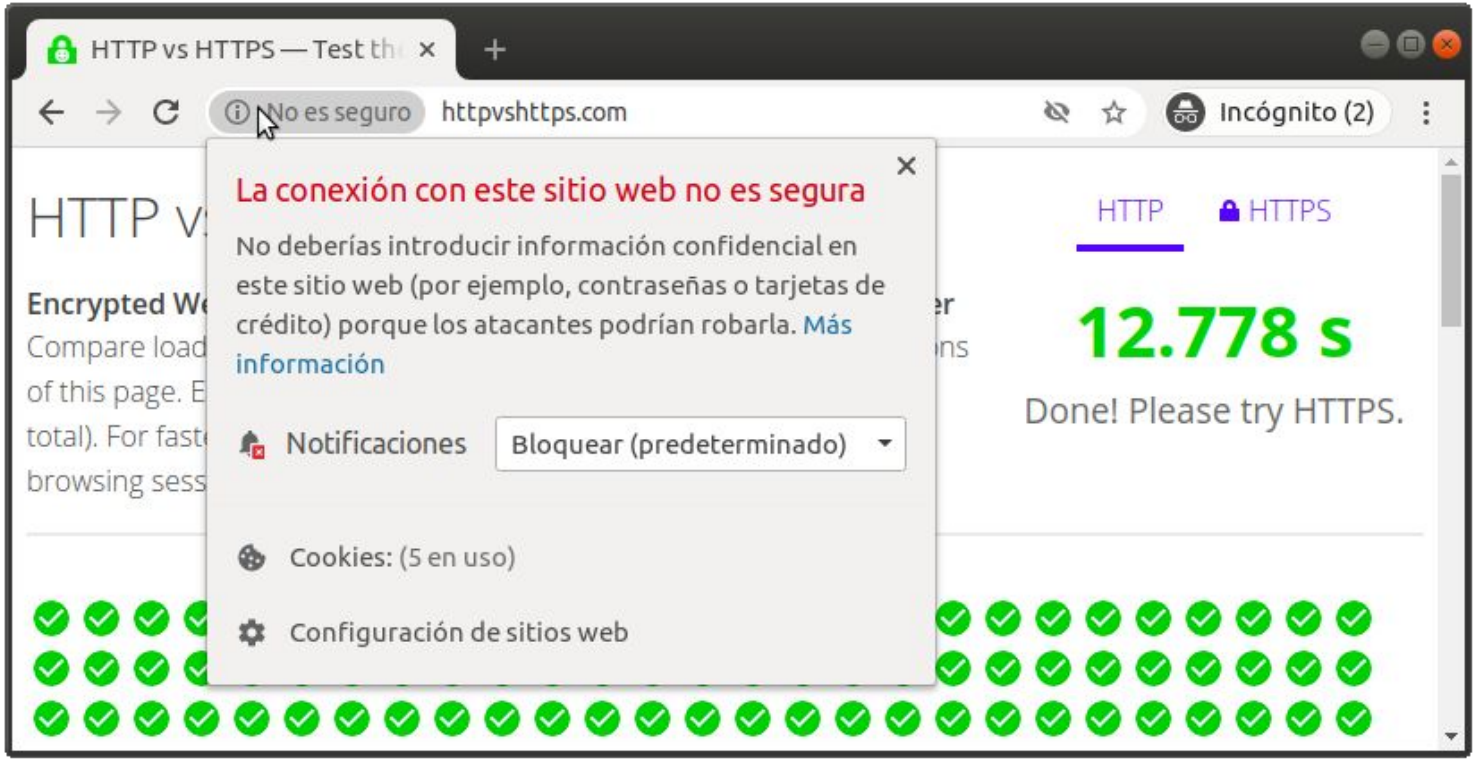


Cómo se distinguen los navegadores HTTP y HTTPs

Comparación en cómo se