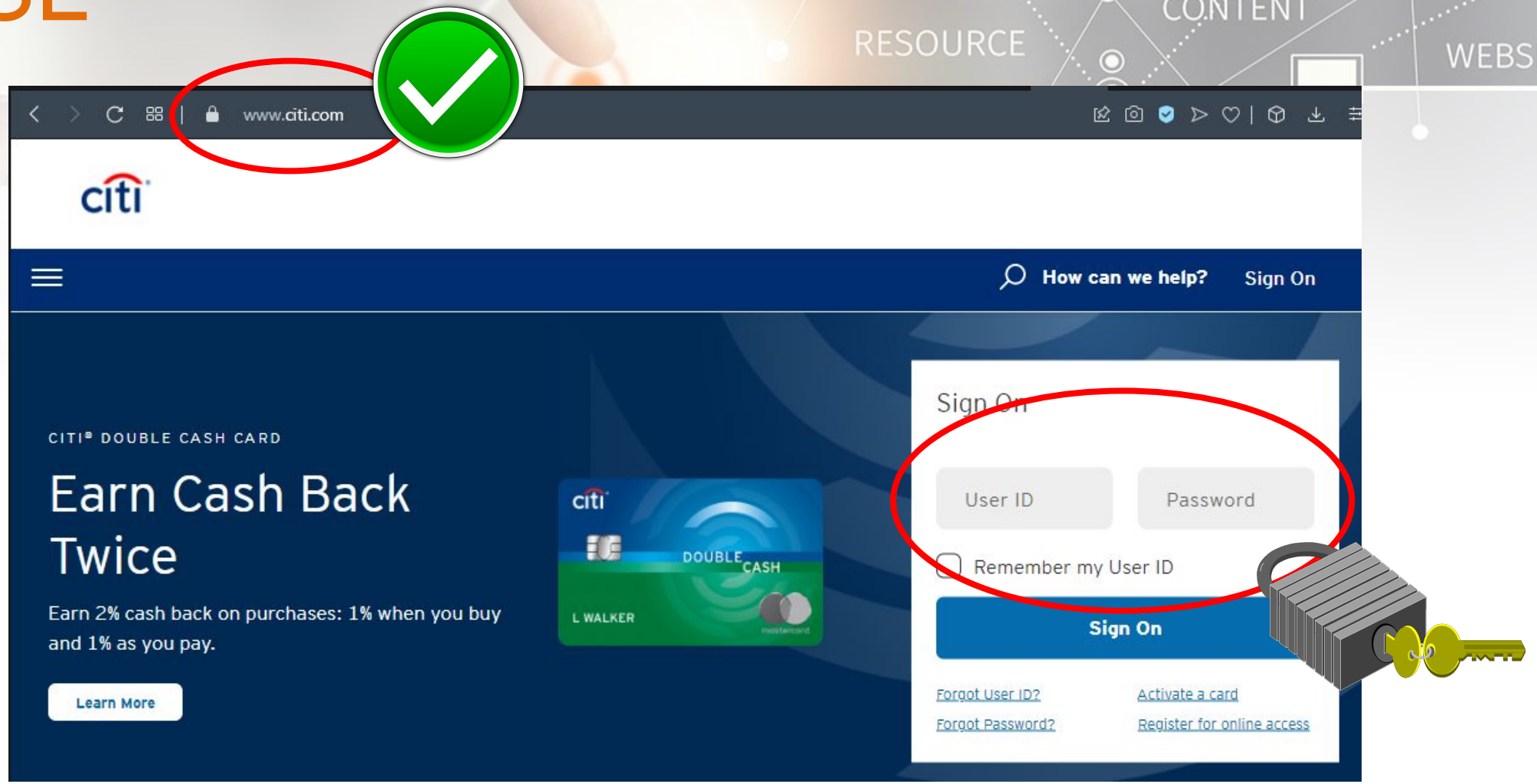

ACCOUNT
SEARCH
SEARCH
NETWORK
ACCOUNT
APPLICATION
COMMUNICATION
WEBSITE
SEARCH
CONTENT
MONITORING
CONTENT
RESOURCE
WEBSITE

TLS / SSL

SSL



Para encriptar datos desde y hacia el servidor, un Web Server puede usar SSL (Secure Sockets Layer).

