Autenticación

Miguel Angel Astor Romero

12 de julio de 2019

Agenda

Introducción

Razonemos:

Introducción

Razonemos:

- ¿Que es la autenticación?

Introducción

Razonemos:

- ¿Que es la autenticación?
- ¿Por que es necesario autenticar?

Introducción

Razonemos:

- ¿Que es la autenticación?
- ¿Por que es necesario autenticar?
- ¿A quién vamos a autenticar?

Introducción

Razonemos:

- ¿Que es la autenticación?
- ¿Por que es necesario autenticar?
- ¿A quién vamos a autenticar?
- ¿Quién realiza el proceso de autenticación?

Definición

Definición de Autenticación

Se refiere a las políticas y mecanismos que permiten verificar la identidad de los participantes de una comunicación.

Definición

Definición de Autenticación

Se refiere a las políticas y mecanismos que permiten verificar la identidad de los participantes de una comunicación.

Enfoques

1. Confiar en que cada cliente asegurará la identidad del usuario. Cada servicio debe establecer políticas que verifiquen la identidad del usuario.
2. Exigir que el cliente se autentique ante los servicios, pero confiar en la identidad del usuario humano.
3. Exigir la autenticación del usuario humano ante cada servicio, y de cada servicio de cara a los usuarios.

Tipos de Autenticación

Se pueder realizar dos tipos de autenticación

Tipos de Autenticación

Se pueder realizar dos tipos de autenticación

Autenticación de Mensajes

Proceso que permite la verificación de que un mensaje ha sido emitido por quien dice ser su autor, y que además no ha sido:

- Alterado en tránsito.
- Retrasado o repetido de forma artificial.

Tipos de Autenticación

Se pueder realizar dos tipos de autenticación

Autenticación de Mensajes

Proceso que permite la verificación de que un mensaje ha sido emitido por quien dice ser su autor, y que además no ha sido:

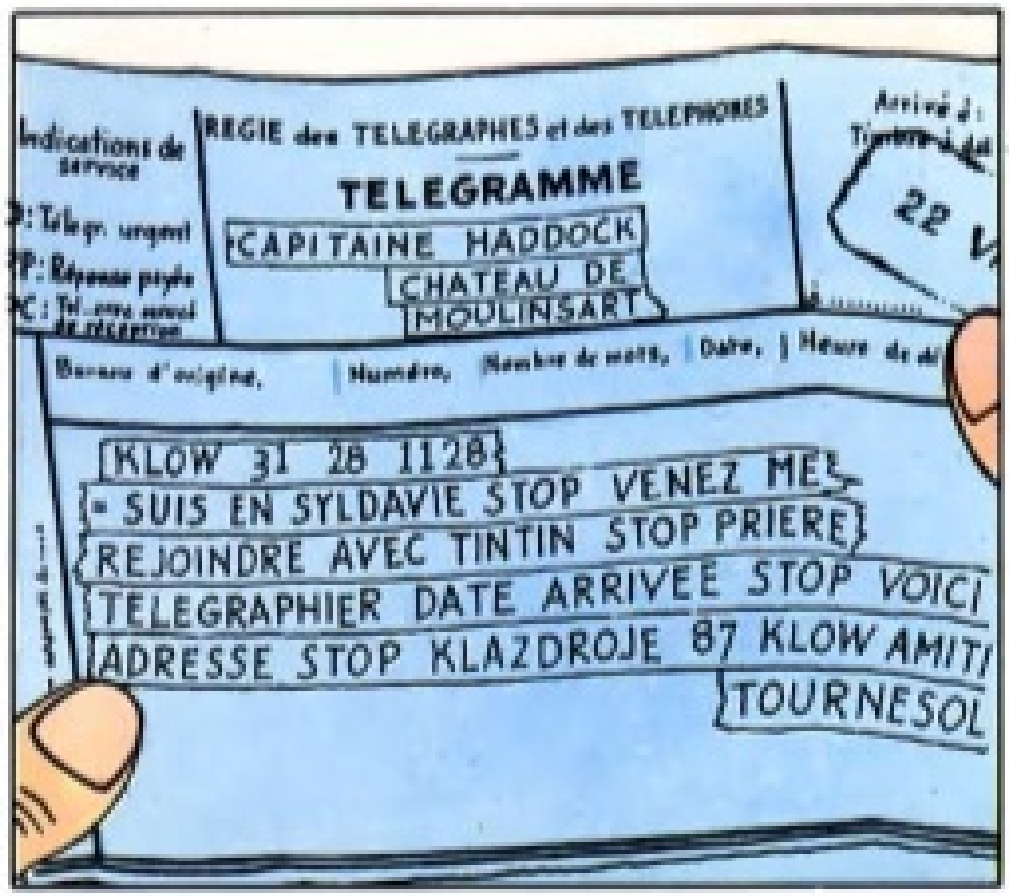
- Alterado en tránsito.
- Retrasado o repetido de forma artificial.

Autenticación de Usuarios

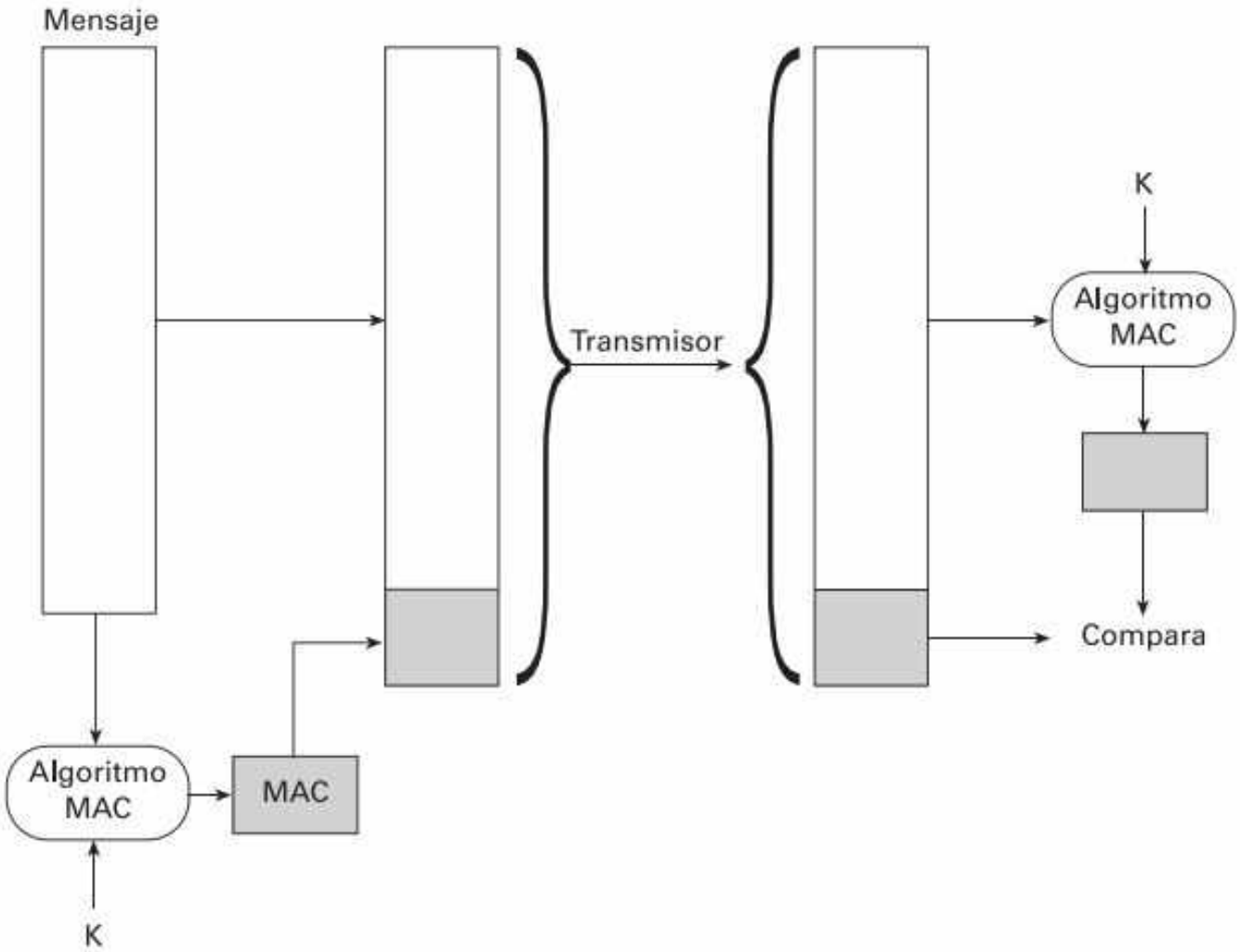
Proceso que permite verificar la identidad de otros pares en un proceso de comunicación.

- En particular se usa para identificar al dueño de una clave pública específica.