muestra un sitio HTTP y uno HTTPs válido

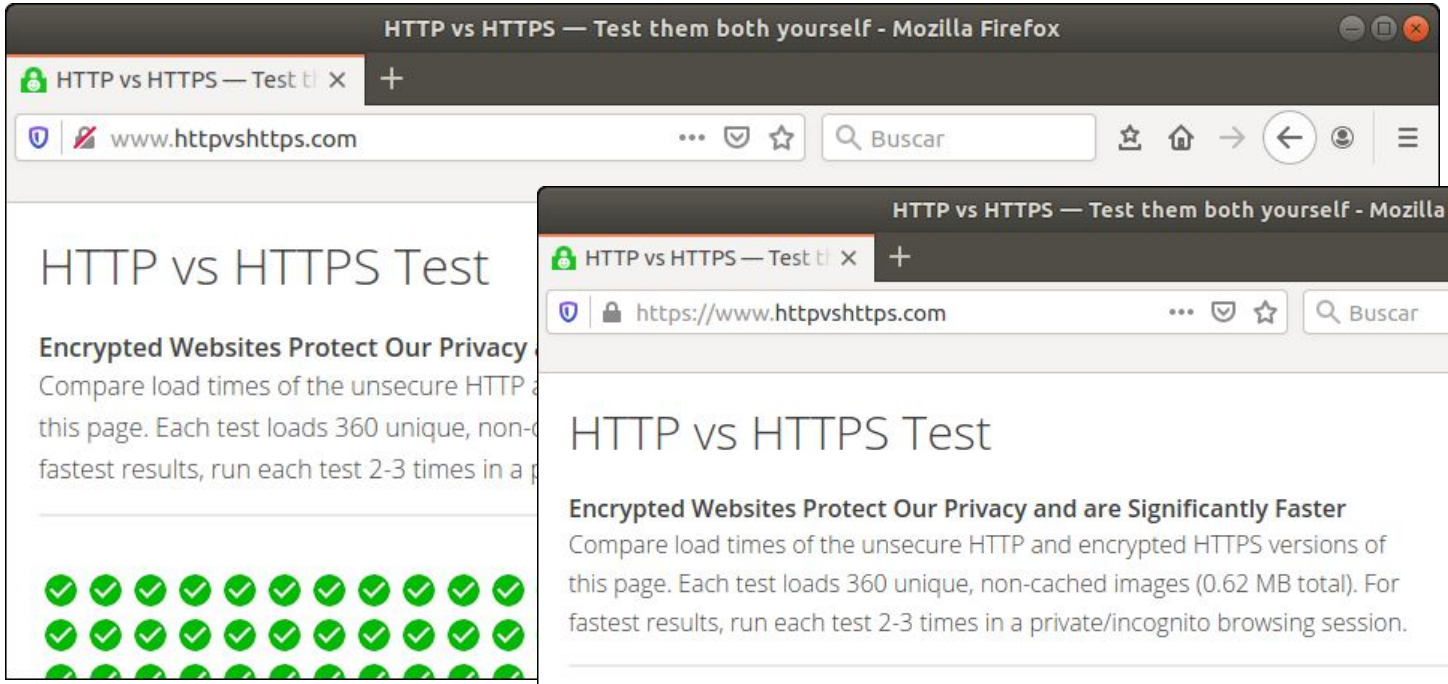


¿Qué significa ese: No es seguro?



