Certificados Digitales y su utilización en Entornos Clínicos

Reche Martínez, D.; García Linares, A.J.; Richarte Reina, J.M.
Dpto. I+D+I. NOVASOFT SANIDAD. Grupo Novasoft

INTRODUCCIÓN

Dentro del área temática de seguridad y protección de la información hoy en día en el entorno sanitario español se dejan de lado muchas características deseables en un sistema de seguro. El objetivo de esta presentación es difundir la necesidad del uso de sistemas de firma digital en estos entornos, además de realizar una introducción a las infraestructuras de clave pública (PKI), y arquitectura básica de administración de certificados digitales en un hospital.

¿CÓMO FUNCIONA EL CIFRADO?

Las técnicas de cifrado se dividen en dos grupos, simétricas y asimétricas. Los simétricas utilizarán la misma clave para cifrar y descifrar mientras que los asimétricas utilizan una clave diferente para cada tarea.

> Al utilizar un cifrado simétrico las dos partes participantes en la comunicación, el emisor y el receptor deben conocer la clave de cifrado/descifrado. Lo cual crea un grave problema, en cuanto la privacidad de la clave se ve comprometida nuestro canal deja de ser seguro. Una consecuencia de ello es que deberemos comunicar la clave al otro extremo por medio de un canal seguro.
>
> Los cifrados asimétricos tienen la ventaja de que una de las claves (la clave de cifrado) puede darse a conocer, lo que denominaremos hacerla pública o publicarla. Mientras mantengamos en secreto la clave de descifrado (llamada clave privada) podemos difundir nuestra clave de cifrado (llamada clave pública) a discreción. Como podemos suponer nadie será capaz de descifrar el mensaje enviado, pero cualquiera puede enviarnos un mensaje cifrado. Con lo cual conseguimos el objetivo perseguido de enviar un mensaje "secreto" y, de paso, evitamos el problema de la difusión de la clave de los sistemas simétricos.
>
> Los cifrados asimétricos, se utilizan además como prueba de identidad. O sea, para demostrar que el emisor del mensaje es el que lo envía realmente y probar que no ha sido suplantado por un impostor. Esto se consigue cifrando con la clave privada y descifrando con la pública. En este caso, si al recibir un mensaje cifrado por alguien conseguimos descifrarlo con su clave pública sabremos sin duda que fue él (o ella) quien lo envió, ya que solo esa persona conoce la clave privada. De esta manera conseguimos asegurar el origen del mensaje, pero el mensaje no será secreto ya que cualquiera podrá descifrarlo con la clave pública del emisor. Esta idea forma la base de la firma digital. RSA, Diffie-Hellman, DSA y la criptografía de curva elíptica son técnicas de cifrados asimétricos utilizados actualmente.

Los cifrados simétricos son normalmente de cien a mil veces mas rápidos que un cifrado asimétrico software típico. Esta característica los han hecho ser, por mucho tiempo, los mas utilizados como método de cifrado para ficheros en almacenamiento local. Los cifrados simétricos mas conocidos incluyen DES, Triple DES, RC2, RC4 e IDEA. La fortaleza de un cifrado simétrico se mide a grandes rasgos con su longitud de clave: 40 bits es generalmente considerado débil y a partir de 128 bits se considera fuerte.

¿COMO ENVIAR UN MENSAJE DE FORMA SEGURA?

Para conseguir una comunicación segura, es buena idea combinar la seguridad y facilidad de la distribución de claves de un cifrado asimétrico con la velocidad de un cifrado simétrico. Esa es la idea aportada por el siguiente protocolo híbrido, que forma la base de muchos criptosistemas actuales

Protocolo 1a: Cifrar un mensaje

Generar una clave Simétrica K
Cifrar el mensaje M con la clave simétrica K obteniendo M*
Obtener la clave pública del receptor
Cifrar la clave simétrica K con la clave publica del receptor obteniendo K*
Enviar {K*,M*}

Protocolo 1b: Descifrar un mensaje

Recibir {K*,M*} y separar los dos campos
Descifrar K* con la clave privada del receptor para conseguir K
Descifrar M* con K para conseguir el mensaje original M

Ya que generamos una clave diferente para cada sesión de mensajes, la clave simétrica se nombra frecuentemente como clave de sesión.

Como ya sabemos, los cifrados asimétricos son mucho mas lentos que los cifrados simétricos por ello, a menudo sucede un hecho curioso, descifrar la clave es mas lento que descifrar el mensaje en si.

¿CÓMO SE DONDE FUE ORIGINADO UN MENSAJE?

