Seguridad y Alta Disponibilidad:
Criptografía III

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León

jesus.moreno.edu@
juntadeandalucía.es

Septiembre 2012

Transparencias adaptadas del material del libro:

Redes de computadores: un enfoque descendente basado en Internet, 2ª edición.Jim Kurose, Keith Ross

Copyright 1996-2002.
J.F Kurose y K.W. Ross.
Todos los derechos reservados.

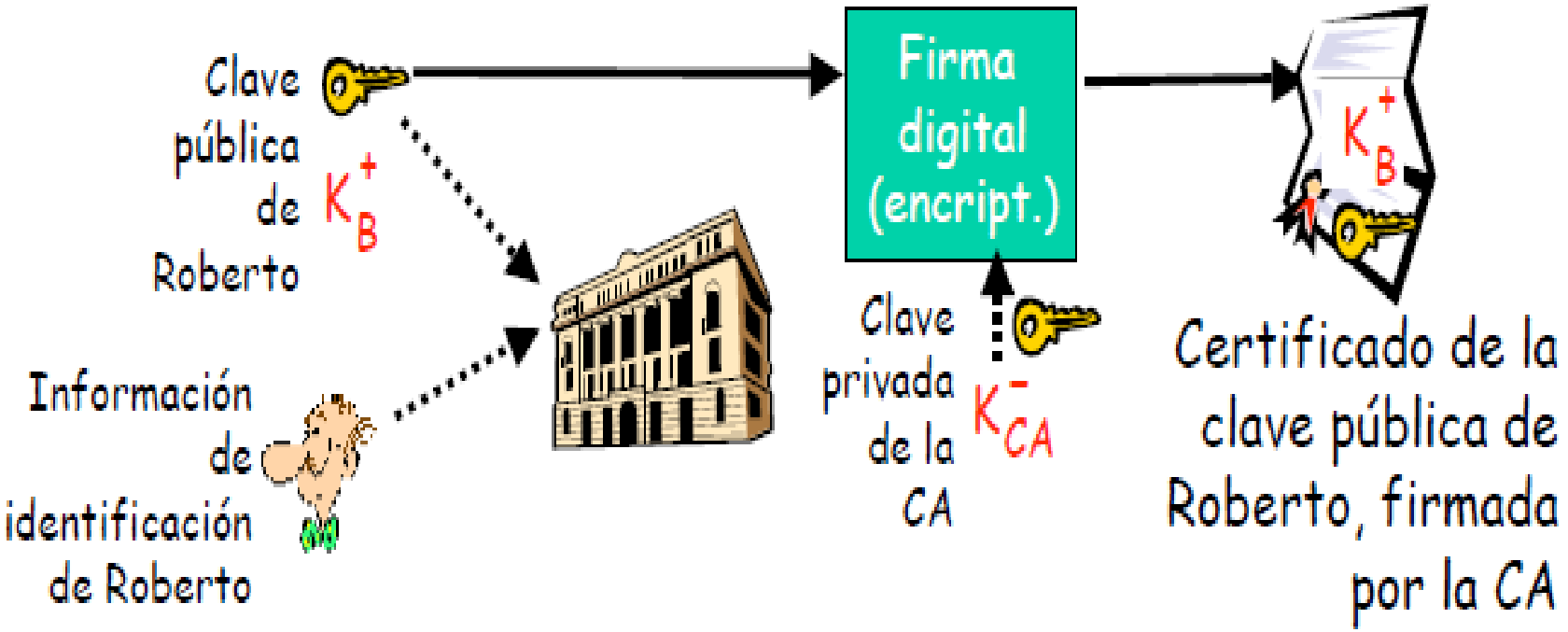
Autoridades de certificación

Autoridad de certificación CA → vincula una clave pública a una entidad particular E (router, persona…)

E debe registrar su clave pública con CA:

- E proporciona una prueba de identidad a CA
- CA crea un certificado que vincula a E con su clave pública
- El certificado contiene la calve pública de E firmada digitalmente por CA → CA afirma *"Esta es la clave pública de la entidad E"*

