Key Exchange con clave pública

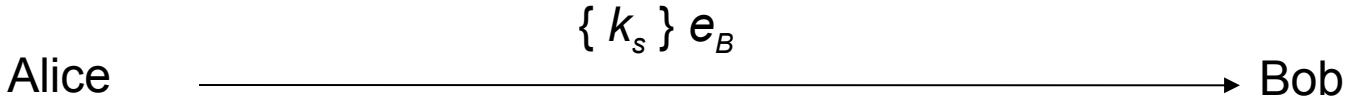
¿ Cómo acuerdan Alice y Bob una clave de sesión ?

Claves de intercambio:

- e_A, e_B son las claves públicas de Alice y Bob, pueden ser conocidas por todos.
- d_A, d_B son las claves privadas de Alice y Bob, solo ellos las conocen.

Solución (versión 1):

- k_s es la clave de sesión (elegida al azar).



Problema y solución

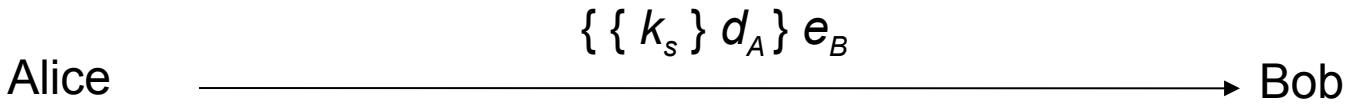
Problema de la solución versión 1:

– Dado que e_B es conocida por todos, Bob no tiene manera de saber que Alice envió el mensaje.

Solución (versión 2):

Usar la clave privada de Alice para firmar la clave de sesión

– k_s es la clave de sesión.

