Cifrado de Chave Pública

INTRODUCCIÓN

O Problema do Cifrado

Para protexer o acceso a información privada a solución máis práctica é segura é o cifrado. Mediante o cifrado transformamos a información a protexer en texto inintelixible utilizando unha contrasinal ou ***palabra chave***. Unicamente as persoas que coñezan esa palabra chave poderán descifrar e acceder a información. O proceso de transformación implica o uso dun ***algoritmo de cifrado*** como AES, DES, 3DES, RC4..., sendo o máis utilizado hoxe en día AES.

> Os sistemas de cifrado no que se emprega a mesma chave para cifrar e descifrar a información se denominan sistemas de ***cifrado simétrico***

O ***cifrado simétrico*** é rápido, apto para cifrar grandes volumes de información e razoablemente seguro. Se emprega de xeito masivo hoxe en día para asegurar a privacidade de acceso a información. ***O problema principal que presenta, é que as partes que participen na comunicación necesitan coñecer a palabra chave do cifrado.***

Mentres que entre particulares é relativamente simple compartir a chave de cifrado (verbalmente por exemplo) cando falamos de comunicacións a través de internet o problema se multiplica. Si alguén consigue interceptar a comunicación da chave de cifrado (que non pode ir cifrada, obviamente) todo o sistema perde completamente a súa seguridade.

> **O cifrado de chave pública resolve o problema da compartición da chave de cifrado**

Para solucionar isto, deseñáronse sistemas de ***cifrado asimétrico***. Nestes sistemas se utilizan dúas chaves de cifrado. A información cifrada cunha chave so se pode descifrar coa outra. Deste xeito si dúas partes nunha comunicación posúen unha das chaves poderán comunicarse de xeito seguro cifrando a información coa chave que posúen e sabendo que unicamente o que ten a outra chave poderá acceder a información.

Si quero poder recibir información confidencial so necesito quedar cunha das chaves e compartir a outra. A información que cifren coa outra chave so a poderei ler eu.

Cifrado de Chave Pública

O ***cifrado de chave pública*** emprega unha combinación de cifrado simétrico e asimétrico para protexer as comunicacións. Mediante este sistema, cada participante crea unha parella de chaves de cifrado asimétrico. Unha das chaves a mantén segura, sin compartila con absolutamente ninguén: **a chave privada**. A outra chave se pon a disposición pública, todo o mundo que queira comunicarse cun participante poderá acceder a ela, denominándose polo tanto **chave pública**.

A información cifrada coa chave pública unicamente será accesible a persoa que estea en posesión da chave privada correspondente.

> O ***proceso de cifrado*** con chave asimétrica consiste en:
> 1.- Se xera unha chave simétrica ao azar
> 2.- Se cifra o documento coa chave simétrica anterior, por exemplo con cifrado AES
> 3.- Se cifra a chave simétrica empregada coa chave pública do destinatario.
> 4.- Se envía o documento coa chave cifrada como adxunto.
>
> *O receptor:*
> 1.- Descifra a chave de cifrado coa súa chave privada
> 2.- Descifra o documento.

Cifrado e Firma Dixital

Os algoritmos de cifrado de chave pública non son moi apropiados para cifrar volumes de información grandes. Para solucionar este problema **o procedemento de cifrado** consiste en crear unha chave de cifrado simétrica ao azar e cifrar con ela a información (por exemplo mediante AES). A chave pública do destinatario se empregará para cifrar unicamente a chave de cifrado simétrica empregada, que se enviará como adxunto á información cifrada.
O destinatario poderá acceder á chave de cifrado mediante o uso da súa chave privada e descifrar a información.

Outro uso común do cifrado de chave pública é a ***sinatura dixital.*** Mediante este procedemento é posible asegurar a autoría e integridade dun documento, de xeito que o destinatario sabe sin ningunha dúbida quen é o autor e que a información do documento non foi alterada por terceiros.

O proceso da ***sinatura dixital*** é o seguinte:

O autor do documento:
1.- Xera un hash da información do documento. Este hash vai a asegurar que a información do documento non está alterada (si se alterara, cando se recalcula o hash non coincide)
2.- Cifra o hash coa chave privada do autor.
3.- Envía o documento co hash cifrado como adxunto

O receptor do documento:
1.- Descifra o hash adxunto coa chave pública do suposto autor. Si consigue descifralo e porque está cifrado coa chave privada do autor, logo temos garantizada a autoría.
2.- Se calcula o hash da información recibida e se comproba que coincide co hash adxunto. Esto garante que a información non foi alterada por terceiros.

O cifrado e firma dixital son procedementos importantísimos na comunicación segura de información sobre dous dos medios máis utilizados en internet: A web e o e-mail. A web se protexe mediante o protocolo ***https*** que emprega cifrado de chave pública para protexer a información e a autenticidade do servidor, evitando o phising. O e-mail utiliza a firma dixital para asegurar a autoría.