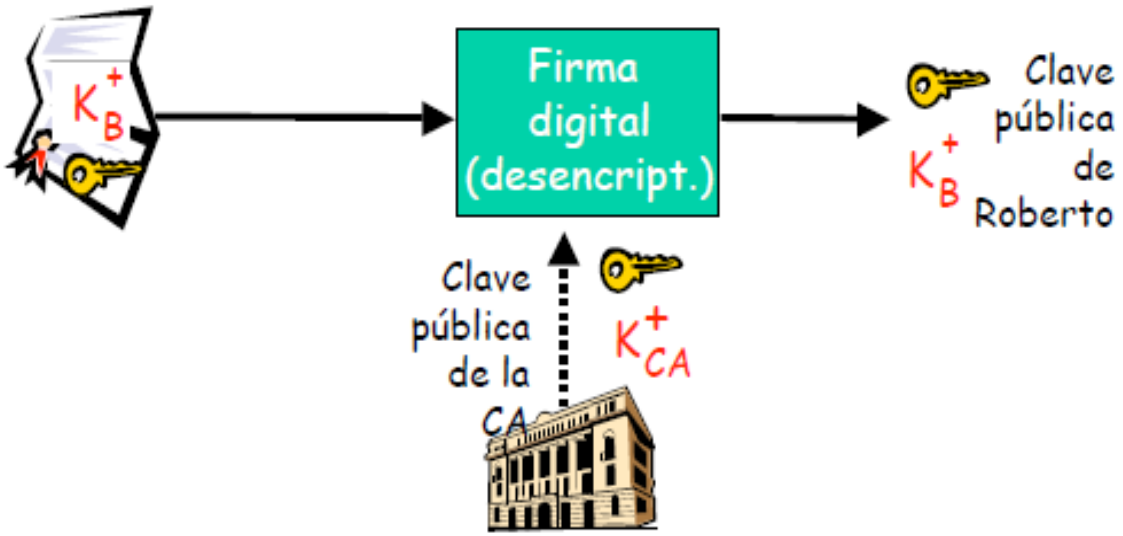
Autoridades de certificación



Autoridades de certificación

Cuando Alicia quiere la clave pública de Roberto, ya no tiene que pedírsela a él (problema MITM), sino que obtiene el certificado (de Roberto, de Internet, de otra persona...)

Tan sólo tiene que aplicar la clave pública de CA al certificado de Roberto para obtener la clave pública de Roberto



Certificados

Este certificado ha sido verificado para los siguientes usos:

Certificado del servidor SSL

Emitido para

Nombre común (CN)	sourceforge.net
Organización (O)	sourceforge.net
Unidad organizativa (OU)	3754508056
Número de serie	13:87:19

Emitido por

Nombre común (CN)	<No es parte de un certificado>
Organización (O)	Equifax
Unidad organizativa (OU)	Equifax Secure Certificate Authority

Validez

Emitido el	22/06/10
Expira el	23/09/11

Huellas digitales

Huella digital SHA1	46:1C:D1:EF:6E:69:1F:86:19:D4:52:28:5D:C0:1B:48:4C:05:98:7A
Huella digital MD5	E4:07:E6:7D:A3:FD:C7:1F:AD:51:85:8E:4D:67:FE:33

Capa de Socket Seguros (SSL)

Proporciona seguridad en la capa de transporte a cualquier aplicación basada en TCP

Es protocolo que se utiliza entre navegadores de Internet y servidores de comercio electrónico, por ejemplo (https://...)