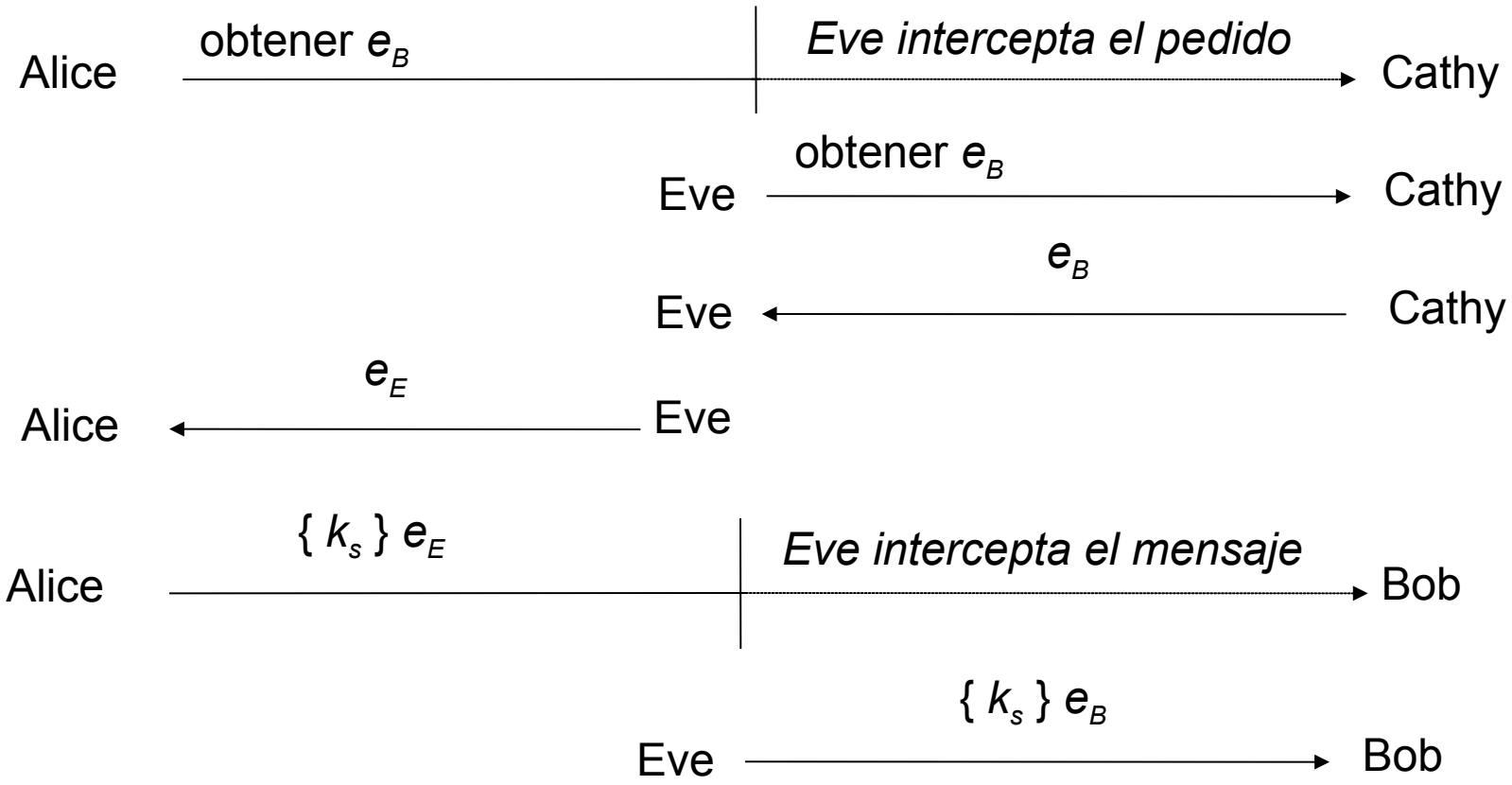


Comentarios

Se asume que Bob posee la clave pública de Alice y viceversa.

- Si no las poseen, cada uno debe obtenerla de un tercero confiable, Cathy.
- Si las claves no se encuentran asociadas a la identidad de su dueño es vulnerable al ataque de Man-in-the-middle.

Ataque Man-in-the-middle



Infraestructura de claves

Objetivo: asociar una clave a la identidad de su poseedor.

Criptografía simétrica

- No es posible dado que las claves son compartidas.

Criptografía asimétrica

- Se asocia la clave pública a la identidad de su poseedor.

Certificado

Una estructura de datos que contiene:

- La identidad del poseedor de la clave pública.
- La clave pública.
- La fecha en la que se emitió.
- Información adicional (ej: identidad del emisor)

firmado por una entidad confiable, por ejemplo Cathy.

$$C_A = \{ e_A \,||\, \text{Alice} \,||\, \ldots \}\, d_C$$

Utilización

Bob obtiene el certificado de Alice

- Si conoce la clave pública de Cathy, puede validar el certificado:
  - Ver si pertenece a Alice
  - Obtener la clave pública de Alice

Problema: Bob necesita la clave pública de Cathy para validar el certificado de Alice.

- El problema pasó a otro nivel, tengo el problema de antes pero con la clave pública de Cathy.
- Aparecen las cadenas de firmas:
  - PGP
  - X.509

PGP

En 1991 Philip Zimmermann publica la versión 1.0 de PGP.

En 1992 aparece la versión 2.0. Su código se escribe fuera de USA para evitar las leyes restrictivas respecto al software criptográfico y sus problemas legales.

La gestión de claves en PGP se basa en la confianza mutua y es adecuada solamente para entornos privados o intranet.

- Las últimas versiones contemplan la utilización de Autoridades Certificantes como certificadores de claves públicas

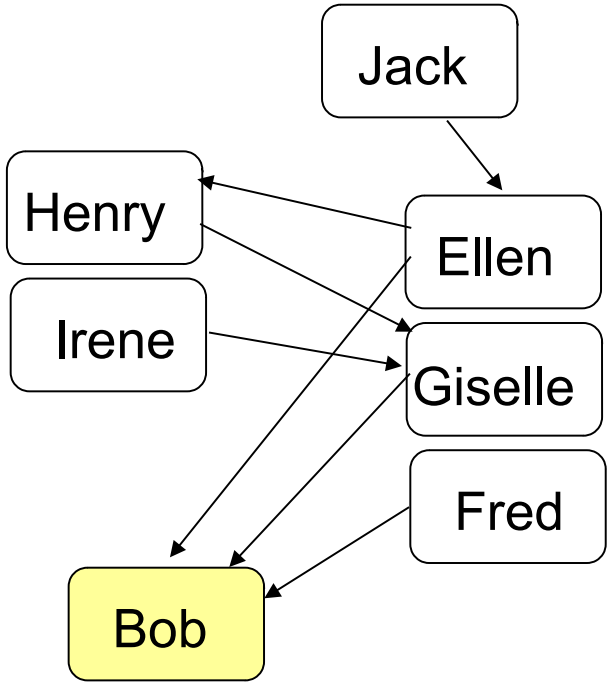
PGP

Datos asociados a las claves:

- versión de PGP
- clave pública junto con el algoritmo (RSA, DSA, DH)
- información sobre la identidad del titular
- firma digital del titular del certificado (auto-firma)
- periodo de validez
- algoritmo simétrico de cifrado preferido
- conjunto de firmas de terceros: (opcional)
  - definen nivel de confianza
  - definen nivel de validez

Validación

- Alice necesita validar la clave PGP de Bob
  - No conoce ni a Fred, ni a Giselle, ni a Ellen.
- Alice obtiene la clave de Giselle
  - Conoce poco a Henry, pero su firma tiene un nivel de confianza que no la conforma.
- Alice obtiene la clave de Ellen
  - Conoce a Jack (es el esposo de Alice), entonces utiliza su clave para validar la de Ellen, luego con esta valida la de Bob.



Las flechas indican firmas.
No se muestran las auto-firmas.

Certificados X.509 v3

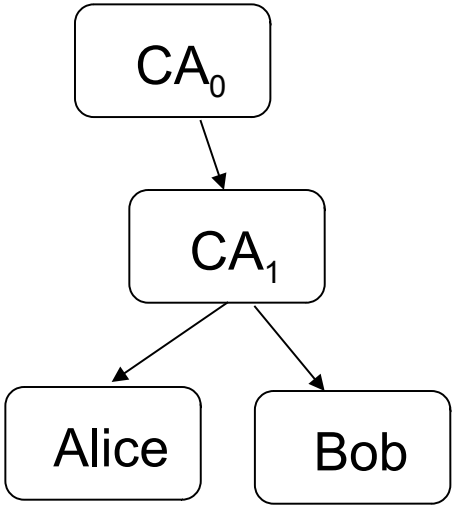
Fueron creados como parte de los mecanismos de control de acceso de los directorios X.500.

Campos de los certificados:

- versión de X.509 (v3)
- número de serie
- algoritmo de firma (sha-256withRSAEncryption)
- nombre del emisor
- periodo de validez
- nombre del titular
- clave pública del titular
- firma: hash del certificado cifrado
- extensiones (opcional)

Validación

- Obtener la clave pública del emisor.
- Descifrar la firma para obtener el hash del certificado.
- Recalcular el hash del certificado y compararlo con el obtenido en el paso anterior.
- Chequear el periodo de validez del certificado.



Emisores

Autoridad Certificante (CA): es una entidad que emite certificados.

Problema:

¿Qué pasa cuando tengo más de una Autoridad Certificante?

Almacenamiento de claves privadas

Es necesario tomar medidas para proteger las claves

- Cifrar el archivo que contiene a la clave
  - Un atacante puede monitorear las teclas que presionamos al ingresar la contraseña para descifrar el archivo.
  - Si la clave queda residente en memoria un atacante podría acceder a ella.
- Utilizar dispositivos específicos (smartcards, tokens criptográficos, etc)
  - La clave nunca sale del dispositivo
  - Ante la posibilidad de robo particionar la clave utilizando mas de un dispositivo.

FIPS 140

- Establecido en 1994 por el NIST para evaluar módulos criptográficos: FIPS 140-1. Actualizado en 2002 para adaptarlo a los cambios tecnológicos: FIPS 140-2
- Actualizado en 2019: FIPS 140-3, entre otros cambios agrega un nivel 5.
- Evalúa solo módulos criptográficos ya sean de hardware o de software.
- En Fips 140-2 Se especifican 4 (cuatro) niveles de seguridad y 11 (once) categorías con requerimientos específicos acordes al nivel deseado.
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Nivel de seguridad 1

- El algoritmo de cifrado deber ser un algoritmo FIPS, por ejemplo AES (FIPS 197), DES (FIPS 46-3), TripleDES (FIPS 81).
- Permite que los componentes de software o firmware se ejecuten en un sistema de propósito general utilizando un sistema operativo no evaluado.
- No se especifican mecanismos de seguridad física.