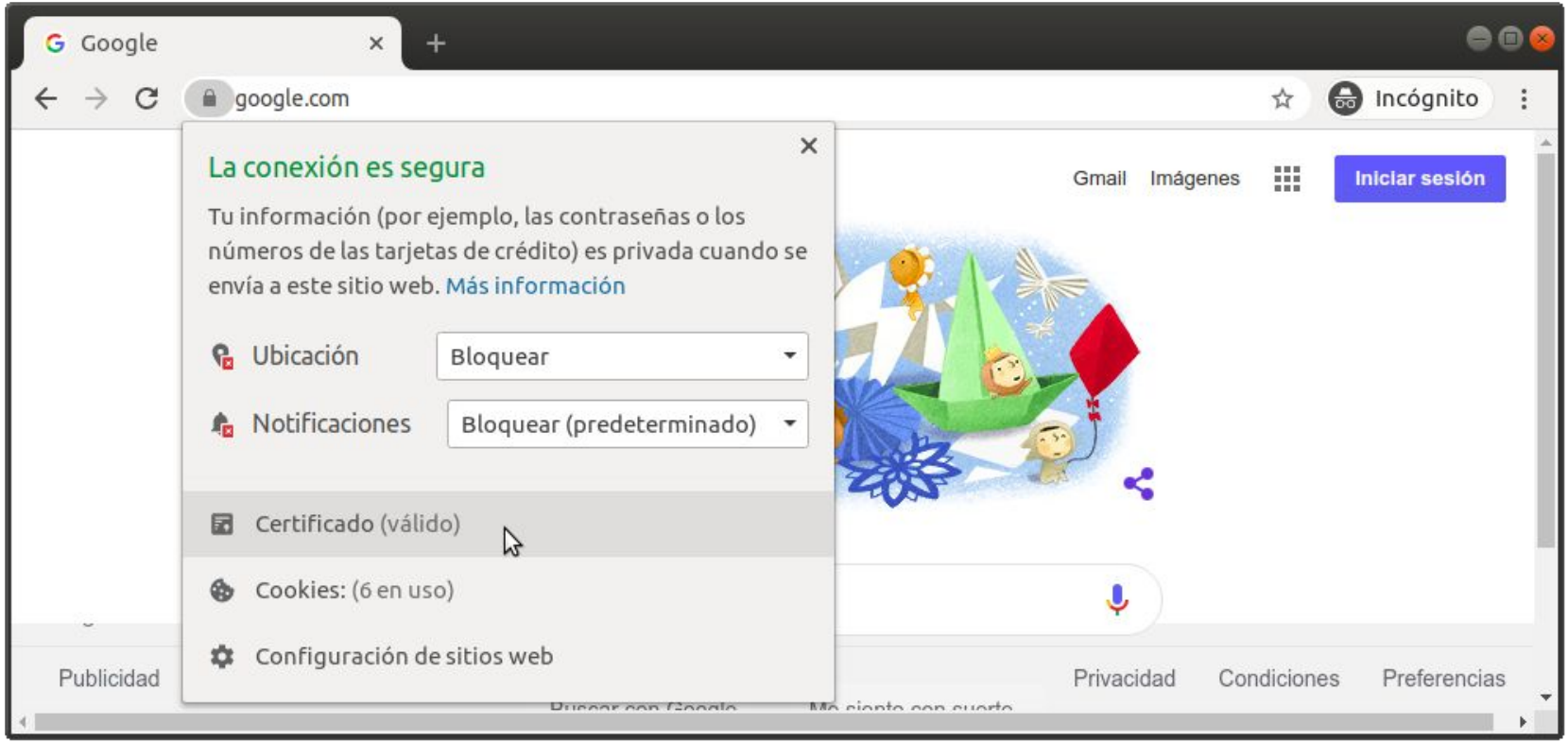
Como se distinguen los navegadores HTTP y HTTPs