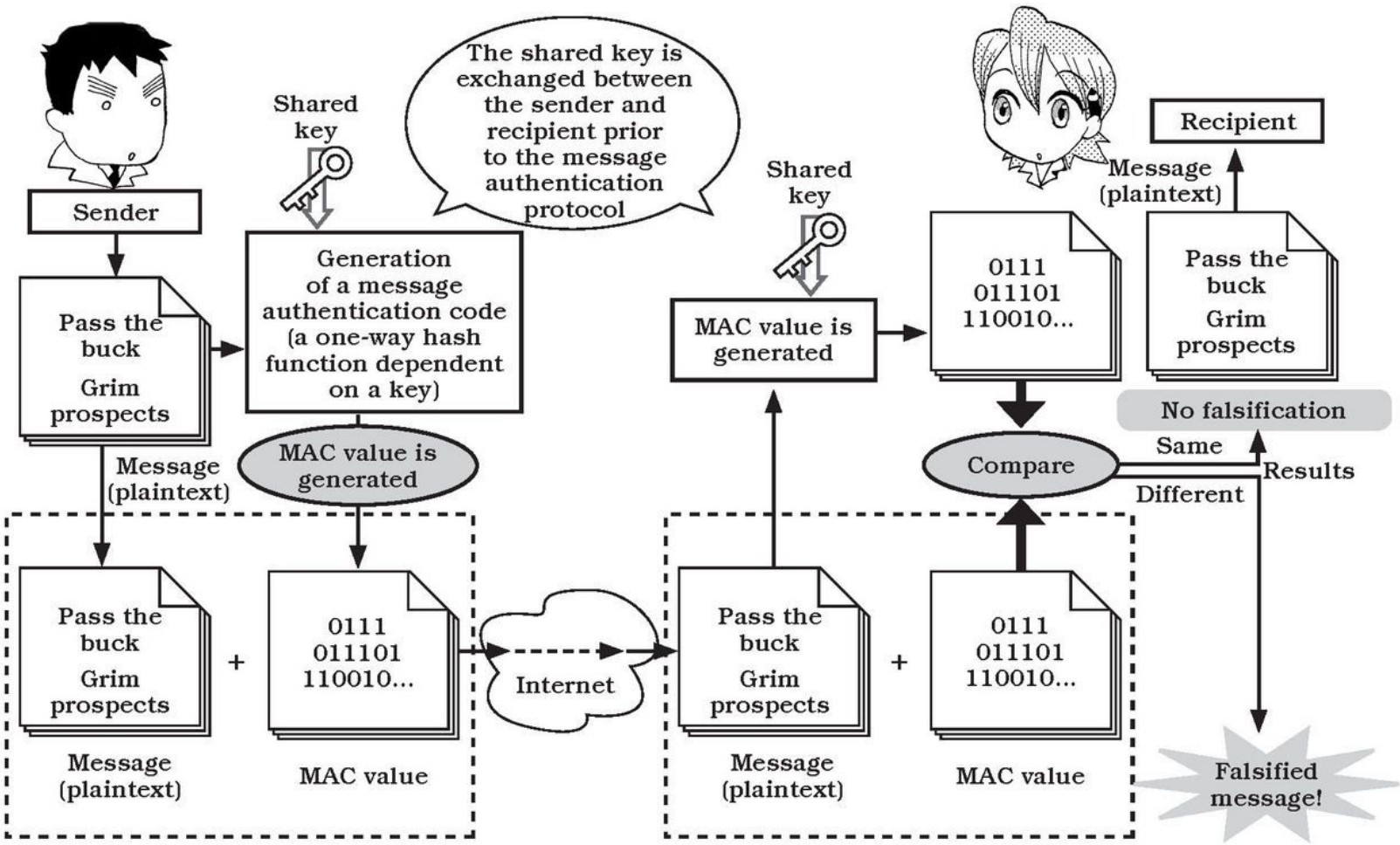

Un télégramme pour vous, Monsieur...
Pour moi ?... Comment sait-on déjà que je suis rentré ?...


REGIE des TELEGRAPHES et des TELEPHONES
TELEGRAMME
CAPITAINE HADDOCK
CHATEAU DE MOULINSART
KLOW 31 28 1128
SUIS EN SYLDAVIE STOP VENEZ ME REJOINDRE AVEC TINTIN STOP PRIERE TELEGRAPHIER DATE ARRIVEE STOP VOICI ADRESSE STOP KLAZDROJE 87 KLOW AMITI
TOURNESOL

Códigos de Autenticación de Mensajes - MAC



Procedimiento de Verificación de un Mensaje con MAC



Funciones Hash

Tambien conocidas como funciones compendio o *digest*.

Requisitos

1. Pueden aplicarse a bloques de datos de cualquier tamaño.
2. Producen salidas de tamaño fijo.
3. $h = H(x)$ es facil de calcular para cualquier mensaje x dado.
4. Dado $h = H(x)$, es imposible obtener el valor de x.
5. Debe ser imposible encontrar un $y \neq x$ tal que $H(y) = H(x)$.

Funciones Hash Modernas

- SHA-256
- Keccak
- SHA-3
- RIPE-MD
- Whirlpool
- bcrypt

Códigos HMAC

$$HMAC_K(M) = H[(K^+ \oplus opad) \| H[(K^+ \oplus ipad) \| M]]$$

Donde:

- H Función *hash* embebida.
- M Mensaje de entrada.
- K Clave secreta.
- K^+ Clave extendida a longitud de un bloque (b).
- $opad$ El byte 0x36 repetido $b/8$ veces.
- $ipad$ El byte 0x5C repetido $b/8$ veces.

Problemas con los Códigos MAC

DRAWBACKS OF MESSAGE AUTHENTICATION CODES

Repudiation is the ability to deny being the sender of a message. For example, a message and MAC value are sent from A to B, and afterward A claims, "I didn't send this message to B. B made this up." There's no way to disprove A's statement, and even if B enlisted the help of a third party to find out the truth, this third party wouldn't have a way to determine whether the message and MAC value were generated by A or by B.

When a message is sent from A to B, B can't verify to a third party C that the message was sent from A. This is because the message and MAC value can be generated by either A or B. In other words, C is unable to determine whether the MAC value was generated by A or B.

Kerberos

- Protocolo de autenticación diseñado en el MIT como parte del proyecto Athena.
- La primera versión pública es Kerberos 4, publicada a finales de los 80.
- Actualmente en la versión 5.
- Las versiones 1 a 3 fueron de desarrollo interno en el MIT.
- Usa únicamente cifrado de clave compartida.

Un Diálogo de Autenticación Simple

$$
\begin{aligned}
(1) \quad & C \rightarrow AS: \quad ID_C \| P_C \| ID_V \\
(2) \quad & AS \rightarrow C: \quad Ticket \\
(3) \quad & C \rightarrow V: \quad ID_C \| Ticket
\end{aligned}
$$

$$Ticket = E_{K_V}[ID_C \| AD_C \| ID_V]$$

Donde:

- C Cliente
- AS Servidor de Autenticación
- V Servicio
- ID_C Identidad de C
- ID_V Identidad de V
- P_C Contraseña de C
- AD_C Dirección de red de C
- K_v Clave compartida por AS y V

Problemas con el Diálogo Simple

Problemas con el Diálogo Simple

1. La contraseña se transmite en claro.

Problemas con el Diálogo Simple

1. La contraseña se transmite en claro.
2. El usuario tiene que colocar su contraseña cada vez que solicita un servicio.

Problemas con el Diálogo Simple

1. La contraseña se transmite en claro.
2. El usuario tiene que colocar su contraseña cada vez que solicita un servicio.

Posibles soluciones:

1. Generar y compartir claves de sesión en lugar de transmitir la clave compartida.
2. Permitir la reutilización del ticket de autenticación para un mismo tipo de servicio.

Diálogo de Autenticación Avanzado

Una vez por sesión de usuario

(1) $C \rightarrow AS: \quad ID_C \| ID_tgs$

(2) $AS \rightarrow C: \quad E_{K_C}[Ticket_{tgs}]$

Una vez por tipo de servicio

(3) $C \rightarrow TGS: \quad ID_C \| ID_V \| Ticket_{tgs}$

(4) $TGS \rightarrow C: \quad Ticket_V$

Una vez por sesión de servicio

(5) $C \rightarrow V: \quad ID_C \| Ticket_V$

$$Ticket_{tgs} = E_{K_{tgs}}[ID_C \| AD_C \| ID_{tgs} \| TS_1 \| TTL_1]$$

$$Ticket_V = E_{K_V}[ID_C \| AD_C \| ID_V \| TS_2 \| TTL_2]$$

Donde:

- TGS Servicio de tickets
- K_C Clave de sesión
- TS Marca de tiempo
- TTL Tiempo de vida

Problemas con el Diálogo Avanzado

Problemas con el Diálogo Avanzado

1. Es posible suplantar la identidad de un usuario dentro de la ventana de una sesión de usuario.

Problemas con el Diálogo Avanzado

1. Es posible suplantar la identidad de un usuario dentro de la ventana de una sesión de usuario.
2. No se realiza autenticación de los servicios ante el cliente.

Problemas con el Diálogo Avanzado

1. Es posible suplantar la identidad de un usuario dentro de la ventana de una sesión de usuario.

2. No se realiza autenticación de los servicios ante el cliente.

Soluciones:

1. Usar claves de sesión adicionales para verificar las identidades de:
   1. El usuario C ante el TGS.
   2. El servicio V ante el usuario C.