Nivel de seguridad 2

- Mayor seguridad física
  - Sellos o revestimientos 'tamper-proof', o cerraduras “pick-resistant” (a prueba de ganzúa) en las cubiertas removibles del módulo.
- Autenticación basada en roles
  - El módulo debe autenticar que el operador esta autorizado a asumir un rol específico y a ejecutar los servicios que le fueron asociados.
- Los componentes de software y firmware deben ejecutarse en un sistema operativo que haya sido evaluado en Common Criteria EAL2 o superior.

Nivel de seguridad 3

- Seguridad física ampliada
  - Suficiente para prevenir que los intrusos accedan a los parámetros críticos de seguridad del módulo criptográfico.
- Autenticación basada en identidad.
- Fuertes requerimientos para leer y alterar los parámetros críticos de seguridad.
- Los componentes de software y firmware deben ejecutarse en un sistema operativo que haya sido evaluado en EAL3.

Nivel de seguridad 4

- Mecanismos de seguridad física:
  - Detección y respuesta a los intentos de acceso físico no autorizados, incluye circuitos de 'zeroization' sobre toda la superficie del dispositivo.
  - Incluye protección contra cualquier compromiso de seguridad debido a las condiciones ambientales o fluctuaciones de temperatura y voltaje fuera de los rangos normales de operación del módulo.
- Autenticación basada en identidad.
- Los componentes de software y firmware deben cumplir los requerimientos funcionales del nivel de seguridad 3 y deben ejecutarse en un sistema operativo que haya sido evaluado en EAL4.

Revocación de claves

Los certificados pueden invalidarse antes de su fecha de expiración.

- Por lo general debido a compromiso de la clave
- Puede ser también por un cambio de situación del titular (*por ejemplo: cambio de cargo*)

Problemas:

- La entidad que revoca el certificado debe estar autorizada a hacerlo.
- La información de revocación debe estar disponible rápidamente.

Revocación de certificados X.509 v3

CRL = Certificate revocation list

Es la lista de los certificados que se encuentran revocados.

Son el equivalente a las listas de tarjetas de crédito robadas.

Sólo el emisor del certificado puede revocar el mismo.

- Para informar la situación, la AC lo agrega a la CRL y la publica.

Revocación de claves PGP

- Los firmantes pueden revocar las firmas.
- Los dueños de los claves pueden revocarlas o permitir que otros lo hagan.
  - La revocación es un mensaje firmado, dicho mensaje tiene un flag para indicar que se trata de una revocación.

Tiempo de vida de las claves

Las claves pueden ser clasificadas según su tiempo de vida en dos tipos:

- Corto plazo:
  - Se generan de manera automática.
  - Se utilizan para un mensaje o una sesión y luego se descartan.
- Largo plazo
  - Son generadas por el usuario de manera explícita.
  - Se utilizan para dos propósitos:
    - Autenticación
    - Confidencialidad (cifrado)

Manejo de claves

En resumen, se deben tener en cuenta los siguientes temas al manejar claves:

- Como se generan las claves.
- Como se asocia una clave a la identidad de su poseedor.
- Como se distribuyen las claves.
- Como dos partes establecen una clave común.
- Como se almacenan las claves de manera segura.
- Que ocurre cuando se compromete una clave.
- Como se destruyen las claves.

PKCS - Public-Key Cryptography Standards

Son un conjunto de especificaciones técnicas desarrolladas por Netscape, RSA y otros cuyo objeto es uniformizar las técnicas y protocolos de criptografía pública.

En 1991 se realiza la publicación de la versión 1.0.

Forma parte de distintos estándares como ANSI PKIX, X9, SET, S/MIME y SSL.

Existen 14 documentos con títulos genéricos que van desde PKCS #1 a PKCS #15.

http://www.rsasecurity.com/rsalabs/pkcs/

Documentos PKCS

PKCS #1: RSA Cryptography Standard
PKCS #2: Incluido ahora en PKCS #1
PKCS #3: Diffie-Hellman Key Agreement Standard
PKCS #4: Incluido ahora en PKCS #1
PKCS #5: Password-Based Cryptography Standard
PKCS #6: Extended-Certificate Syntax Standard
PKCS #7: Cryptographic Message Syntax Standard
PKCS #8: Private-Key Information Syntax Standard
PKCS #9: Selected Attribute Types
PKCS #10: Certification Request Syntax Standard
PKCS #11: Cryptographic Token Interface Standard
PKCS #12: Personal Information Exchange Syntax Standard
PKCS #13: Elliptic Curve Cryptography Standard
PKCS #15: Cryptographic Token Information Format Standard

PKI – Public Key Infraestructure

Es una combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía de clave pública.