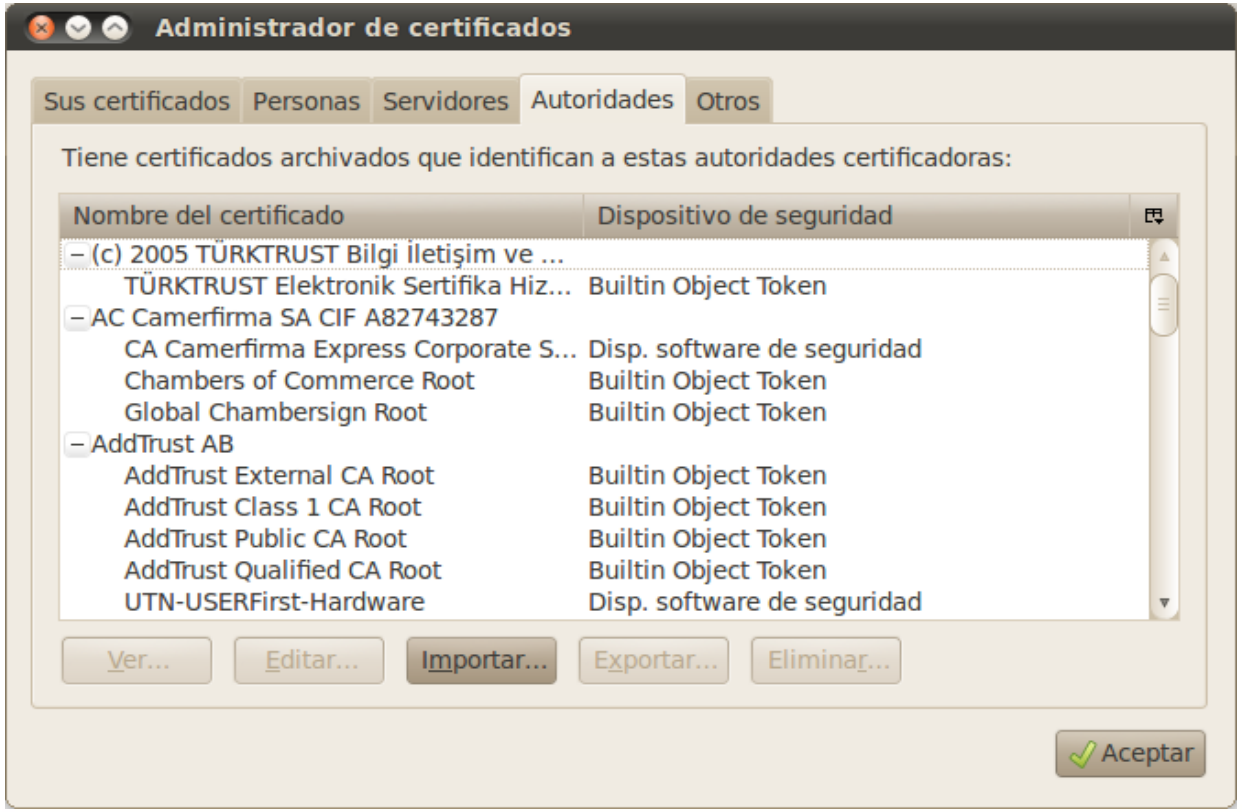
Servicios de seguridad:

- Autenticación del servidor
- Cifrado de datos
- Opcional – Autenticación del cliente

Capa de Socket Seguros (SSL)

Autenticación del servidor:

1. Los navegadores incluyen claves públicas de autoridades de certificación de confianza



Capa de Socket Seguros (SSL)

Autenticación del servidor:

2. El navegador solicita su certificado al servidor, que habrá sido emitido por alguna autoridad de certificación de confianza