SSL

Secure Sockets Layer

- Desarrollado por Netscape en 1994
- RFC 6101 define SSL 3.0 (Agosto 2011)
- Una capa intermedia entre protocolos de aplicación y de transporte (TCP)
- Permite a un servidor que "hable" SSL autenticarse a sí mismo con un cliente que "hable" SSL
- Permite a un cliente autenticarse con un servidor
- Permite encriptar la conversación entre cliente y servidor

Nociones básicas de criptografía

Roy

Moss

M: mensaje en texto plano

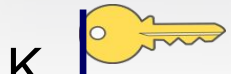
$K_R(M)$: mensaje cifrado con clave K_R

$M = K_M(K_R(M))$

Clave simétrica

Roy

K_S
Clave compartida



K_S

Moss

Texto plano → Algoritmo de encriptación → Texto cifrado → Algoritmo de des-encriptación → Texto plano

La clave que se usa para encriptar es la misma que se usa para desencriptar

Claves asimétricas

Roy

Moss

Un mensaje codificado con la clave pública de Moss sólo podrá desencriptarse con la clave privada de Moss.

Clave asimétrica

Roy

K_{M+}
Clave privada
de Roy

Texto plano

Algoritmo
de
encriptación

Texto cifrado

K_{M-}
Clave pública
de Roy

Algoritmo
de des-
encriptación

Texto plano

Moss

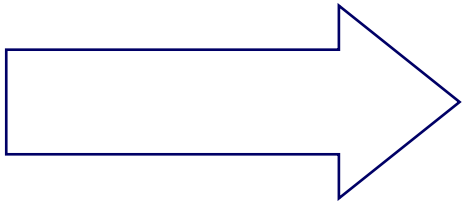
Un mensaje codificado con la clave privada de Roy sólo podrá desencriptarse con la clave pública de Roy.

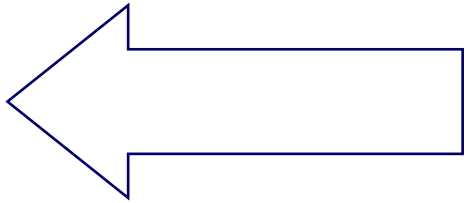
Claves públicas

¿Cómo hace Roy para asegurarse que habla con Moss y no con alguien que se hace pasar por él?

Clave pública de Moss

PassPhrase





Clave privada de Moss

PassPhrase

Claves públicas

¿Cómo hace Roy para enviar un mensaje de forma tal que sólo lo pueda leer Moss y se asegure que sea de Roy?

Clave privada de Roy

Clave pública de Moss

MENSAJE

Claves públicas

¿Cómo hace Roy para enviar un mensaje de forma tal que sólo lo pueda leer Moss y se asegure que sea de Roy?

