

Criptografía y Seguridad de Datos

Aplicaciones de autenticación: Certificados X.509

Carlos Figueira.

Universida Simón Bolívar

Basado en láminas del Profesor

Henric Johnson (<http://www.its.bth.se/staff/hjo/>

henric.johnson@bth.se)

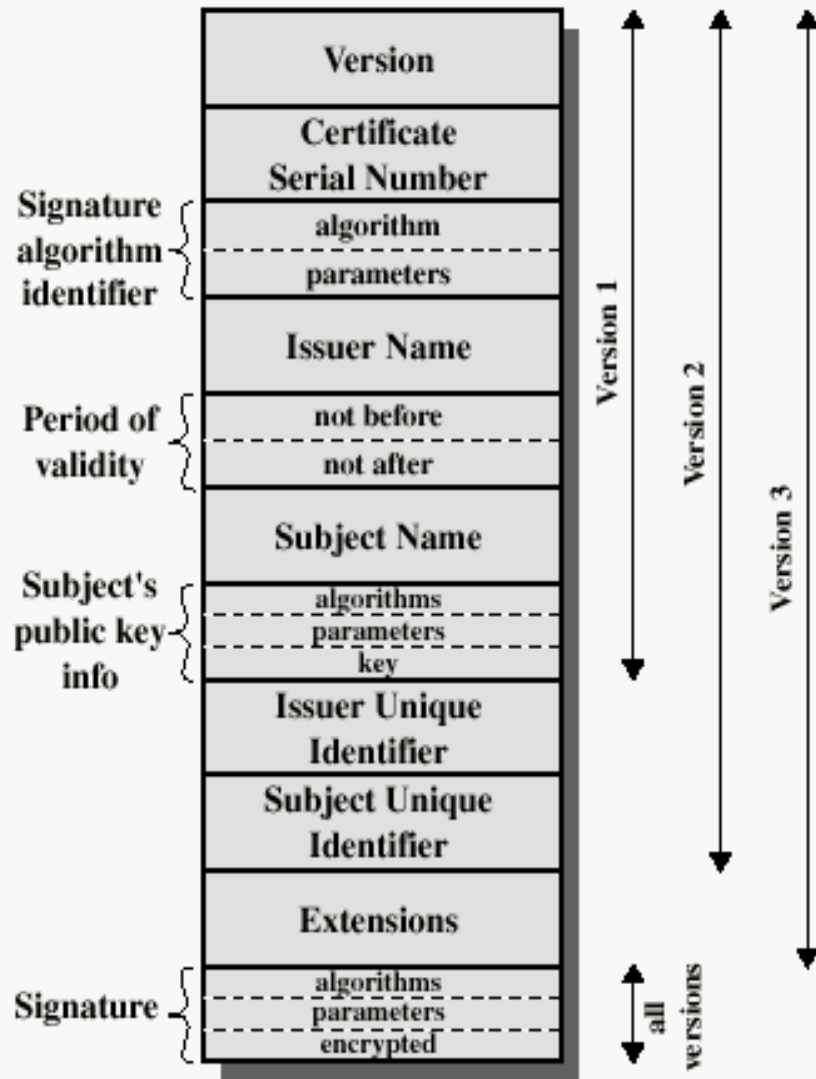
Problemas con la clave pública

- Una clave pública debe tener ciertas garantías, en particular
 - que es efectivamente del usuario o fuente deseada
 - que aún es válida: para evitar ataques de repetición (replay attacks), compromisos por envejecimiento ...
- Solución: certificados de clave pública