3. El navegador utiliza la clave pública de CA para extraer del certificado la clave pública del servidor

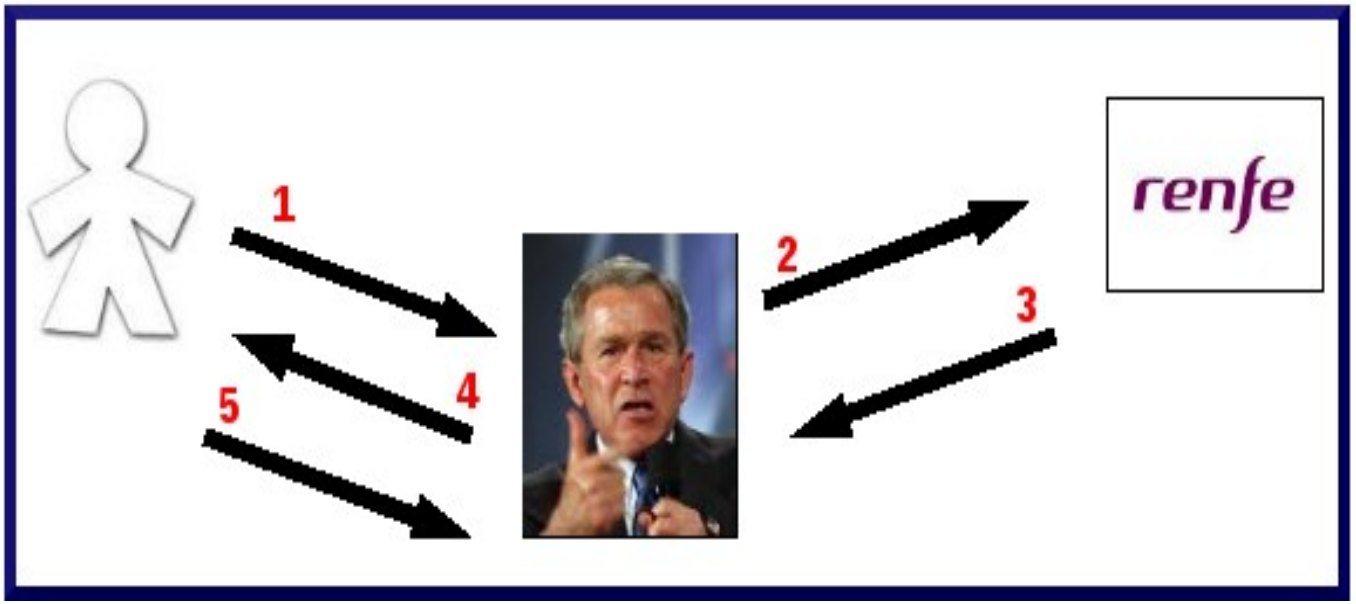
Capa de Socket Seguros (SSL)

Sesión SSL cifrada:

1. El navegador genera una clave de sesión simétrica, la cifra con la clave pública del servidor (que acaba de obtener del certificado) y se la envía al servidor.
2. Con su clave privada, el servidor descifra el mensaje y obtiene la clave de sesión.
3. El navegador y el servidor conocen la clave de sesión, con la que cifrarán todos los datos que tengan que intercambiar

Ejercicio

Un usuario inocente quiere comprar un billete en renfe.es, pero un atacante malvado (por ejemplo, G.W. Bush) le ha hecho un ataque MITM.



Ejercicio

1. Cuando el navegador del usuario envía un mensaje a renfe.es pidiéndole el certificado, en realidad ese mensaje le llega a Bush.