Comparación en como se muestra un sitio HTTP y uno HTTPs válido

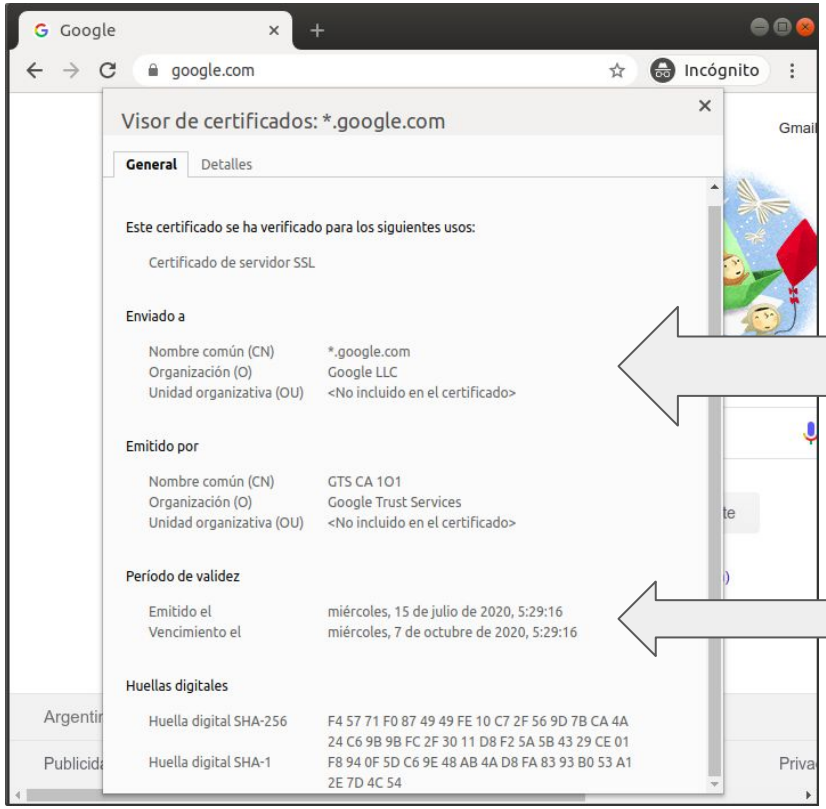


Navegando en un sitio seguro

Navegando en un sitio seguro



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.

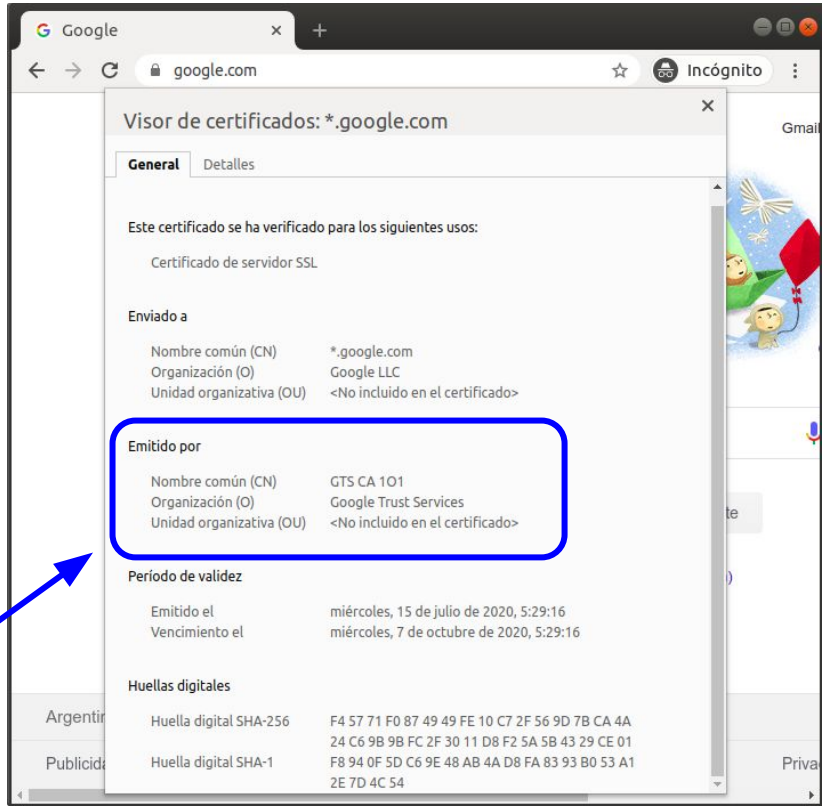
El certificado está firmado digitalmente por una CA

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.