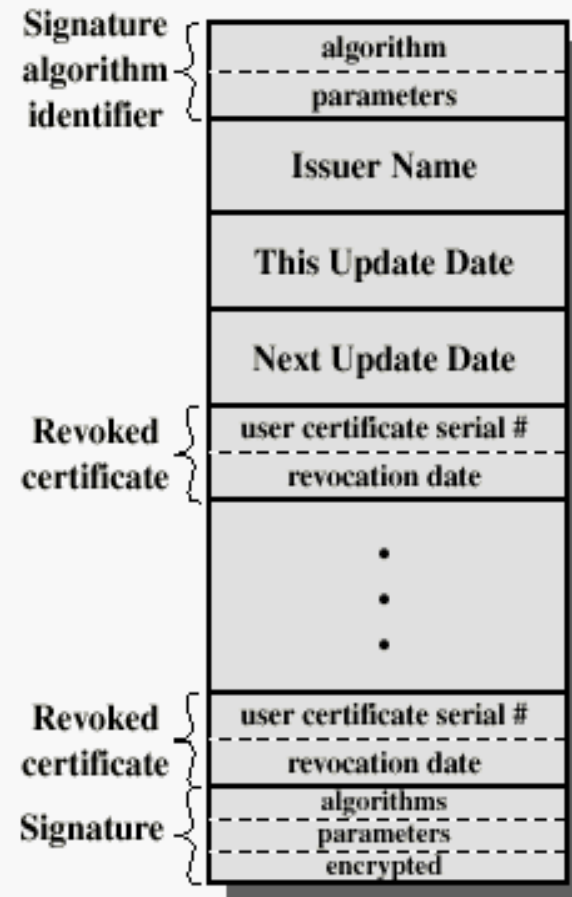
Servicio de Autenticación X.509

- Conjunto de servidores distribuidos que mantienen una base de datos sobre usuarios
- Cada certificado contiene la clave pública de un usuario y está firmada con la clave privada de una autoridad certificadora AC
- Usado en S/MIME, IP Security, SSL/TLS y SET.
- Se recomienda usar RSA