Esquema de Mensajes de Kerberos 4

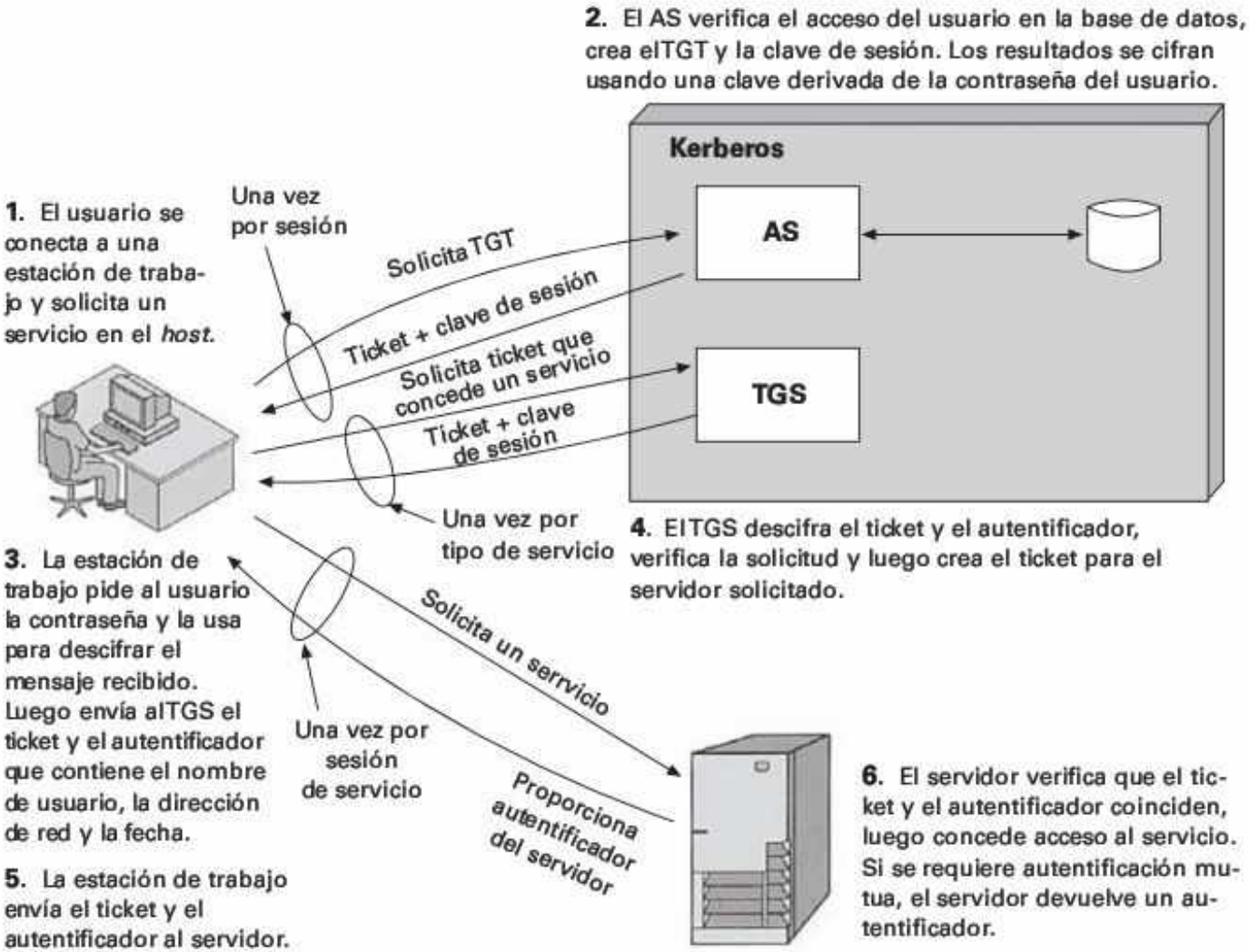


Figura 4.1 Esquema general de Kerberos

Diálogo de Autenticación de Kerberos 4

(a) Intercambio de servicio de autentificación: para obtener un TGT

(1) C → AS: $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C: $E_{Kc}[K_{c,tgs} \| ID_{tgs} \| TS_2 \| Tiempo\ de\ vida_2 \| Ticket_{tgs}]$

$Ticket_{tgs} = E_{Ktgs}[K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Tiempo\ de\ vida_2]$

(b) Intercambio de TGS: para obtener un ticket que concede un servicio

(3) C → TGS: $ID_v \| Ticket_{tgs} \| Autentificador_c$

(4) TGS → C: $E_{Kc,tgs}[K_{c,v} \| ID_v \| TS_4 \| Ticket_v]$

$Ticket_{tgs} = E_{Ktgs}[K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Tiempo\ de\ vida_2]$

$Ticket_v = E_{Kv}[K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Tiempo\ de\ vida_4]$

$Autentificador_c = E_{Kc,tgs}[ID_C \| AD_C \| TS_3]$

(c) Intercambio de autentificación cliente/servidor: para obtener un servicio

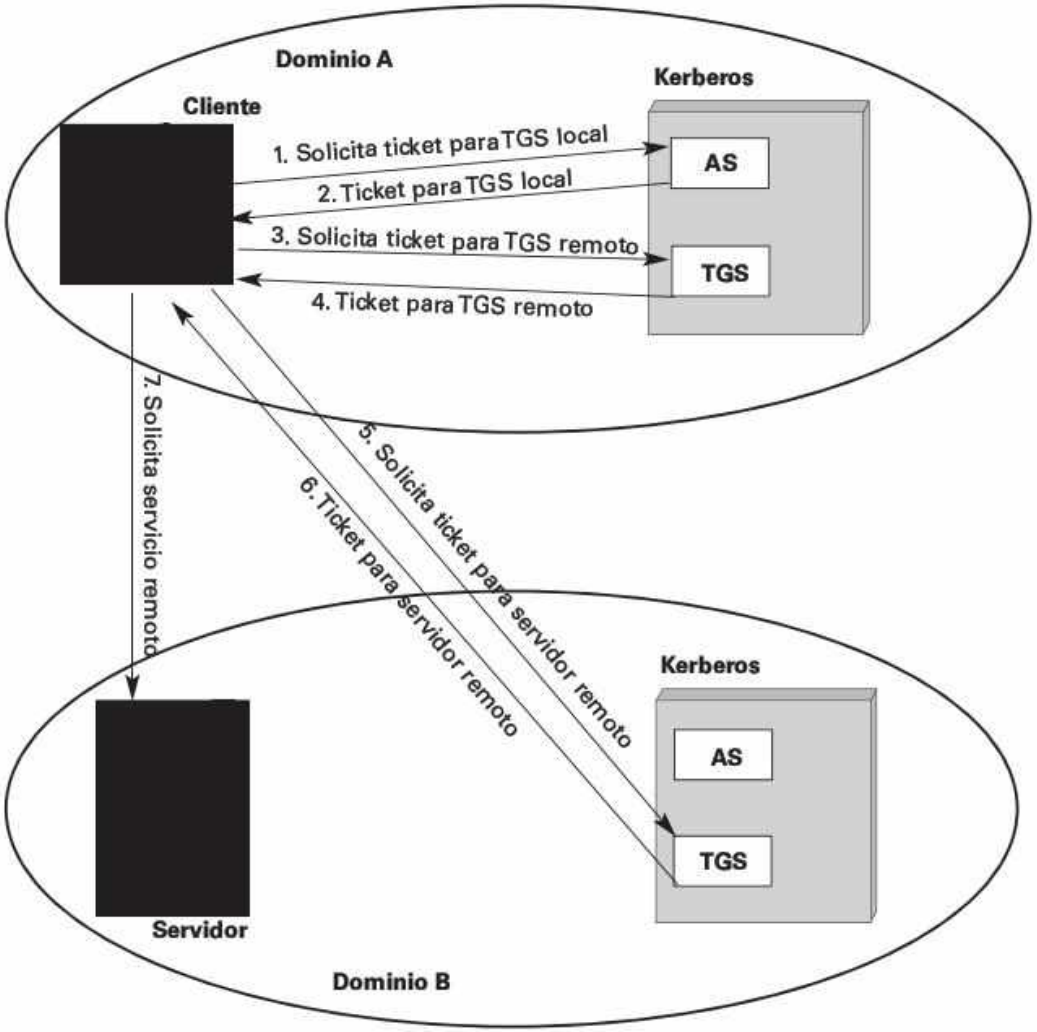
(5) C → V: $Ticket_v \| Autentificador_c$

(6) V → C: $E_{Kc,v}[TS_5 + 1]$ (para autentificación mutua)

$Ticket_v = E_{Kv}[K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Tiempo\ de\ vida_4]$

$Autentificador_c = E_{Kc,v}[ID_C \| AD_C \| TS_5]$

Kerberos 4 en Múltiples Dominios



Problemas de Entorno en Kerberos 4

1. Solo admite cifrado DES en modo PCBC no estándar.
2. Usa direcciones IP explícitamente.
3. Declaración de ordenamiento de bytes no estándar.
4. Tiempos de vida solo pueden especificarse en bloques de 5 minutos y tiene un límite de 21 horas por sesión de usuario/servicio.
5. No admite delegación de identidades.
6. Autenticarse ante N dominios requiere N^2 relaciones.

Problemas Técnicos en Kerberos 4

1. Uso de doble cifrado innecesariamente.
2. Uso de DES en modo PCBC no estándar y susceptible a ataques.
3. Reutilización de claves de sesión es susceptible a ataques de repetición.
4. Las claves de sesión son susceptibles de romperse por fuerza bruta con relativa facilidad.

Para resolver estos problemas se plantea el protocolo Kerberos 5:

RFC 4120 *The Kerberos Network Authentication Service (V5)*

Kerberos 5

(a) Intercambio de servicio de autentificación: para obtener el TGT

(1) C → AS: $Opciones \| ID_C \| Dominio_c \| ID_{tgs} \| Tiempos \| Nonce_1$

(2) AS → C: $Dominio_c \| ID_C \| Ticket_{tgs} \| E_{Kc}[K_{c,tgs} \| Tiempos \| Nonce_1 \| Dominio_{tgs} \| ID_{tgs}$

$Ticket_{tgs} = E_{K_{tgs}}[Indicadores \| K_{c,tgs} \| Dominio_c \| ID_C \| AD_C \| Tiempos]$

(b) Intercambio de TGS: para obtener un ticket que concede un servicio

(3) C → TGS: $Opciones \| ID_v \| Tiempos \| Nonce_2 \| Ticket_{tgs} \| Autentificador_c$

(4) TGS → C: $Dominio_c \| ID_C \| Ticket_v \| E_{K_{c,tgs}}[K_{c,v} \| Tiempos \| Nonce_2 \| Dominio_v \| ID_V]$

$Ticket_{tgs} = E_{K_{tgs}}[Indicadores \| K_{c,tgs} \| Dominio_c \| ID_C \| AD_C \| Tiempos]$

$Ticket_v = E_{Kv}[Indicadores \| K_{c,v} \| Dominio_c \| ID_C \| AD_C \| Tiempos]$