Componentes más comunes:

- Autoridad certificante
- Autoridad de registro
- Tercero usuario (Relying party)
- Suscriptores
- Repositorios

Autoridad certificante

"Son terceras partes confiables que dan fe de la veracidad de la información incluida en los certificados que emiten"

Emite certificados digitales según su política de certificación (CP = Certificate Policy).

- Reglas que indican la aplicabilidad de un certificado digital a una comunidad y/o a una clase de aplicaciones con requerimientos de seguridad en común.
- Incluyen la definición de un perfil de certificados.

Autoridad certificante

Opera según su manual de procedimientos de certificación (CPS = Certificate Practice Statement)

- Declaración de las prácticas que emplea para emitir, administrar, revocar y renovar certificados.

Referencias útiles:

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- https://cabforum.org/

Autoridad de registro

Es la entidad responsable de una o mas de las siguientes funciones:

- identificar y autenticar a los suscriptores de certificados.
- aprobar o rechazar las solicitudes de certificados.
- iniciar la revocación certificados.
- procesar las solicitudes de revocación de los suscriptores.
- aprobar o rechazar las solicitudes de renovación de certificados.

Terceros usuarios y suscriptores

Terceros usuarios

Son los receptores de un certificado que actúan basados en el mismo y/o en cualquier firma digital que se verifique con ese certificado.

Suscriptor

Es el sujeto que solicita la emisión de un certificado.

Repositorios

Son las estructuras encargadas de almacenar la información relativa a la PKI.

Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de certificados revocados.

Solicitud de certificados

1. El suscriptor genera un par de claves. Firma la clave pública y la información que lo identifica con su clave privada. Luego envía todo a la AC.
   - Prueba que posee la clave privada correspondiente.
   - Protege la información enviada a la AC.

2. La AC verifica la firma del suscriptor en los datos recibidos.

   Opcionalmente se puede verificar la información por otros medios.
   - Presencia física
   - Correo electrónico
   - Legajo de personal, etc.

   En este paso interviene la AR.

Solicitud de certificados (cont)

3. La AC firma la clave pública y parte de la información que el suscriptor envió con su clave privada y crea el certificado.
   - De esta manera asocia a suscriptor con su clave pública y sus datos.

4. El suscriptor recibe el certificado y verifica la firma de la AC y los datos del certificado.
   - Se asegura que la AC no cambio sus datos.
   - Protege la información del certificado.

5. La AC publica el certificado.

Confianza

Necesitamos poder responder las siguientes preguntas:

- ¿cómo se determina en que certificados se puede confiar ?
- ¿cómo se establece la confianza ?
- ¿bajo qué circunstancias la confianza puede ser limitada o controlada en un entorno dado ?

Modelos de confianza

Existen varios modelos:

- Jerárquico
- Modelo web
- Bridge CA
- Certificación cruzada
- Reconocimiento cruzado
- CTL (lista de certificados confiables)
- …

Tipos de certificados

Según el uso que podemos encontrar:

- Certificados SSL
- Certificados S/MIME (correo electrónico)
- Certificados S/MIME (personales)
- Certificados para la firma de código
- Certificados para AC
- Certificados para WPA-SPK
- Certificados para VPN
- …

Certificados digitales (X.509 v3)

Campos

– version	versión de la estructura = v3
– serialNumber	id. única del certificado
– signatureAlgorithm	algoritmo de firma
– issue	nombre del emisor
– validity	vigencia desde/hasta
– subject	nombre del suscriptor
– subjectPublicKeyInfo	clave pública del suscriptor
– signature	hash del certificado cifrado
– extensions	extensiones (opcional)

Identificación

Cada certificado se puede identificar en forma inequívoca utilizando

- serialNumber + issuer

Campos issuer y subject

- Contienen atributos
- Los atributos están definidos en X.520
- Pueden definirse atributos nuevos