Formatos X.509

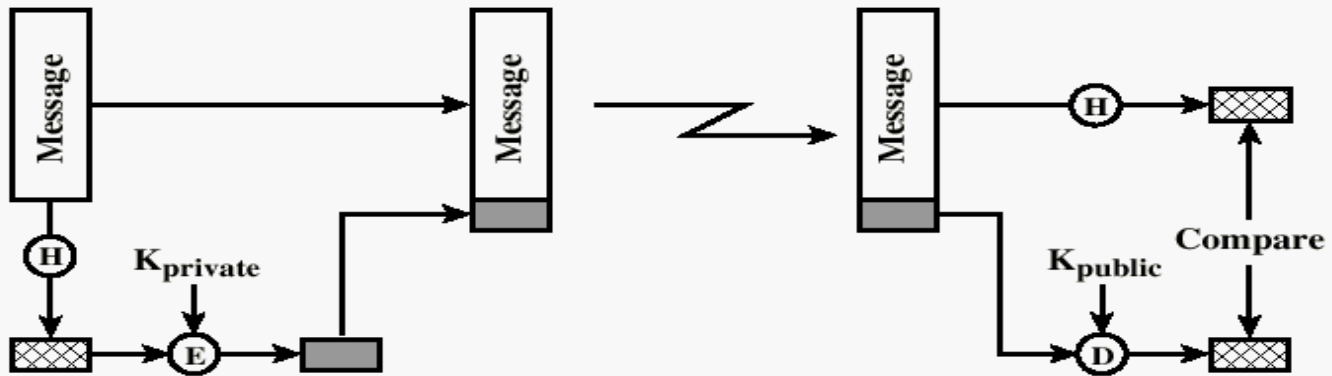


(a) X.509 Certificate



(b) Certificate Revocation List

Enfoque típico de firma digital



(b) Using public-key encryption

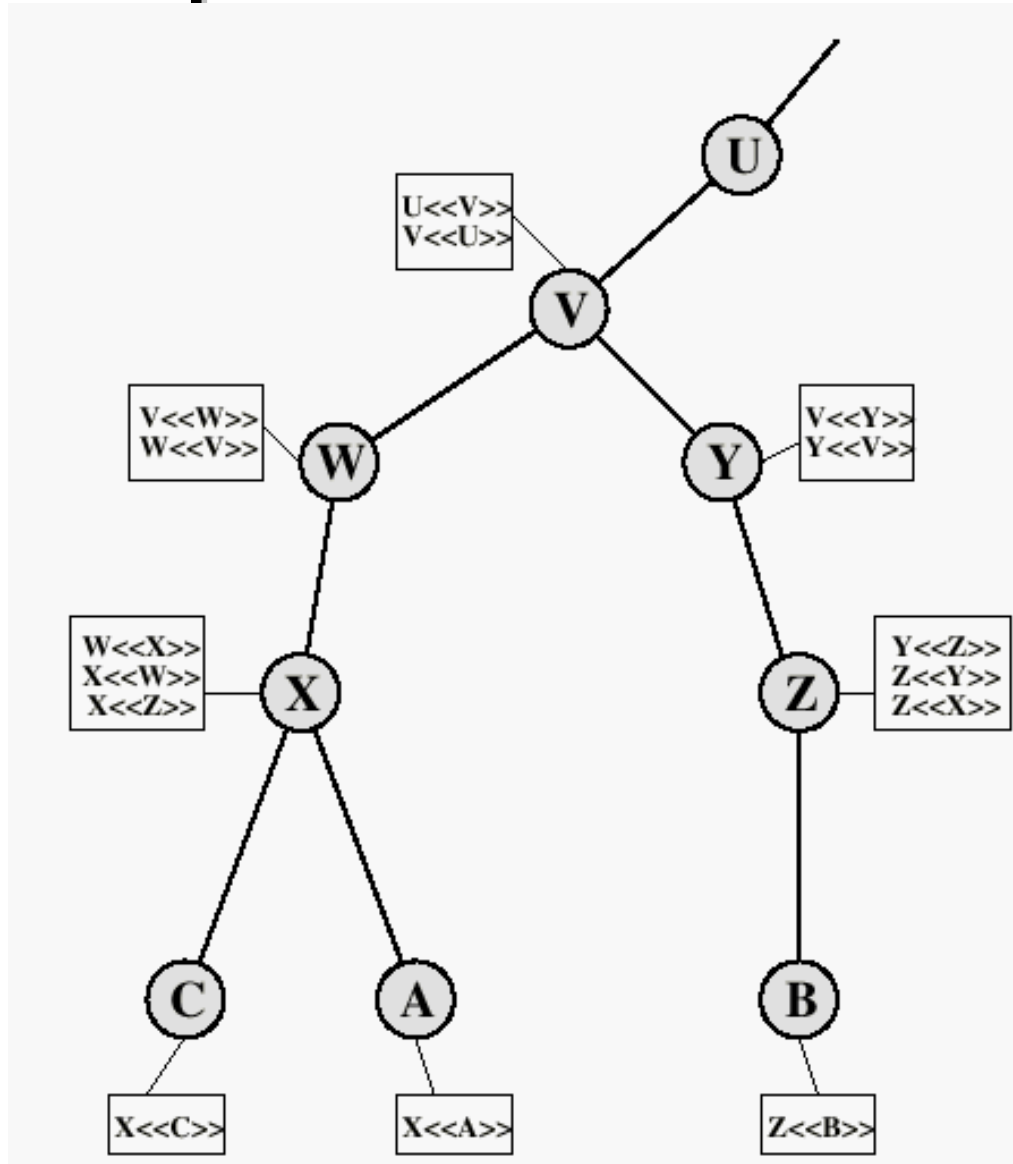
Obteniendo un certificado de usuario

- Características de certificados generados por una AC:
 - Cualquier usuario con acceso a la clave pública de la AC puede obtener la clave pública del usuario que fue certificada
 - Sólo la AC puede modificar el certificado sin ser detectado

Nomenclatura

- $Y\langle\langle X\rangle\rangle$ certificado de usuario X emitido por AC Y
- $Y\{I\}$ firma de I por parte de Y. Formado por I con un resumen criptográfico cifrado