Los mensajes cifrados proporcionan confidencialidad. Por ejemplo, puede asegurar que nadie verá los datos de su tarjeta de crédito a través de la red. Sin embargo, la confidencialidad es solo una parte de la historia. Cientos de tiendas de su ciudad probablemente ya tienen los datos de su tarjeta. Para realizar cualquier transacción electrónica segura, el requisito mas importante es asegurar que el mensaje viene de la persona que esta autorizada para enviarlo y que no ha sido suplantado. Ambas propiedades, conocidas como **integridad** y **autenticidad**, están proporcionadas por la firma electrónica. Para entender como funciona, debemos introducir una tercera clase de algoritmos: las funciones resumen (hash).

Mientras los cifrados asimétricos usan distintas claves para cifrar y descifrar y los simétricos usan una única clave, las funciones resumen solo cifran. Nunca se puede recuperar el mensaje original desde una función resumen. Es lo que se denomina funciones de un único sentido. ¿Para que sirven entonces?.

Las funciones resumen proporcionan una *huella digital* del mensaje (es decir una prueba indeleble del mensaje). Al aplicar una función resumen a un mensaje obtenemos una cadena de 16 a 20 bytes. Un mensaje particular siempre arroja el mismo resumen, pero es algo menos que imposible encontrar dos mensajes diferentes con el mismo resumen. Se puede mejorar la eficiencia de las claves privadas para proporcionar autenticación, evitando cifrar el mensaje entero con la clave privada, usando una función resumen.

La firma se realiza con una clave privada y la verificación con una pública

Protocolo 2a: Firmar un Mensaje

Resumir el mensaje M obteniendo H.
Cifrar H con la clave privada del emisor obteniendo S.
Enviar {M,S}

Protocolo 2b: Verificación de un mensaje firmado

Recibir {M,S} y separarlos
Resumir el mensaje M y obtener H'.
Obtener la clave publica del emisor.
Descifrar S con la clave publica obteniendo H''.
Comparar H' y H''

Si H' y H'' son iguales, el mensaje se ha verificado correctamente. Si son diferentes, o el mensaje ha sido modificado en el trayecto o el emisor no es quien dice que es.

La **Verificación** es el proceso de comparación de dos elementos, el mensaje que ha sido firmado y la misma firma.

¿POR QUÉ NECESITO CERTIFICADOS?

Los certificados digitales son un medio de unir sin ambigüedad una persona (o entidad) a su clave publica. Para hacerlo mas simple, la idea es que una entidad externa, una tercera parte confiable o autoridad de certificación (CA) coge sus datos personales y su clave pública, los empaqueta juntos y después firma el paquete. Un certificado digital prueba su identidad mucho mejor que su clave pública.

Al considerar los protocolos de seguridad, mas que simples algoritmos de seguridad, el uso de certificados digitales crece en importancia. Existen numerosas situaciones del mundo real donde la seguridad proporcionada por un par de claves simples no es suficiente.

INTRODUCCION A LOS CERTIFICADOS DIGITALES

Un certificado digital es un documento con cuatro componentes principales:

- Una clave pública
- Información que una la clave con el usuario
- Información sobre el emisor del certificado
- La firma digital del emisor del certificado

Los certificados digitales se clasifican como certificados auto-firmados o certificados CA-firmados de acuerdo a si fueron firmados por el propietario de la clave pública o por otra autoridad, respectivamente.

Los certificados actúan primero como contenedores para una clave pública, por ello a menudo podemos referirnos a «cifrado usando un certificado» cuando realmente significa «cifrado usando la clave pública contenida en un certificado». Sin embargo, ya que los certificados contienen mas información que simplemente la clave pública, tienen muchos mas usos. Los campos de información típicos en un certificado son los siguientes:

- El nombre del usuario
- La dirección de correo electrónico
- El nombre de la empresa en la que trabaja
- El número de teléfono
- Información similar sobre el emisor del certificado
- Un identificador único para el certificado (un número de serie)
- Un indicador del nivel de veracidad del certificado
- Una fecha de emisión
- Una fecha de expiración

La información recogida sobre el propietario se denomina Nombre distinguido del propietario o *Dname*. Un certificado contiene dos Dnames: El del propietario y el del emisor del certificado.

El identificador único del certificado facilita enormemente la tarea de tratar con múltiples receptores o un receptor con múltiples claves. Cuando ciframos un mensaje para múltiples receptores, ciframos una copia de la clave de sesión con la clave pública de cada receptor y etiquetamos cada clave cifrada con el identificador del certificado usado para cifrarla. Los receptores solo necesitan ir a través de la lista de claves cifradas hasta encontrar una etiquetada con el identificador de su certificado para encontrar la clave de sesión cifrada con su clave pública.

Si firma un mensaje, debería adjuntar su certificado con él. Esto asegura que el receptor tendrá una copia de la clave pública a mano, mejor que tener que obtenerla a través de la base de datos. Esto también resuelve cualquier confusión acerca de que clave pública ha sido usada en el caso de que el emisor tenga mas de un par de claves.