- En la definición de atributo se especifican:
  - Identificador único (OID)
  - Caracteres admitidos
  - Valores posibles
  - Longitud máxima
  - Reglas de búsqueda

Atributos

- Los atributos más comunes son:
  - countryName { 2 5 4 6 }
  - organizationName { 2 5 4 10 }
  - organizationalUnitName { 2 5 4 11 }
  - stateOrProvinceName { 2 5 4 8 }
  - localityName { 2 5 4 7 }
  - commonName { 2 5 4 3 }
  - title { 2 5 4 12 }
  - surNam { 2 5 4 4 }
  - givenName { 2 5 4 42 }
  - initials { 2 5 4 43 }
  - pseudonym { 2 5 4 65 }
  - serialNumber { 2 5 4 5 }

Atributos

- Tienen tipos específicos, por ejemplo:
  - PrintableString
  - IA5String
  - DirectoryString

- Poseen longitudes máximas
- Algunos sistemas no controlan la longitud de los campos, mientras que otros fallan si los tamaños superan los estándares

Fechas de validez

- Las fechas de vigencia están expresadas respecto del meridiano de Greenwich

- Pueden ser:
  - GeneralizedTime YYYYMMDDhhmmssZ
  - UTCTime YYMMDDhhmmssZ

$$1950 \leq YY < 2050$$

Extensiones

- Proveen un método para asociar atributos a un certificado digital

- Se utilizan para:
  - manejar la herencia de certificación
  - restringir el uso del certificado
  - aportar mayores precisiones en el uso del certificado

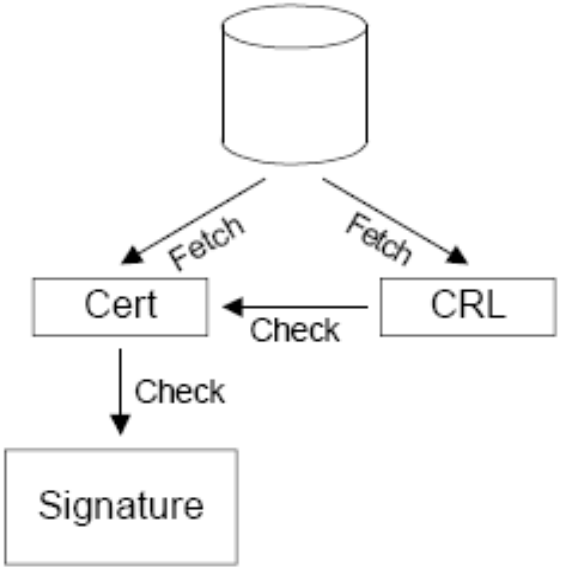
Extensiones

Las siguientes son algunas extensiones:

- Authority Key Identifier / Subject Key Identifier
- Key Usage / Extended Key Usage
- Certificate Policies
- Authority Alternative Name / Subject Alternative Name
- Basic Constraint
- CRL Distribution Points
- Authority Information Access

CRLs

- Constituyen un medio para verificar el estado de validez de un certificado digital.
- Las AC están obligadas a publicar permanentemente la CRL, que tiene un período de validez.



CRLs

- Campos
  - version versión de la estructura = v2
  - signature algoritmo de firma
  - issuer nombre del emisor
  - thisUpdate fecha de emisión
  - nextUpdate fecha de próxima emisión
  - revokedCertificates lista de certificados revocados
    - userCertificate nro de serie del cert. revocado
    - revocationDate fecha de revocación (hasta seg.)
    - crlEntryExtensions extensiones relac. c/cert. revocado
  - crlExtensions extensiones relac. con la CRL

CRLs

Extensiones:

- Authority Key Identifier
- CRL Number / Delta CRL Indicator / Delta CRL DP
- Issuing Distribution Point

Extensiones de una entrada de CRL:

- Reason Code
- Hole Instruction Code

Problemas

- No contienen el estado actual de los certificados
- La responsabilidad por la verificación recae en el usuario
- Presentan problemas de volumen y de distribución

Soluciones

- Puede dividirse el alcance (scope) de una CRL para reducir la cantidad de certificados incluidos.
- Pueden emitirse “delta CRL” sólo con los nuevos certificados revocados.
- Existen “CRL indirectas” emitidas por claves distintas a las de la Autoridad Certificante.