Jerarquía de AC X.509



Ej. de Cadena de confianza

- A confía en X (tiene su clave pública de forma segura, su certificado lo firma X)
- Puede A confiar en certificados firmados por B? Existe ruta de certificación

$X \ll W \gg$ $W \ll V \gg$ $V \ll Y \gg$ $Y \ll Z \gg$
 $Z \ll B \gg$

- También B en A (B confía en Z), por

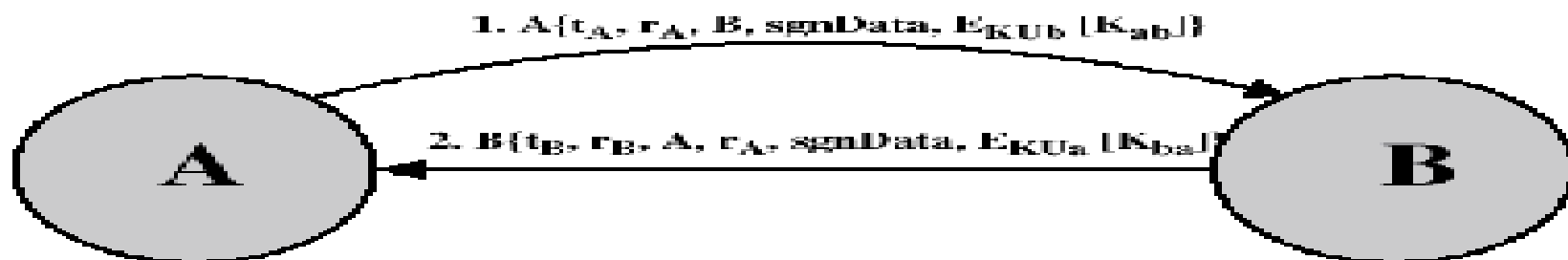
$Z \ll Y \gg$ $Y \ll V \gg$ $V \ll W \gg$ $W \ll X \gg$
 $X \ll A \gg$

Revocación de certificados

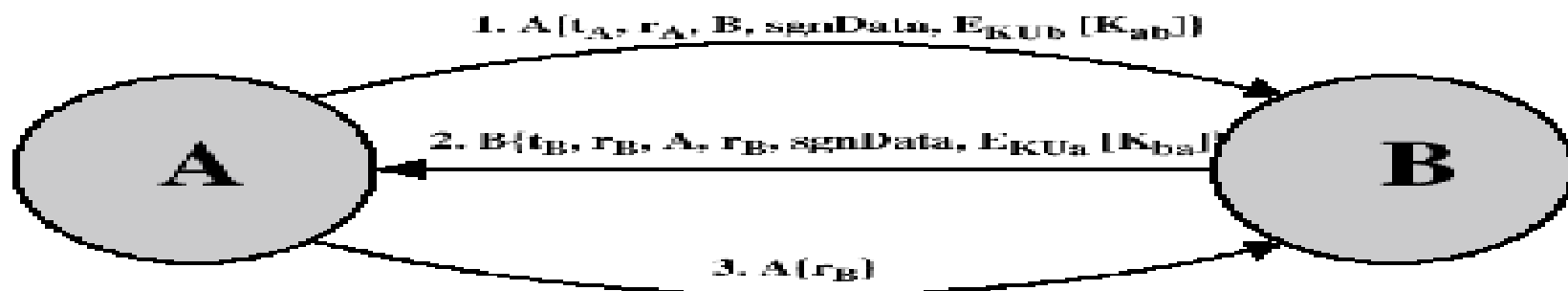
- Razones para revocar:
 - Se sospecha que la clave secreta del usuario puede estar comprometida
 - El usuario ya no está certificado por la AC
 - Se sospecha que el certificado de la AC está comprometido



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

Figure 4.5 X.509 Strong Authentication Procedures