O ***e-mail*** se transmite en texto claro e pode pasar por múltiples intercambiadores de correo onde se pode alterar o contido moi facilmente. Ademais, a composición dun correo en texto claro permite especificar como remitente a dirección de correo do remitente ao valor que se desexe sin ningunha garantía de veracidade, por iso, a firma de e-mail debería ser prioritaria, e resulta dende o punto de vista da seguridade incluso máis importante que o cifrado, xa que garantir a autoría e a veracidade da información transmitida é básico.

Debilidade do Cifrado de Chave Pública

Como todo sistema, o cifrado de chave pública ten unha debilidade importante: **¿Como aseguramos que a chave pública da que dispoñemos pertence realmente a quen pensamos?**

Si a chave pública que empregamos é falsa, cando ciframos un documento este estará accesible para o verdadeiro propietario da mesma. Estaremos pensando que comunicamos cunha persoa e o estaremos facendo con outra. Ademais os documentos asinados dixitalmente polo impostor os tomaremos como verdadeiros.

Para evitar isto, se recorre ao uso de ***certificados de chave pública***.

Un certificado de chave pública é un documento electrónico que se utiliza para identificar ao propietario dunha chave pública. Un certificado inclúe información sobre o propietario dunha chave pública, o uso "autorizado" para esa chave, un período de validez e a propia chave pública que se está certificando.

Para asegurar a autenticidade destes certificados existen dúas aproximacións, unha centralizada (X509) e outra descentralizada (PGP).

X509

As Autoridades de Certificación

X509 é un estándar que define un formato para a creación de ***certificados de chave pública*** e unha infraestrutura para garantir a súa autenticidade.

X509 utiliza ***autoridades de certificación (CA)*** que son entidades encargadas de verificar e certificar a autenticidade dos certificados que expide. As autoridades de certificación posúen os seus propios certificados que se empregarán para verificar as firmas dixitais dos certificados que expidan mediante a sinatura dixital dos mesmos. Eses certificados estarán asinados dixitalmente por outra autoridade de certificación de maior rango.

> Obviamente ***existe como mínimo unha autoridade de certificación da que nos debemos fiar***, xa que non ten ninguén por enriba que asegure a autenticidade do seu propio certificado. Esas autoridades de certificación expiden os seus propios certificados e reciben o nome de autoridades raíz, ou ***root CA.*** *O software que faga uso de cifrado de chave pública X509 debe incorporar os certificados das root CA das que se fíe*.

Os CSR e os Certificados

Cando necesitamos un certificado X509 para asegurar un servizo público (ou interno a unha empresa) o procedemento a seguir é o seguinte:

1.- Creación dunha parella de chaves publica/privada
2.- Crear unha solicitude de certificado CSR (Certificate Sign Request). Esta solicitude levará basicamente a información “persoal” do certificado que identificará ao seu propietario e o uso para o que se desexa empregar.
3.- Enviar o CSR a unha autoridade de certificación

A autoridade certificadora verificará a autenticidade dos datos presentes no certificado de acordo ao nivel exixido (*certificate policy)*, que pode ser:

- **Validación de dominio**
  Utiliza os datos do DNS para validar a autenticidade da información de propietario presente no certificado. Nos DNS dun dominio se poden obter os rexistros whois que facilitan información sobre o propietario do dominio que se pode empregar para contrastar coa información presente na solicitude. **Este sistema de validacion non asegura 100% que unha entidade esté realmente ligada co certificado.**

- **Validación de organización**
  A validación de organización exixe que o solicitante teña dereitos de xestión dobre o nome de dominio, e probablemente que a entidade teña existencia legal. Os criterios empregados se deben indicar na ***certificate policy*** empregada.

- **Validación estendida**
  A validación estendida realiza comprobacións máis exhaustivas, e os certificados deste tipo unicamente poden ser emitidos por un pequeno conxunto de autoridades certificadoras que realizan comprobacións sobre os dereitos legais da entidade solicitante sobre a información incluída no certificado.

> Os principais navegadores amosan información sobre o estado do certificados de validación estendida e a entidade legal a quen pertencen. A maior parte deles amosan o nome da compañía a quen pertence o certificado e poden resaltalo cun símbolo ou cor especial na barra de direccións.

PGP

PGP é un sistema de cifrado de chave pública na que a autenticidade das chaves públicas se basea na confianza entre iguais establecendo “Redes de Confianza” en lugar de facelo en entidades certificadoras centralizadas.

A información ligada a unha chave pública (certificado) pode ser asinada dixitalmente por outro usuario no que se confíe. A firma pode facerse segundo diversos niveis de confianza.

PGP gracias a súa simplicidade e a non precisar o uso de autoridades de certificación centralizados foi utilizado habitualmente no correo electrónico, organizándose “festas de firmado” na que distintos usuarios firmaban as chaves públicas de outros mediante encontros persoais.

Para obter fácilmente as chaves públicas existen repositorios públicos como *https://www.rediris.es/keyserver/index.html.es*, *http://pgp.mit.edu/* ou *https://keybase.io/*