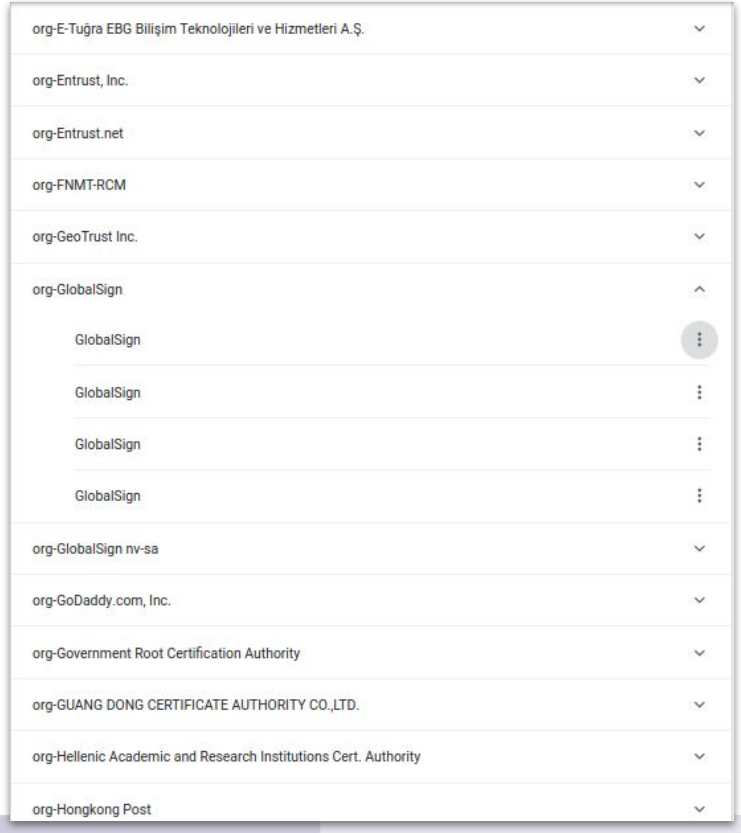
Entidad en la que confiamos!!!



Algunas Autoridades de Certificación en las que Chrome confía

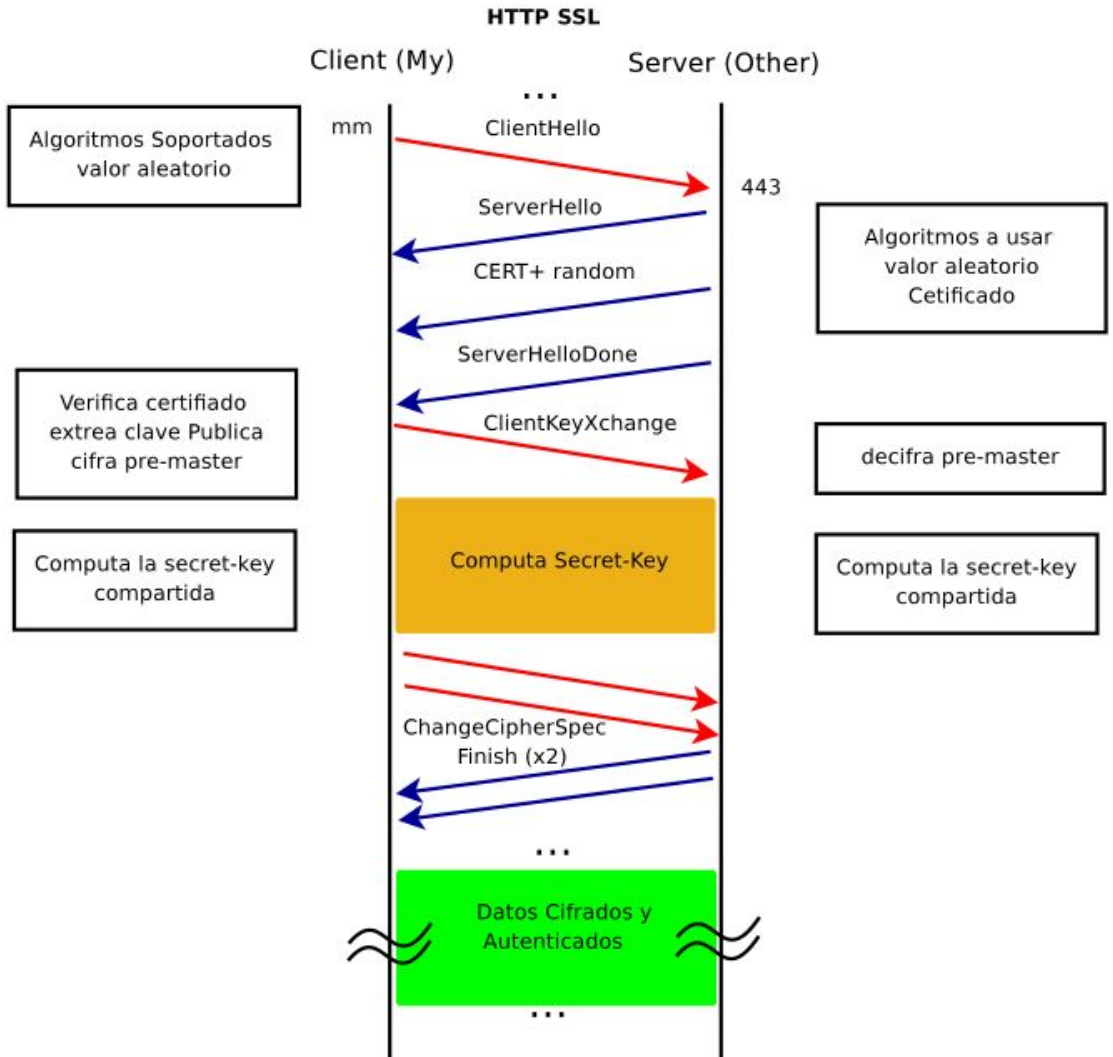
Por defecto nuestros los navegadores vienen con conjunto de **Autoridades de certificación en la que se confía.**