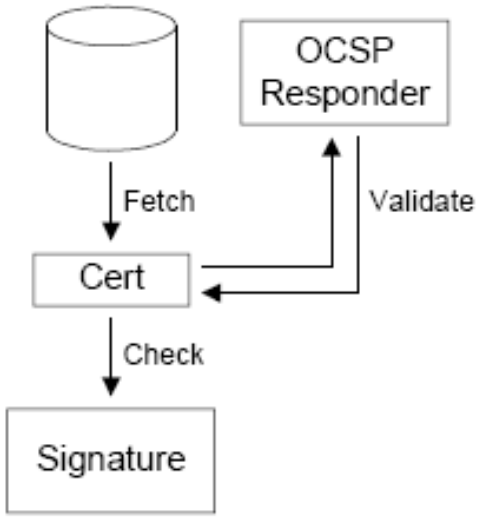
OCSP

Servicio que permite saber si un certificado es válido o no.

Requiere de la Autoridad Certificante para responder las consultas.

Retorna una respuesta firmada conteniendo el estado del certificado.

- Hay tres estados posibles: “good”, “revoked” y “unknown”.



Referencias

Para mas información:

- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

CAA

DNS Certification Authority Authorization (CAA) Resource Record

Permite que cada dominio defina que CAs pueden emitirle certificados.

Desde el 8/9/17, las CAs están obligadas a consultar este valor antes de emitir un certificado.

Referencias:

https://tools.ietf.org/html/rfc6844

Certificate Pinning

- **Técnica que buscaba detectar posibles certificados maliciosos, pero que respetan la cadena de confianza.**
- **Para http, HPKP (HTTP Public Key Pinning)**

- **Deprecado!**

Referencias:

RFC 7469 – Public Key Pinning Extension for HTTP
https://tools.ietf.org/html/rfc7469

https://unaaldia.hispasec.com/2017/11/google-declara-obsoleto-http-public-key-pinning-hpkp.html

Certificate Transparency

El objetivo del proyecto transparencia de certificados es proteger el proceso de emisión de certificados al proporcionar un marco de trabajo abierto para supervisar y auditar los certificados de HTTPS.

Se recomienda a todas las CA que escriban los certificados que emiten para registros públicamente verificables, inviolables y que solo se puedan anexar. En el futuro, es posible que los navegadores decidan no aceptar certificados que no se hayan escrito para dichos registros.

Referencias:
https://tools.ietf.org/html/rfc6962
https://www.certificate-transparency.org/what-is-ct
http://blog.elevenpaths.com/2016/11/certificate-transparency-el-que-el-como.html

El eslabón más débil…

- **Null Byte en el certificado:**
  - X509 usa ASN.1 que representa a los strings como en PASCAL.
  - Las aplicaciones suelen estar programadas en C…
  - ¿Qué pasa si solicito un certificado para www.facebook.com\0.midomino.com ?

  Ref: http://downloads.asterisk.org/pub/security/AST-2015-003.pdf

- **Usando el 3 para evitar la validación de OCSP:**
  - La respuesta no siemre esta firmada
  - MiTM modificar el valor por un 3 (try later)
  - OCSP falla de modo abierto…

  Ref: https://randomoracle.wordpress.com/2009/07/31/ocsp-this-fail-brought-to-you-by-the-number-three/

Propiedades de la información

La información debe reunir las siguientes condiciones:

- Autoría
- Integridad
- Confidencialidad
- Disponibilidad

¿ Qué es un documento digital ?

- Un mensaje de correo electrónico (eMail)
- Datos ingresados a un formulario Web
- Los valores insertados en una Base de Datos
- Una transacción bancaria
- Una imagen (scan) de un documento en papel
- Un archivo cualquiera de la PC
- Una grabación digital de audio o video
- …

¿ Qué **no** es un documento digital ?

- El flujo de información entre un servidor y una estación de trabajo
- El procedimiento de logon a un sistema
- ...

Problemática actual

Dado un documento en formato digital:

- No es posible determinar con certeza el autor.
- Un documento en formato digital es fácilmente alterable, no existiendo evidencia de dicha alteración.
- El autor puede no reconocerlo. No es susceptible de verificación ante terceros.

Por lo tanto:

“No se puede reemplazar el papel”

Necesitamos ...