$Autentificador_c = E_{K_{c,tgs}}[ID_C \| Dominio_c \| TS_1]$

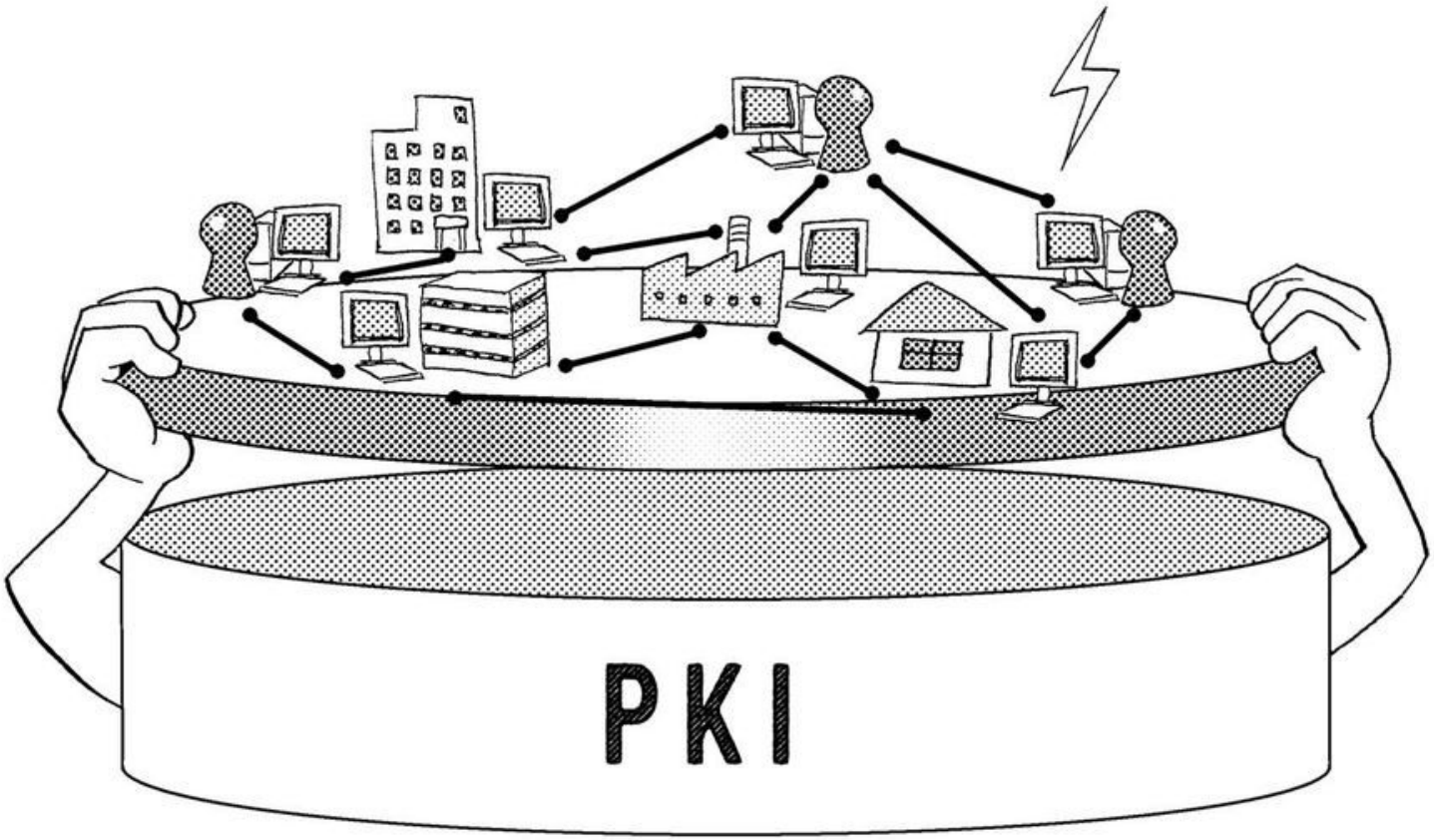
(c) Intercambio de autentificación cliente/servidor: para obtener servicio

(5) C → V: $Opciones \| Ticket_v \| Autentificador_c$

(6) V → C: $E_{K_{c,v}}[TS_2 \| Subclave \| Seq\#]$

$Ticket_v = E_{Kv}[Indicadores \| K_{c,v} \| Dominio_c \| ID_C \| AD_C \| Tiempos]$

$Autentificador_c = E_{K_{c,v}}[ID_C \| Dominio_c \| TS_2 \| Subclave \| Seq\#]$


PKI

Serie ITU-T X.500

La serie X.500 de recomendaciones de la ITU-T definen un servicio de directorios:

Número ITU-T	Número ISO	Título del estándar
X.500	9594-1	Conceptos, modelos y servicios
X.501	9594-2	Modelos
X.509	9594-8	Certificados de claves públicas
X.511	9594-3	Definición de servicios abstractos
X.518	9594-4	Procedimiento de operación distribuida
X.519	9594-5	Especificación de protocolos
X.520	9594-6	Tipos de atributos seleccionados
X.521	9594-7	Clases de objetos seleccionados
X.525	9594-9	Replicación
X.530	9594-10	Administración del directorio

Norma ITU-T X.509

- La recomendación X.509 define las siguientes estructuras:

  Certificado digital documento firmado por una autoridad confiable que valida la identidad del dueño de una clave pública específica.

  Lista de revocación lista de certificados revocados por una autoridad.

- También define tres modos de autenticación: unidireccional, bidireccional y tridireccional.

Norma ITU-T X.509

- La recomendación X.509 define las siguientes estructuras:

  Certificado digital documento firmado por una autoridad confiable que valida la identidad del dueño de una clave pública específica.

  Lista de revocación lista de certificados revocados por una autoridad.

- También define tres modos de autenticación: unidireccional, bidireccional y tridireccional.

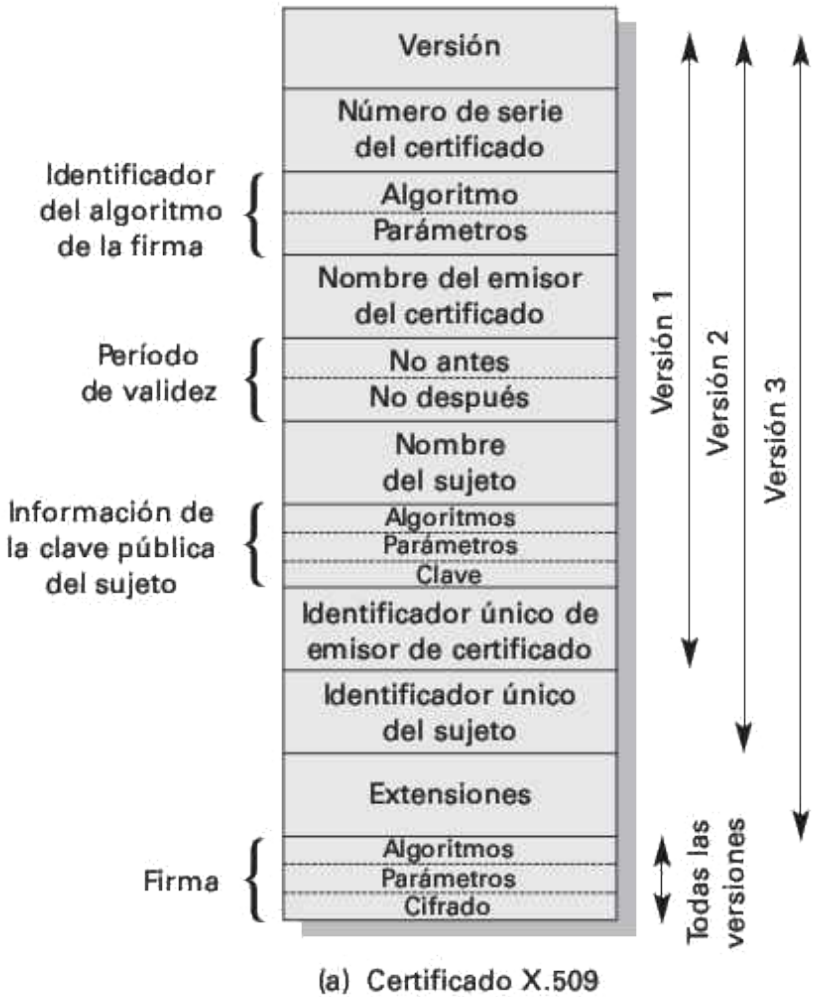
Uso en protocolos de Internet

- RFC 8446 TSL 1.3 y versiones anteriores.
- RFC 4301 IPsec.
- RFC 8550 S/MIME 4.0 y versiones anteriores.