Como un certificado tiene una firma digital, esta firma requiere un certificado que le permita ser validada. Este certificado también requerirá un certificado para su validación, de esta forma se crea una cadena de certificados que es terminada con un certificado auto-firmado.

El estándar para certificados digitales esta recogido en la recomendación X.509 de la IETF. Y son considerados por todos como una gran mejora en la seguridad de la transmisión de la clave pública.

AUTORIDADES DE CERTIFICACIÓN Y TERCERAS PARTES CONFIABLES

Una CA es una aplicación que coge una clave pública y la pone en un certificado, además de desarrollar algunas tareas de mantenimiento de certificados. Ya hemos mencionado que los certificados pueden ser auto-firmados o CA-firmados. Cuando un certificado es auto-firmado, no aporta beneficios particulares en la determinación de la veracidad de la clave. Sin embargo, cuando un certificado es CA-firmado, conlleva una implicación: que alguna tercera parte confiable (TTP) o CA ha verificado que la clave pública pertenece al usuario indicado, y esta dispuesta a certificarlo. Ahora usted puede confiar en cualquier certificado firmado por la CA, mientras ocurra lo siguiente:

- Confíe en la política de registro de clientes de la CA (el rigor con el que verifica la clave pública del propietario).
- Esté seguro de que la clave pública de la CA esta asociada actualmente a la CA.

La segunda condición puede ser comprobada verificando la huella digital del certificado de la CA u obteniendo el certificado de la CA firmado por otra CA, que debe entonces adjuntar su propio certificado.

¿QUÉ ES UNA INFRAESTRUCTURA DE CLAVE PUBLICA?

La amplia adopción de estas técnicas de criptografía requieren una PKI global, basada en un conjunto de estándares estrictamente definidos que controlan cada aspecto del ciclo de vida de un certificado. En la guía de «Internet X.509 Public Key Infrastructure PKIX Roadmap», el grupo de trabajo de PKIX define una PKI como «*El conjunto de hardware, software, gente y procedimientos necesarios para crear, manejar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública*».

Una PKI comprende cinco tipos de componentes:

- **CAs:** Son las responsables de emitir y revocar certificados.
- **RAs:** Verifican la unión entre claves públicas y la identidad de sus propietarios.
- **Usuarios Certificados:** Personas, maquinas o agentes software a los que se les ha emitido certificados y que los usan para firmar documentos digitalmente.
- **Clientes:** Validan firmas digitales y su camino de certificación desde una clave publica conocida de una CA confiable.
- **Repositorios:** Almacenan y ponen a disposición los certificados y las CRLs.

Una PKI debe llevar a cabo, al menos, estas funciones:

- Registro
- Certificación
- Recuperación de clave
- Generación de claves
- Actualización de clave
- Certificación cruzada
- Revocación

UTILIDAD DE LA PKI EN UN HOSPITAL

En el entorno hospitalario existe un claro ejemplo de utilidad del uso de PKIs, ya que se requiere un especial cuidado en el control de acceso a la información clínica, aún mas si tenemos en cuenta la legislación vigente de la LOPD. Es mas que deseable la equiparación de la historia clínica electrónica a la historia clínica manuscrita. En este sentido, la firma electrónica es un requisito imprescindible para poder aseverar que cualquier documento que forma parte ella ha sido firmada por el profesional responsable y además asegurar su integridad. Si vamos mas allá, una característica fundamental de la PKI en el entorno clínico sería la capacidad de auditoria. Es decir saber quien ha hecho que en cada momento. Otra característica necesaria en la manipulación de los datos clínicos es la necesidad de integridad y autenticidad de los informes interconsulta.

Novasoft esta trabajando en el desarrollo de aplicaciones especificas en estos entornos que estarán totalmente integradas como los sistemas de información hospitalaria y de atención primaria en el nuevo marco extensible de aplicaciones xHIS

REFERENCIAS

1. Applied Cryptography: Protocols, Algorithms and Source Code in C
   Bruce Scheneier, Jhon Wiley & Sons; 2nd edition 1995
2. Handbook of Applied Cryptography
   Alfred J. Menezes et al, CRC Press 1996
3. Criptography and Network security: Principles and Practice
   William Stallings, Prentice Hall; 3rd edition 2002
4. Public Key Infraestructure X.509
   http://www.ietf.org/html.charters/pkix-charter.html
5. Secure socket layer
   http://www.openssl.org/
6. Documentación técnica PKI eTrust de Computer Associates
   http://www.cai.com/
7. Documentación técnica PKI UniCERT de Baltimore
   http://www.baltimore.com/
8. Documentación técnica RSA security
   http://www.rsasecurity.com/