- Autenticidad del autor

  Atribuir el documento a su autor (una persona o aplicación) en forma fehaciente (identificar al autor)

- Integridad del contenido

  Asegurar que el documento no fue modificado luego de ser firmado (integridad del contenido)

- No repudio del documento

  Garantizar que el emisor del mensaje no pueda negar (o repudiar) su existencia o autoría. Es susceptible de verificación.

Firma digital

Conjunto de datos expresados en formato digital que se utiliza para:

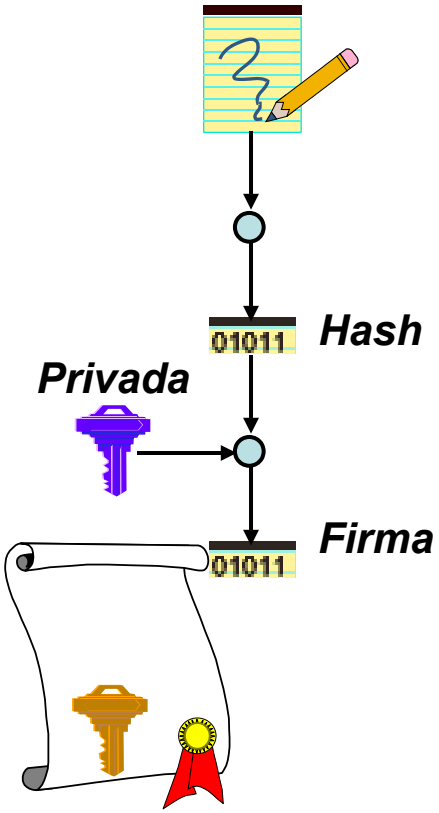
- Identificar a un firmante.
- Verificar la integridad del contenido de un documento digital.

Que cumpla con los siguientes requisitos …

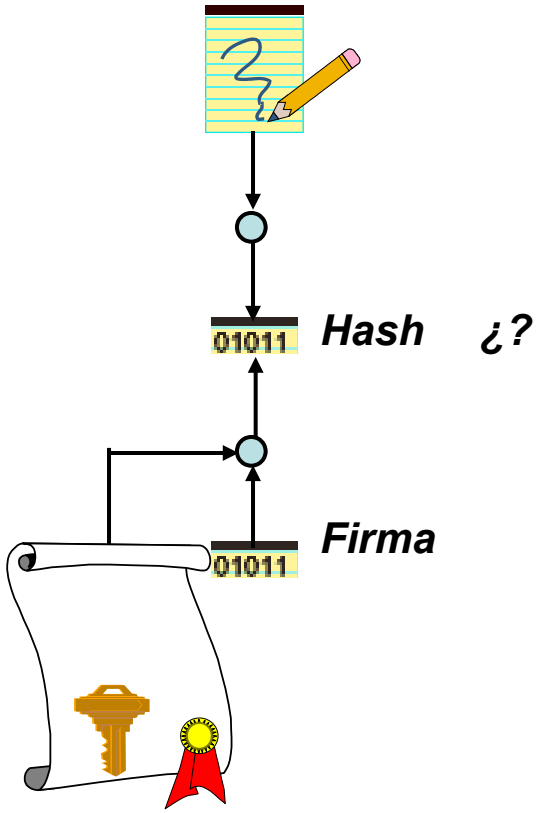
- Pertenecer únicamente a su titular.
- Encontrarse bajo su absoluto y exclusivo control.
- Ser susceptible de verificación.
- Estar vinculada a los datos del documento digital poniendo en evidencia su alteración.

Funcionamiento

Cuando se Firma



Cuando se Verifica



Sistema de firma digital

- Hay 4 actores principales:
  - Quien firma (el suscriptor).
  - Quien(es) necesita(n) verificar la firma. (el tercero usuario)
  - Quien testimonia que una firma digital pertenece a una cierta persona. (la autoridad certificante)
  - Quien controla el sistema.

Más referencias

Para más información:

- RFC 5751 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification
- RFC 5652 - Cryptographic Message Syntax (CMS)
- RFC 5126 - CMS Advanced Electronic Signatures (CAdES)

- Comandos Openssl CA
- https://blog.cloudflare.com/introducing-cfssl/

Bibliografía adicional