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



HTTPS
HTTP sobre TLS/SSL

- Utiliza por defecto el puerto 443
- Lleva a cabo un handshake (negociación) antes del intercambio de datos.



Otros protocolos seguros

El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de son versiones seguras de programas que emplean protocolos que no lo son. Ejemplos:

- SSH utiliza SSL/TLS por debajo.
- SMTP y NNTP pueden operar también de manera segura sobre SSL/TLS.
- POP3 e IMAP4 sobre SSL/TLS son POP3S i IMAPS.

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.

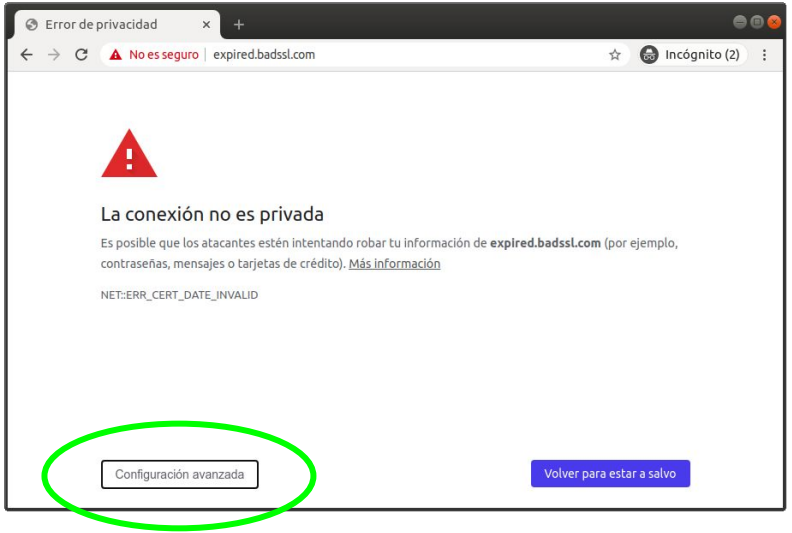
Cuando ocurre alguna de estas situaciones, el navegador alerta al usuario. Es importante que el usuario entienda que el problema es que **no se puede asegurar la identidad del sitio visitado**.

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

Más información

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!!



Problemas cuando usamos HTTPs

En estos dos videos pueden encontrar más información para complementar:

- https://youtu.be/tHhFQaurGAg (muy básico y sencillo)
- https://youtu.be/pOeWmStBOYY (un poquito más detallado)
- https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https (un poco más de info en Digicert!)