Clave pública de Moss

Clave privada de Roy

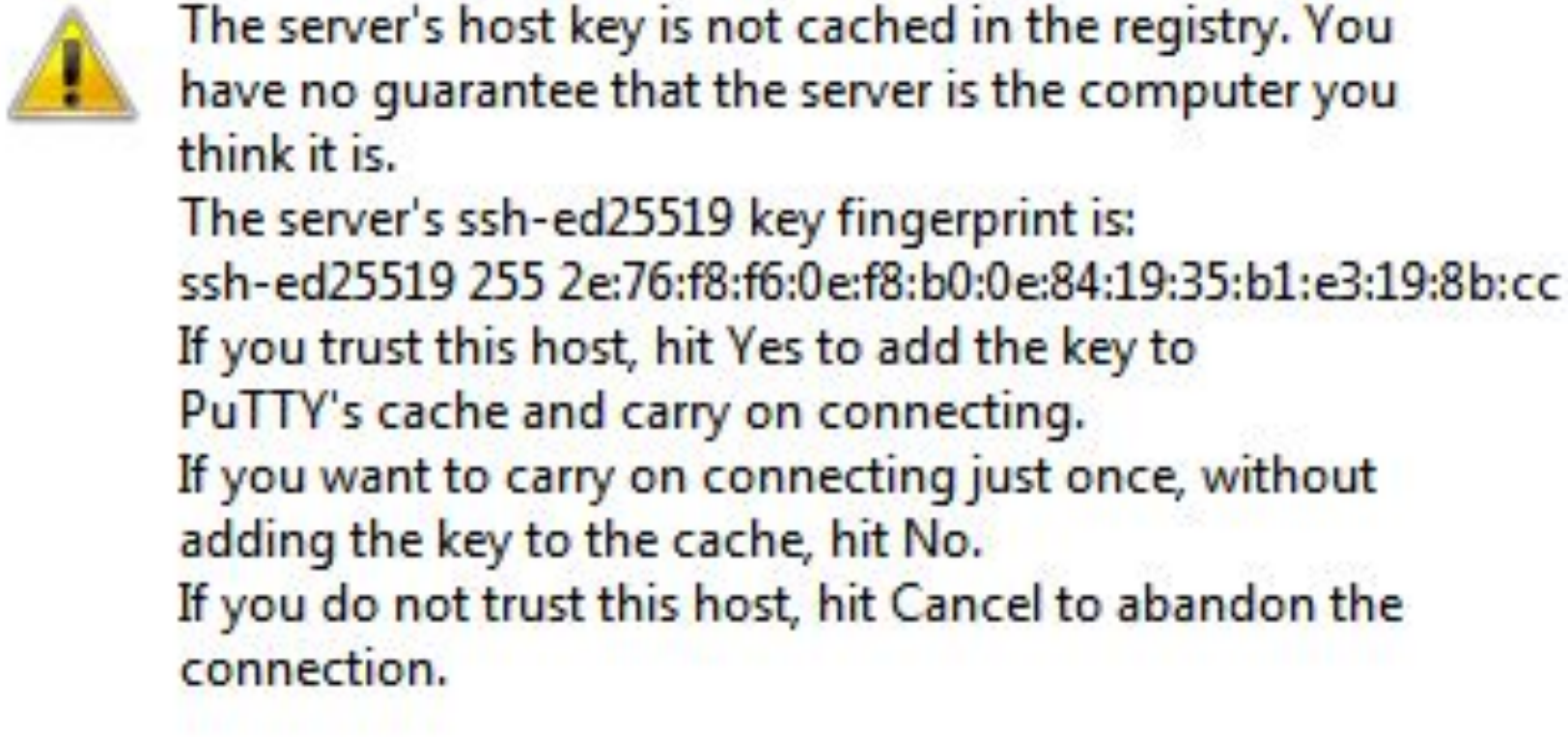
MENSAJE

SSL

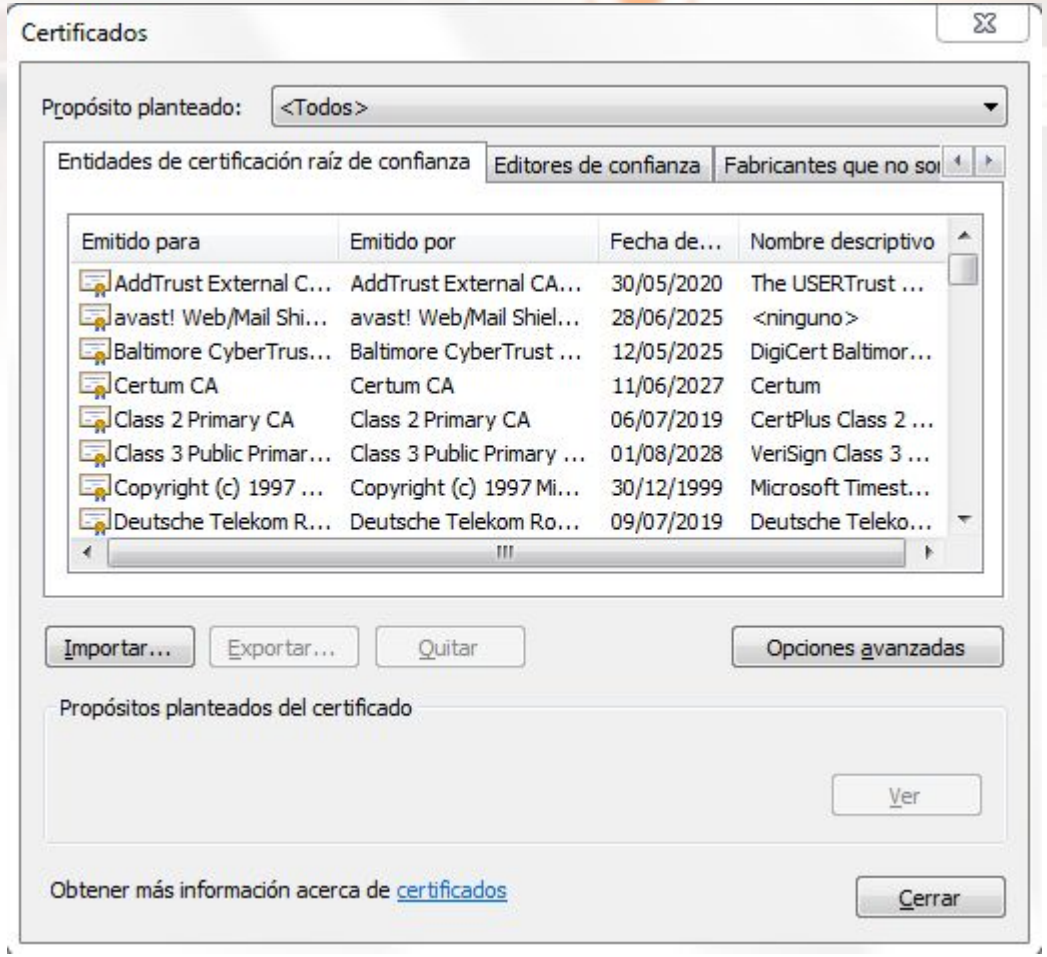
Creación de certificados

I. Crear una clave pública y privada
II. Crear un certificado que incluya la clave del servidor
III. Firmar el certificado, por un CA reconocido o por uno mismo.

¿Por qué aparece a veces?



SSL: Listado de entidades certificantes.



Los certificados incluyen:

- La clave pública de la autoridad
- Los datos de la autoridad (nombre, e-mail)
- Período de vigencia
- Identificación del firmante
- Firma digital del firmante

SSL handshaking

Solicitud de conexión segura (https://.....)

Envío de certificado X.509 conteniendo clave pública

Cliente verifica autenticidad del certificado

Cliente genera clave simétrica aleatoria y la encripta usando clave pública del servidor

Cliente y servidor conocen la clave simétrica y encriptan los datos con ella durante la sesión

TLS

Transport Layer Security

- TLS 1.0 está basado en SSL 3.0 (a veces TLS es llamado SSL 3.1)
- RFC 5246 define TLS 1.2
- Conexión segura por puerto: 443 para "*https*", 993 para "*IMAPs*", 995 para *"POPs"*, etc. Usa SSL
- Conexión segura por protocolo: comienza con un "hello" inseguro y luego cambia a una conexión segura. Ejemplo: comando STARTTLS en SMTP
- TSL y SSL proprocionan el mismo nivel de encriptación. Difieren en cómo se inicia la conexión segura.

DNS over TLS (DoT)

- Por defecto el puerto 853
- Incorporado en forma nativa en algunos Linux
- Dos modos:
  - modo estricto
  - modo de privacidad oportunista
- Soportado por algunos servidores:
  - ver https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers

DNS over HTTPs (DoH)

- Se configura en cada browser que lo soporte (en Firefox está por defecto)
- RFC 8484
- El cliente usa GET o POST para enviar una query DNS codificada