Estructura de un Certificado X.509

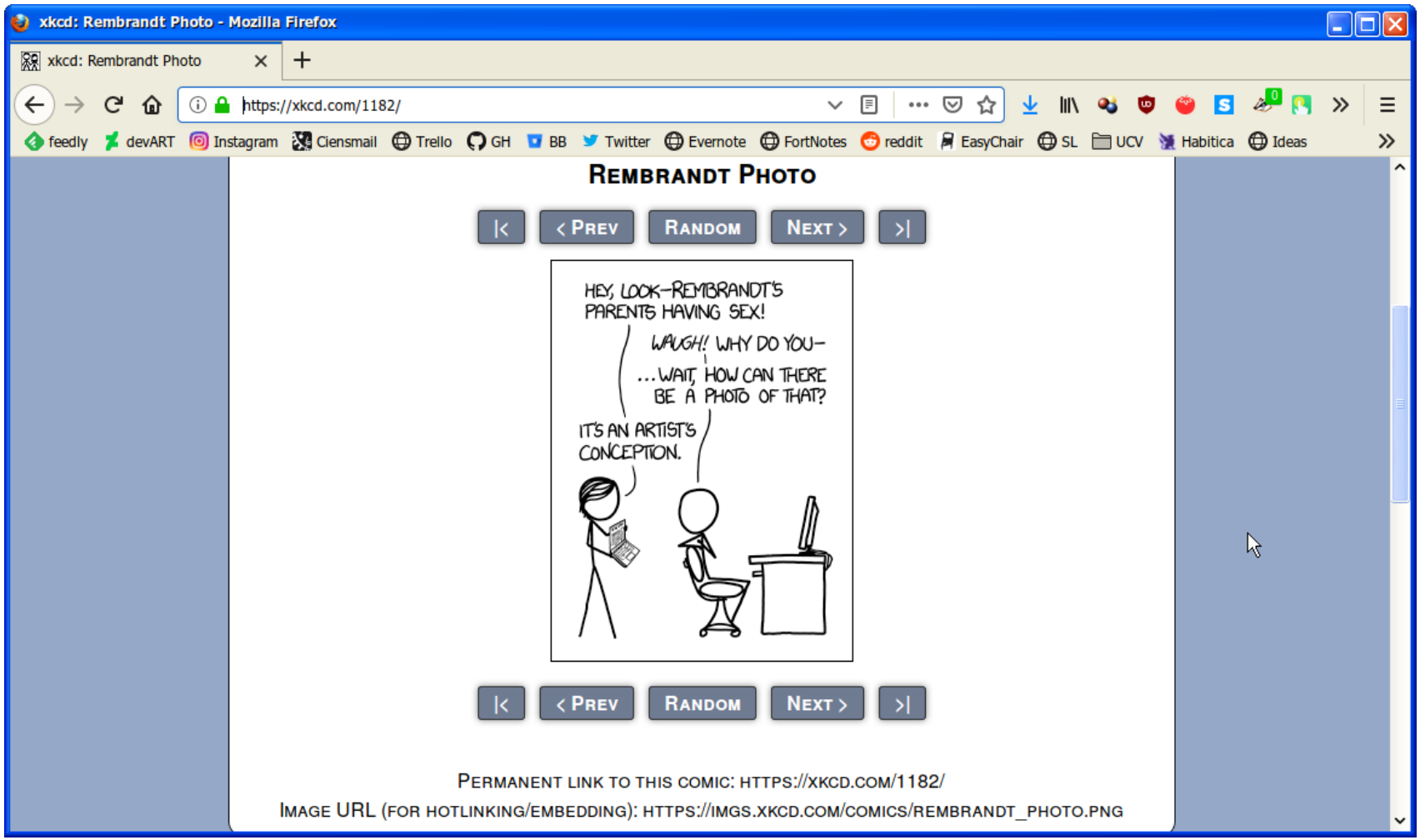
Campos Importantes

- Versión.
- Número de serie.
- Emisor.
- Período de validez.
- Sujeto.
- Clave pública del sujeto.
- Identificadores únicos (x2).
- Firma.

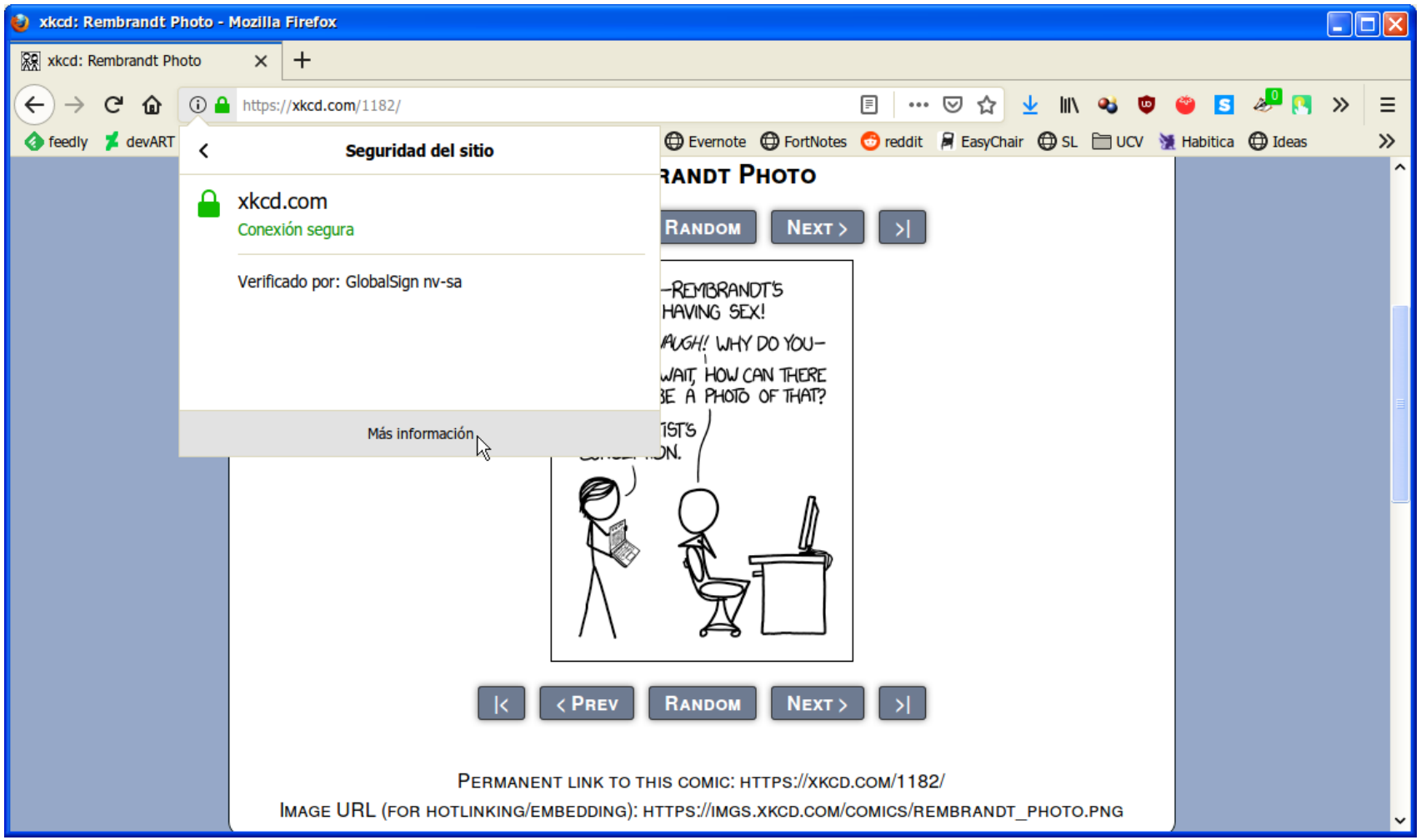


(a) Certificado X.509

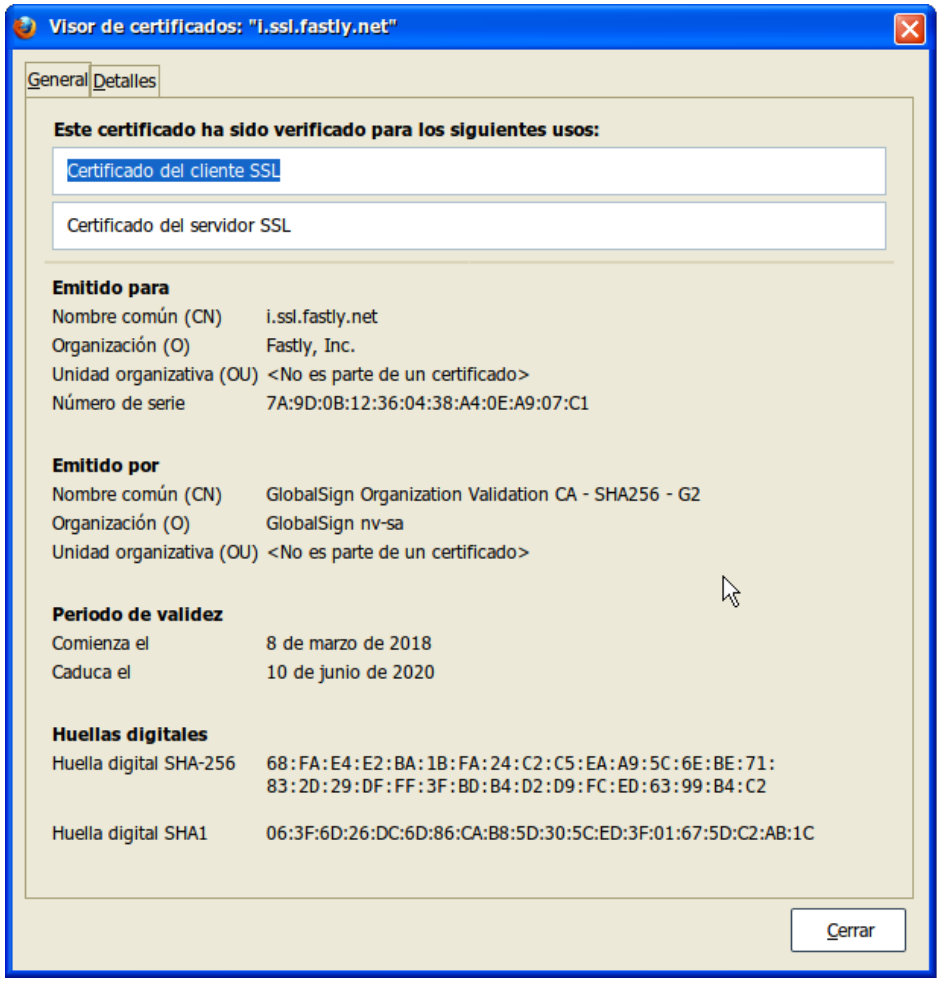
Observando un Certificado X.509 Manualmente - 1/3