2. Para que nadie note nada, el sr. Bush (una persona de gran inteligencia) reenvía la petición a renfe.es.

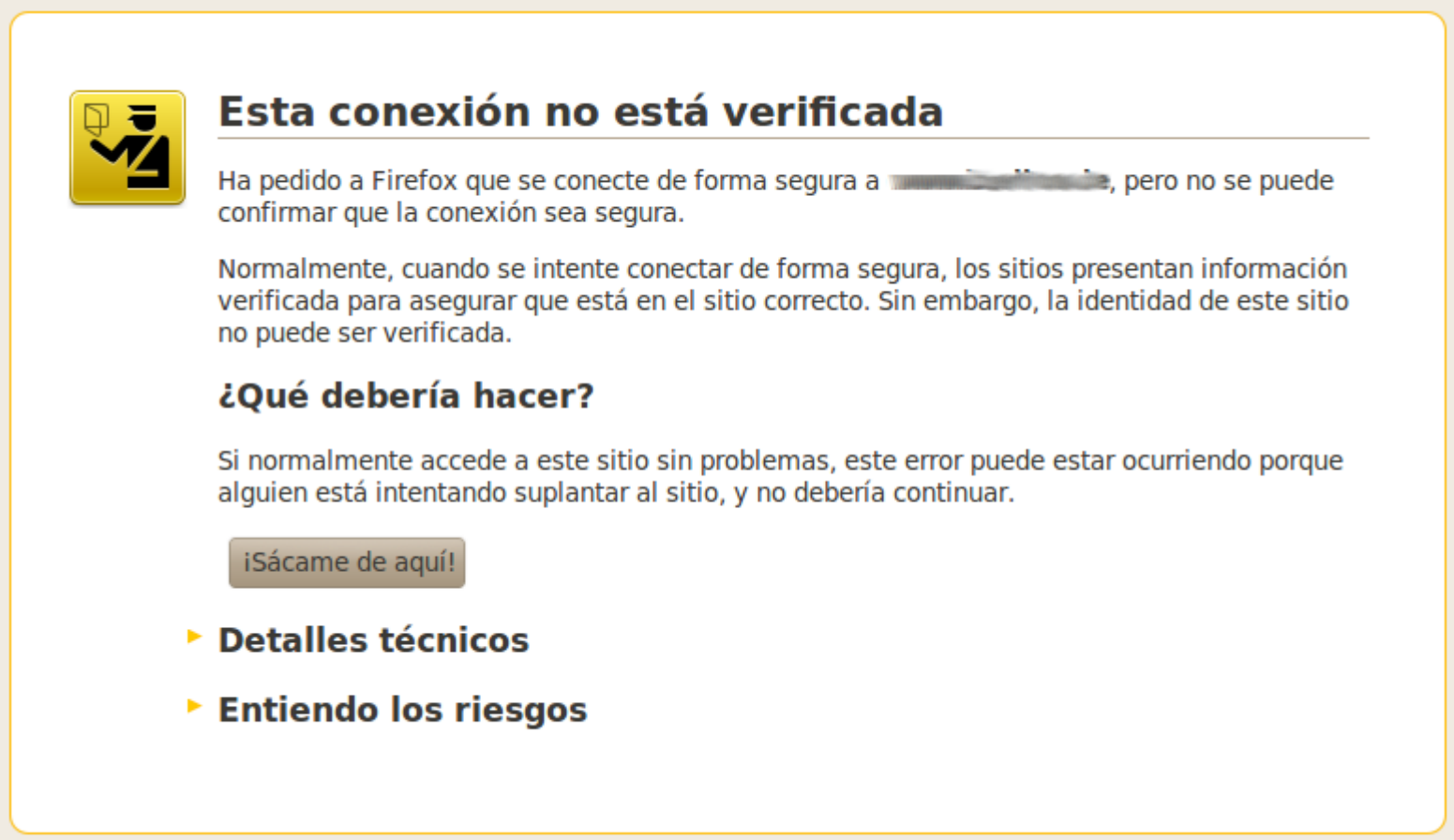
3. renfe.es envía su certificado al usuario, aunque el mensaje llega de nuevo a Bush.

4. Bush envía el certificado al usuario inocente.

5. Llega el momento clave. El navegador del usuario va a generar la clave de sesión que usará para cifrar toda la comunicación con renfe.es y poder enviar los datos bancarios con tranquilidad, pero el sr. bush ha interceptado el mensaje.

¿Funcionaría este ataque y podría obtener Bush los datos bancarios del usuario inocente?

Ejercicio


Esta conexión no está verificada
Ha pedido a Firefox que se conecte de forma segura a [redacted], pero no se puede confirmar que la conexión sea segura.
Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.
¿Qué debería hacer?
Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.
¡Sácame de aquí!
Detalles técnicos
Entiendo los riesgos

Lecturas

- Mitos y leyendas: "Compruebe el candadito del navegador para estar seguro" I (Phishing) → artículo
- Mitos y leyendas: "Compruebe el candadito del navegador para estar seguro" II (Troyanos) → artículo
- Investigadores consiguen hacer que cualquier certificado SSL parezca válido → artículo