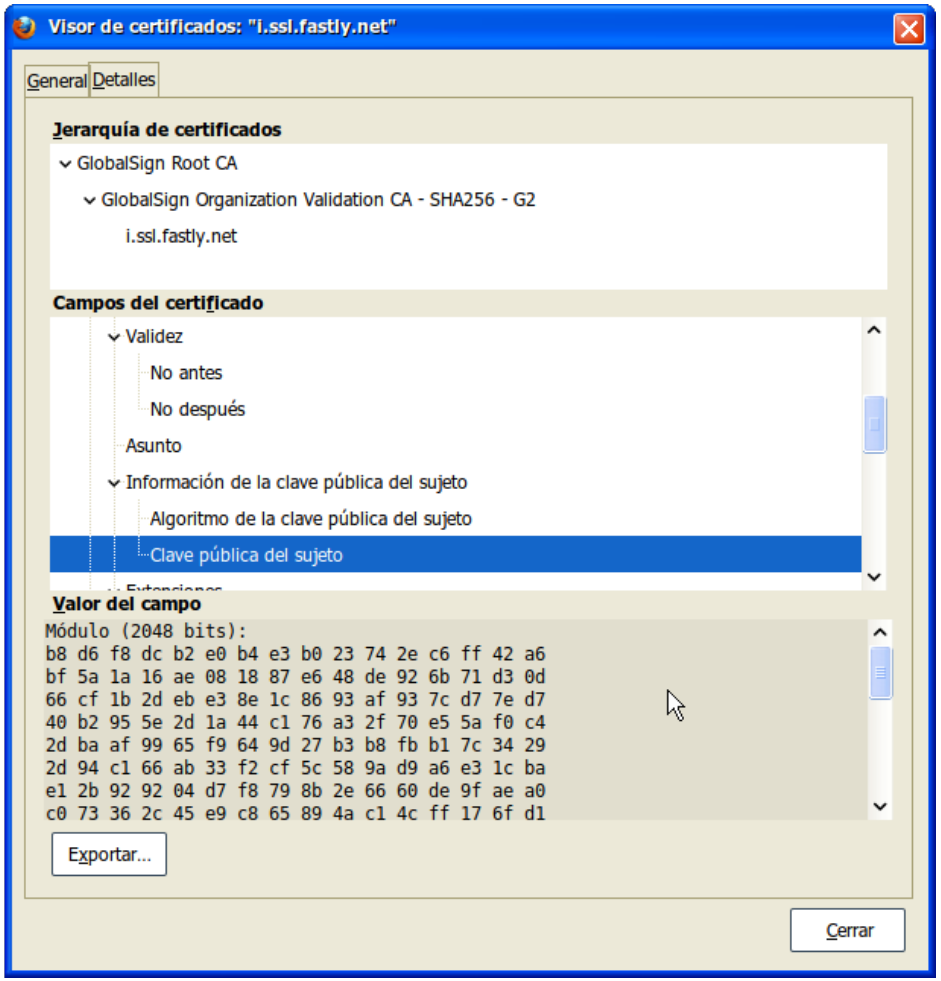


Observando un Certificado X.509 Manualmente - 2/3



Observando un Certificado X.509 Manualmente - 3/3





Procedimientos de Autenticación con X.509

Dados A y B que desean autenticarse, X.509 establece los siguientes modos:

Procedimientos de Autenticación con X.509

Dados A y B que desean autenticarse, X.509 establece los siguientes modos:

Autenticación Unidireccional

1. La identidad de A.
2. Que los mensajes emitidos por A son auténticos.
3. Que los mensajes de A van dirigidos a B.
4. La integridad y originalidad de los mensajes de A.

Procedimientos de Autenticación con X.509

Dados A y B que desean autenticarse, X.509 establece los siguientes modos:

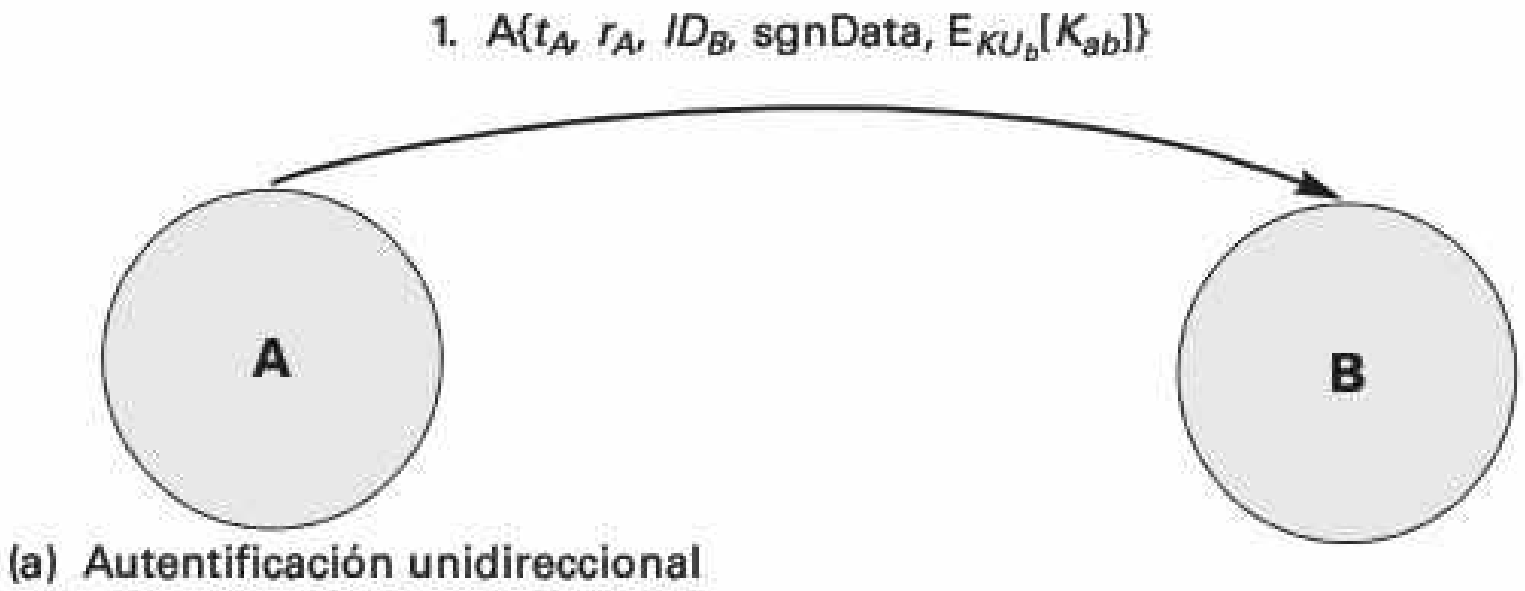
Autenticación Unidireccional

1. La identidad de A.
2. Que los mensajes emitidos por A son auténticos.
3. Que los mensajes de A van dirigidos a B.
4. La integridad y originalidad de los mensajes de A.

Autenticación Mutua o Bidireccional

1. La identidad de B.
2. Que los mensajes emitidos por B son auténticos.
3. Que los mensajes de B van dirigidos hacia A.
4. La integridad y originalidad de los mensajes de B.

Autenticación Unidireccional



(a) Autentificación unidireccional

t_A marca de tiempo.

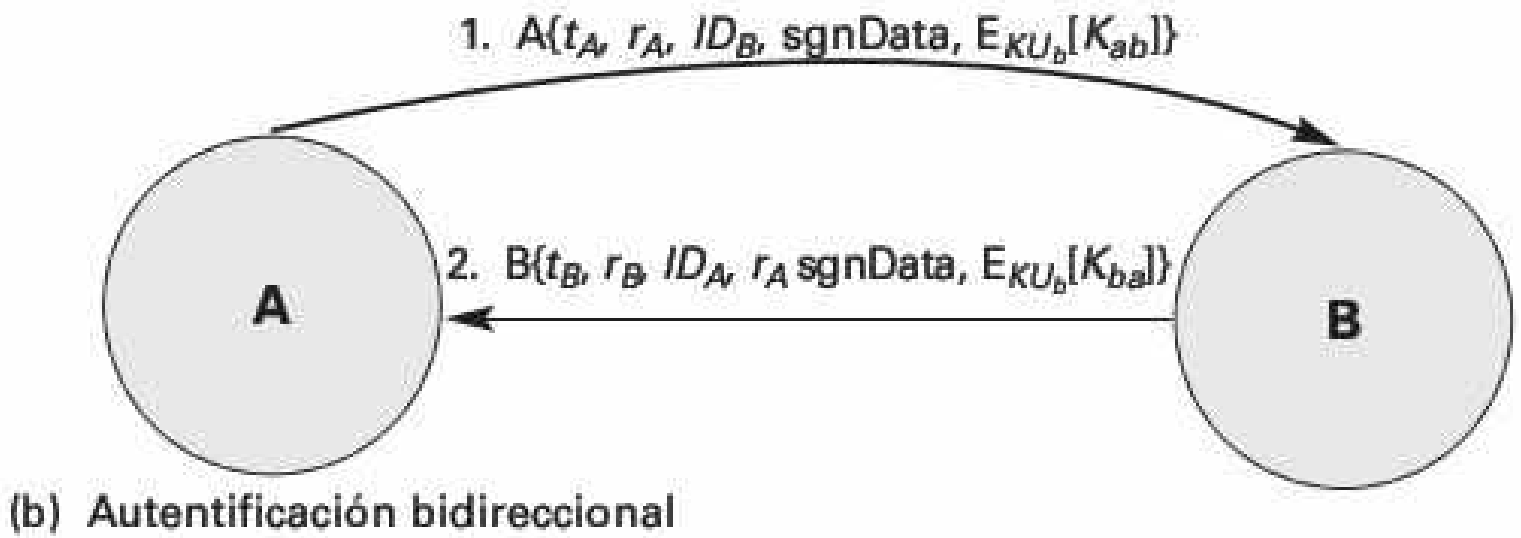
r_A *nonce*.

ID_B identidad de B.

sgnData datos y firma del mensaje.

$E_{KU_a}[K_{ab}]$ clave de sesión.

Autenticación Mutua o Bidireccional

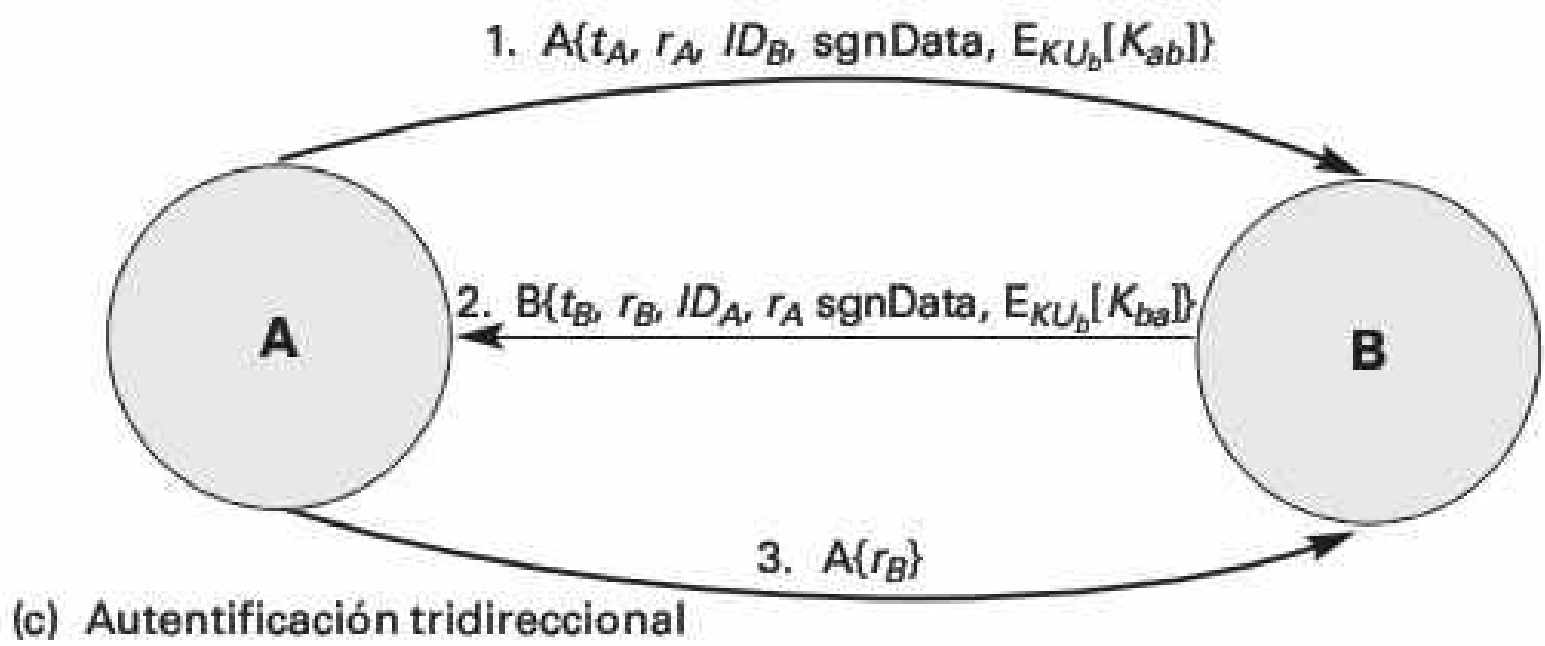


(b) Autentificación bidireccional

- t_B marca de tiempo.
- r_B *nonce*.
- ID_A identidad de A.
- $r_A sgnData$ datos y firma del mensaje.
- $E_{KU_b}[K_{ba}]$ clave de sesión.

Autenticación Tridireccional

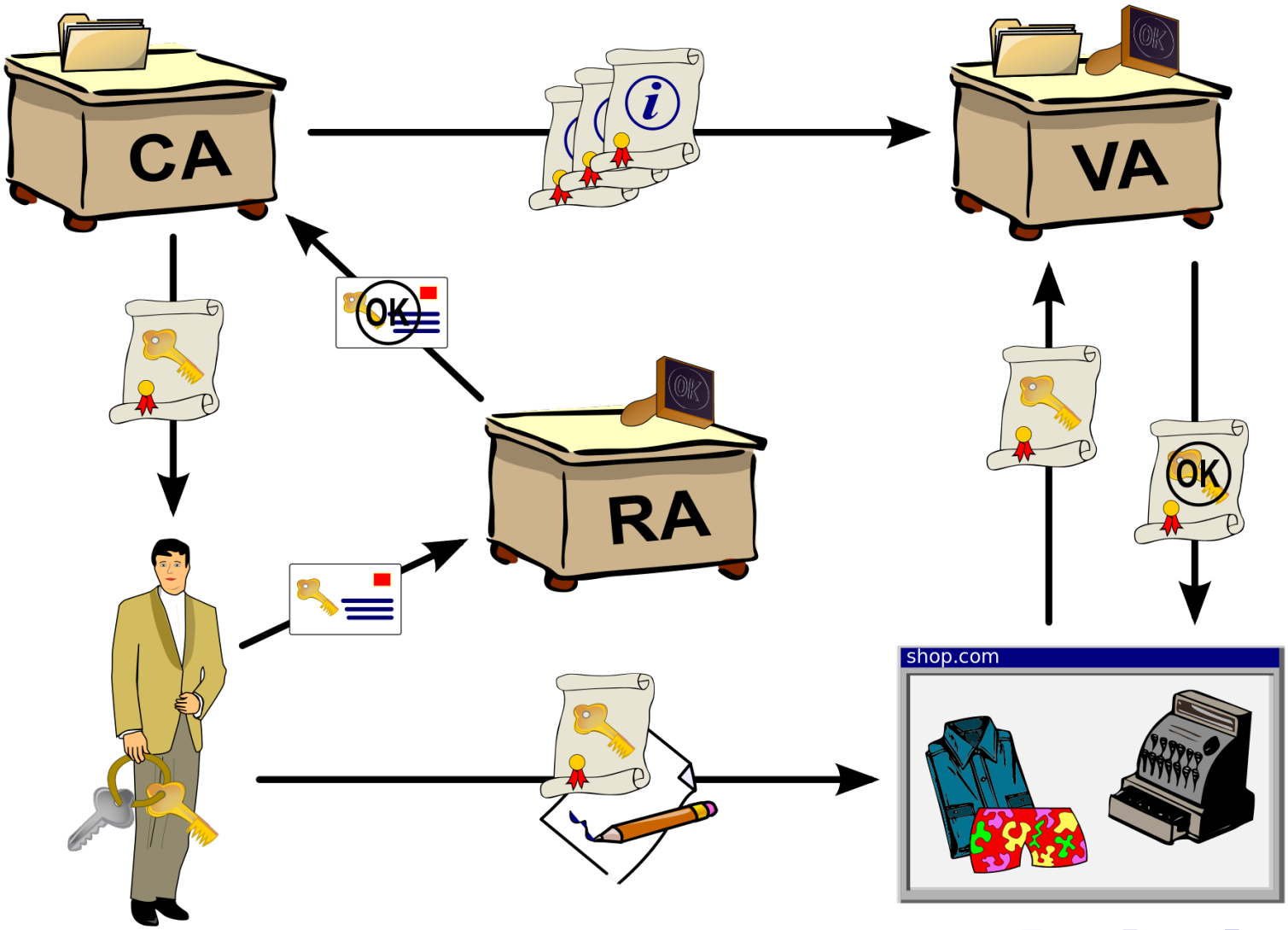
Modo adicional que provee resistencia a ataques de repetición sin necesidad de sincronización de relojes.



(c) Autentificación tridireccional

$A\{r_B\}$ copia firmada de r_B.

Certificación Digital



Obtención y Verificación de un Certificado

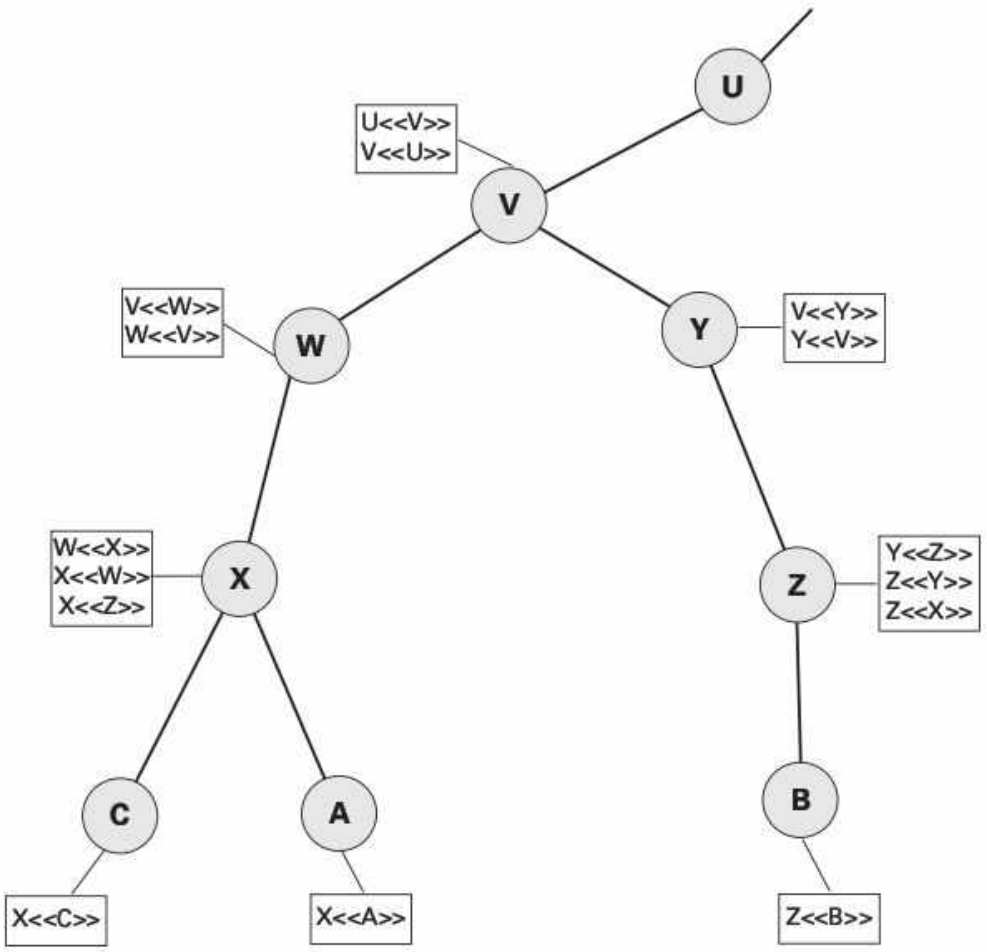


Figura 4.4 Jerarquía de X.509: un ejemplo hipotético

- En el esquema de PKI X.509 una CA puede generar certificados para autoridades intermedias las cuales a su vez pueden certificar a otras autoridades, hasta llegar al sujeto final.

Obtención y Verificación de un Certificado

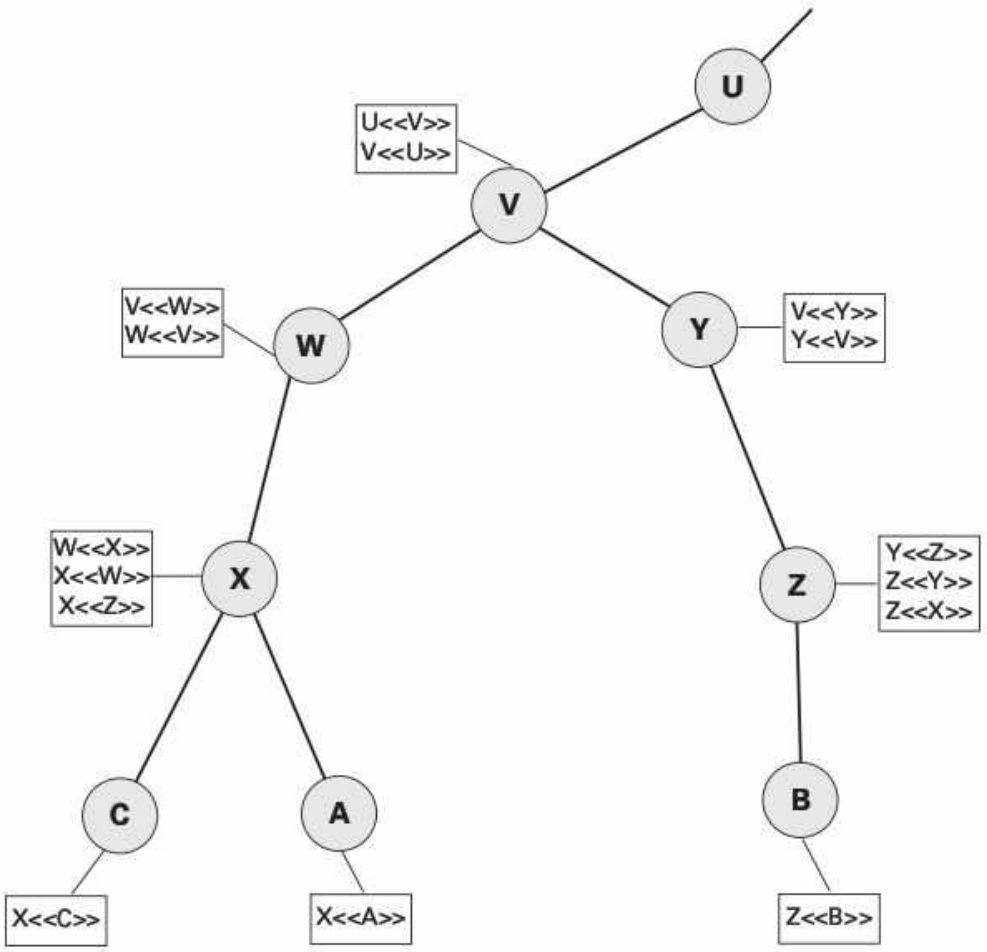


Figura 4.4 Jerarquía de X.509: un ejemplo hipotético

- En el esquema de PKI X.509 una CA puede generar certificados para autoridades intermedias las cuales a su vez pueden certificar a otras autoridades, hasta llegar al sujeto final.
- Para verificar un certificado se pide al servicio de directorio que construya una cadena de certificados.

Revocación de Certificados

Es responsabilidad del usuario el verificar si un certificado es válido.

(b) Lista de revocación de certificados

¿Por qué revocar un certificado?

Revocación de Certificados

Es responsabilidad del usuario el verificar si un certificado es válido.

(b) Lista de revocación de certificados

¿Por qué revocar un certificado?

1. Se sospecha/sabe que la clave privada del dueño del certificado está comprometida.

Revocación de Certificados

Es responsabilidad del usuario el verificar si un certificado es válido.

(b) Lista de revocación de certificados

¿Por qué revocar un certificado?

1. Se sospecha/sabe que la clave privada del dueño del certificado está comprometida.
2. El usuario ya no está certificado por la CA correspondiente.

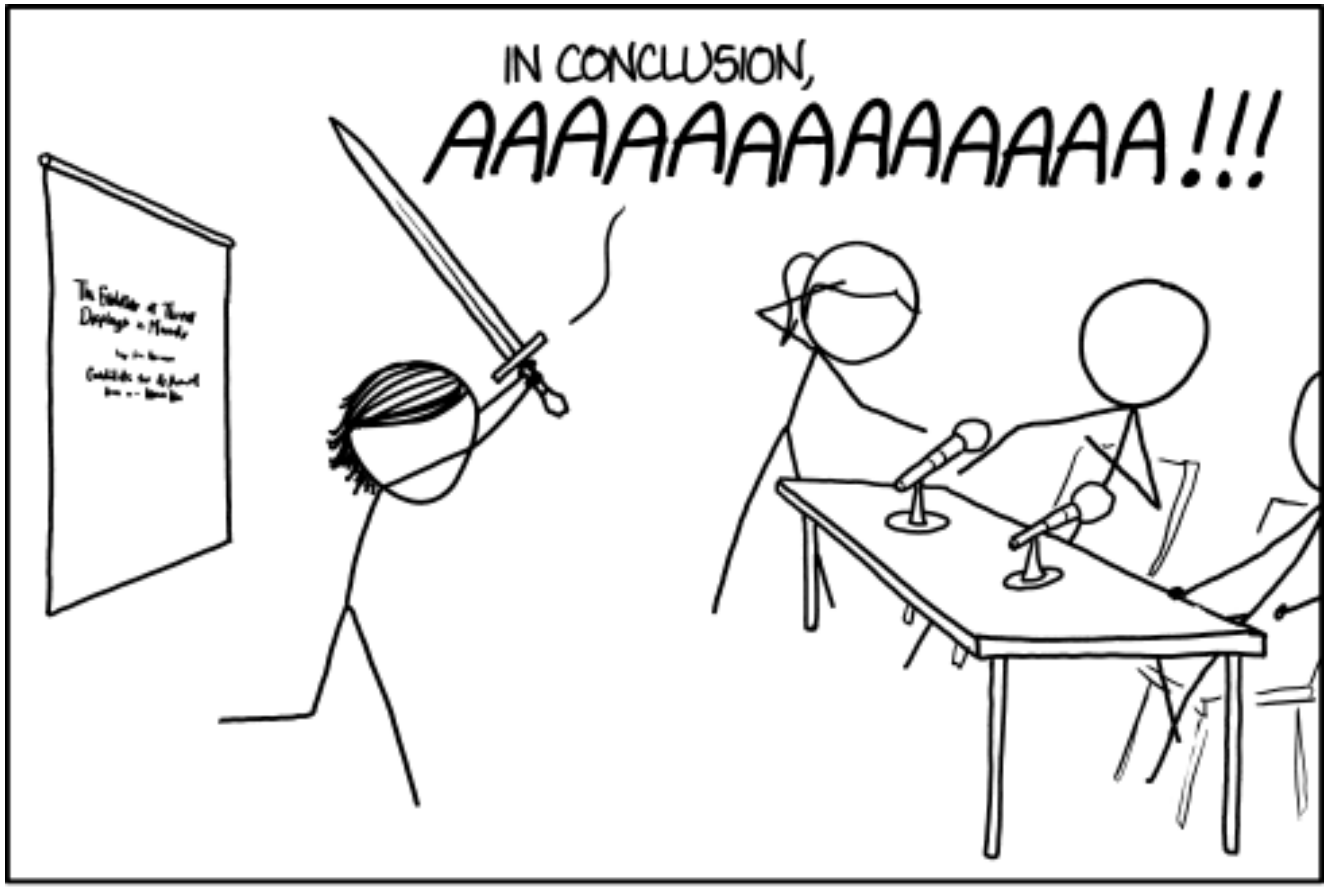
Revocación de Certificados

Es responsabilidad del usuario el verificar si un certificado es válido.

(b) Lista de revocación de certificados

¿Por qué revocar un certificado?

1. Se sospecha/sabe que la clave privada del dueño del certificado está comprometida.
2. El usuario ya no está certificado por la CA correspondiente.
3. Se sospecha/sabe que el certificado/clave privada de la CA está comprometida.



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

Conclusiones

- La autenticación se puede resolver de múltiples maneras:
  - Autenticando los mensajes individualmente.
  - Autenticando a los usuarios.
- La autenticación de usuarios puede hacerse mediante técnicas de cifrado simétrico o con cifrado de clave pública.
- Existen más técnicas de autenticación. En particular las llamadas pruebas de cero conocimiento.

Tarea

- Revisar las páginas 107 a 111 del libro de Stallings en español[1] y el apéndice 4A del mismo libro (páginas 123 a 126) y realizar un resumen de a lo sumo 4 páginas de lo siguiente:
  1. Diálogo de mensajes del protocolo Kerberos 5.
  2. Mecanismo de generación de claves de sesión de Kerberos 4.
  3. Modo PCBC del criptosistema DES.
- Revisar las páginas 217 a 223 del libro *Manga Guide to Criptography* y hacer un resumen de a lo sumo 3 páginas sobre el mecanismo de identificación conocido como *Zero-Knowledge Interactive Proof*.

Fecha de entrega

- Viernes 26 de julio.

[1] Fundamentos de Seguridad en Redes: Aplicaciones y Estándares, 2ª Edición.

Próxima Clase

- Verificación de Integridad de Datos
  - Requerimientos
  - Sumas de Verificación
  - Firmas Digitales
  - Blockchain

¿Preguntas?