Entenda o que é um certificado digital SSL (OPENSSL)

fonte: http://www.nit10.com.br/dicas_tutoriais_ver.php?id=68&pg=0

1. O que é "Certificado Digital"?

É um documento criptografado que contém informações necessárias para identificação de uma pessoa física ou entidade jurídica. Qualquer conteúdo eletrônico que foi assinado digitalmente tem garantia de autenticidade de origem. Por exemplo: ao receber uma requisição, verifica-se os campos do certificado digital, a partir desses dados pode-se ter certeza que a origem da requisição é confiável e autentica.
Um certificado digital é emitido por uma Autoridade Certificadora (AC), uma entidade confiável do ponto de vista jurídico. No entanto, isso não impede que você mesmo crie um certificado digital para fins particulares, como mostraremos posteriormente nesse mesmo documento.

O certificado digital é transmitido através de uma conexão segura, que usa um protocolo de transmissão específico para transmitir dados criptografados: o SSL (Secure Socket Layer). Você só poderá usar um certificado digital se a aplicação (navegador da web, cliente de e-mail, etc) que você estiver utilizando implementar o suporte a conexões seguras.

Para que um certificado digital seja válido do ponto de vista jurídico, a operação de emissão do certificado deve envolver duas entidades:

* uma AR (Autoridade de Registro)
* e uma AC (Autoridade Certificadora)

O papel de uma AR (Autoridade de Registro) é requisitar a emissão de certificados digitais de uma AC (Autoridade Certificadora). Por exemplo: Uma organização financeira (Ex.:um banco) determina que cada usuário deve realizar transações criptografadas; então, ela (organização financeira) requisita certificados digitais de uma AC (Autoridade Certificadora) para todos os seus funcionários. Se a organização possuir cem funcionários, então, a AC (Autoridade Certificadora) irá gerar um certificado para cada funcionário, cem certificados ao todo.

Observação: Uma AR também pode ser uma AC e vice-versa.

Antes de prosseguirmos com a explicação, será necessário que o conceito de hash, criptografia e chaves sejam totalmente esclarecido.

*** Hash**

Uma função é dita unidirecional ou de hash quando possui a característica de transformar um texto de qualquer tamanho em um texto ininteligível de tamanho fixo. Além disso, ela também se caracteriza por ser fácil de calcular e difícil de serem invertidas. Um exemplo simples de uma função unidirecional, porém não aplicada à criptografia é o cálculo do resto da divisão de um número por outro. Se, por exemplo, criar-se uma função que calcule o resto da divisão de qualquer número por 10 o que temos é que qualquer que seja o número que será dividido por 10 o resultado é sempre um número entre 0 e 9. Isto é, o processo de cálculo é bem simples porém como saber se o resultado do resto for, por exemplo, 9 qual foi o número que divido por 10 gerou resto 9. É muito difícil

afirmar com certeza visto que existem infinitos números que divididos por 10 darão resto 9. A esse fato damos o nome de colisão. Isto é, quando dois números diferentes aplicados à função de hash geram o mesmo resultado dizemos que houve uma colisão. Nesse ponto é que se faz a diferença entre uma função de hash criptográfica e uma não criptográfica. A função de hash criptográfica é aquela que foi elaborada a possuir o mínimo de colisões possível. O HASH é one-way, ou seja, ao aplicar qualquer algoritmo HASH em qualquer conteúdo, será muito difícil ou quase impossível resolver o cálculo e chegar ao conteúdo original.
Podemos citar como exemplo o MD5 (Message Digest) e o SHA (Security Hash Algorithm).

Há dois tipos de criptografia utilizados atualmente: simétrica e assimétrica.

*** criptografia simétrica**
Ocorre quando duas partes trocam informações criptografadas e ambas utilizam a mesma chave criptográfica para decriptografar os dados transmitidos.
Podemos citar o base64 como algoritmo de criptografia simétrica.

* A criptografia assimétrica acontece quando duas partes trocam informações criptografadas porém, a origem geralmente utiliza uma chave privada para criptografar os dados e o destino utiliza uma chave pública para fazer o caminho inverso (decriptografar). A origem da chave pública é a chave privada mas, é totalmente improvável (teoricamente) que através da chave pública reconstrua-se a chave privada.

- O que é uma chave?

Antes de definir um conceito, vamos fazer uma analogia:
em uma casa nós geralmente encontramos portas e cofres para ajudar a garantir maior segurabilidade do imóvel. Para ter acesso aos compartimentos da casa será necessário uma chave pois, em cada um deles há uma porta ou cofre, cada qual com sua fechadura.

Temos:

* Cômodos na casa (quarto, sala, etc)
* Uma chave ou senha para cada meio de acesso (porta ou cofre)
* Uma chave-mestra capaz de operar (abir, fechar) qualquer porta ou cofre da casa.
* Uma fechadura em cada um dos meios de acesso aos cômodos ou compartimentos

Apenas pessoas que possuem a chave podem obter acesso em qualquer um dos cômodos da sua casa através de uma das portas. Se você é dono da casa, por que outras pessoas além de você possuem uma ou mais chaves para acessar compartimentos do imóvel? Porque você permitiu o acesso ao entregar a chave de um ou mais cômodos às pessoas autorizadas. Você é o único indivíduo que pode abrir qualquer uma das portas pois, também é o único que possui uma chave-mestra capaz de operar (abrir, fechar) qualquer uma das fechaduras. Mesmo em poder da chave de cada cômodo, qualquer indivíduo nunca poderia criar ou obter uma chave-mestra.
Para entender o que é e principalmente onde são aplicáveis os conceitos de chave pública e chave privada, basta imaginar:

Cômodos da casa <--> Arquivos no seu computador (criptografados ou não)
Chave-mestra <--> Chave privada

Outras chaves <--> Chaves públicas
Fechaduras <--> Algoritmos criptográficos

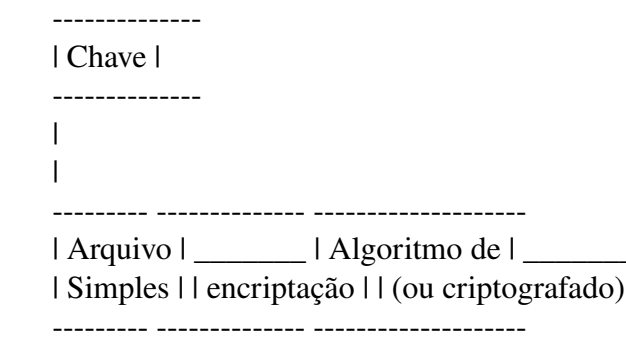
Assim sendo...

Tenhos um arquivo, desejamos criptografá-lo. Apenas uma pessoa será autorizada a realizar o método decriptográfico. Então, definimos o algoritmo criptográfico que será usado para cifrar o conteúdo. Feito isso, utilizamos a chave criptográfica para gerar uma cópia criptografada do arquivo de origem. Para que outras pessoas (autorizadas) visualizem o conteúdo do arquivo, utilizamos a chave privada para gerar chaves públicas. Dessa forma, apenas as pessoas que possuírem a chave pública poderão decriptografar o arquivo cifrado. Se o receptor do arquivo possuir sua chave pública, além de decriptografar também poderá criptografar arquivos utilizando nossa chave pública, e apenas o dono da chave privada poderá decriptografá-los.

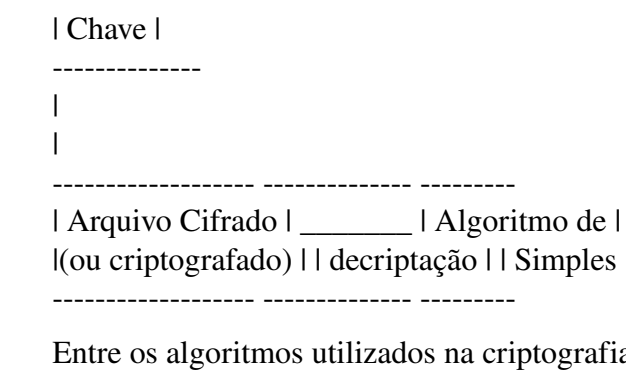
Nota: Da mesma forma que você não entregaria a sua chave-mestra para ninguém, a chave privada também não deve ser entregue. Com a sua chave privada, qualquer um pode decriptografar suas informações e criar chaves públicas para que outras pessoas também o façam.

Ilustrando a situação da criptografia assimétrica:

Criptografando:



Decriptografando:



Entre os algoritmos utilizados na criptografia assimétrica podemos citar o DES (Data Encryption Standard), o 3DES (Triple Data Encryption Standard) e o IDEA (International Data Encryption Algorithm).

Por que utilizar uma chave?

No caso da criptografia simétrica, não existe o conceito de chave pública e chave privada. O método criptográfico é realizado por um algoritmo de

domínio público e qualquer pessoa pode facilmente decriptografar conteúdos criptografados simetricamente (é como se você entregasse a chave-mestra da sua casa para qualquer pessoa). Conclui-se que a forma mais segura de criptografar conteúdo em nosso contexto tecnológico é a criptografia assimétrica. Obs.: Nenhum método criptográfico não-assimétrico é considerado suficientemente seguro para trafegar em uma rede tão insegura como a internet.

O certificado digital é gerado através de uma chave privada. Essa chave é intransferível e não deve estar em domínio de qualquer outra pessoa que não seja você mesmo, nem mesmo a AC (Autoridade Certificadora) que emitiu o certificado tem uma cópia da sua chave privada (que é gerada no seu computador). A partir da chave privada seus certificados digitais e suas chaves públicas são gerados. Se alguém obeter sua chave privada poderá gerar certificados digitais e passar-se por você em alguma transação na rede. Se por acaso ocorrer algum incidente fraudulento (uma transação bancária, por exemplo) e seu certificado foi usado para realizar a farsa, em primeira instância você será o principal suspeito.

Além de preservar a sua chave privada e seus certificados, alguns pré-requisitos e princípios básicos de segurança são necessários para garantir a segurança e confiabilidade dos seus certificados:

* As AC"""""""""""""""""""""""""s e as AR"""""""""""""""""""""""""s devem ser confiáveis entre si. Se isso não acontecer,
a possibilidade de fraudes e clonagens de certificados digitais aumentam consideravelmente. Por esse motivo, as AC"""""""""""""""""""""""""s devem restringir o número de AR"""""""""""""""""""""""""s parceiras apenas às entidades de sua confiança. Por esse motivo, é sempre bom informar-se sobre a relação da organização com a AC e principalmente sobre o processo de obtenção e geração da sua chave privada e os certificados emitidos.

* Caso haja suspeitas de roubo, clonagem ou adulteração de informações em algum processo que envolva o seu certificado digital, faça o pedido de revogação IMEDIATAMENTE! É a única maneira de contestar algum fato ou transação realizada por algum usuário mal intencionado.

* Nunca deixe sua chave privada em locais de acesso público (cd-rom, disquete, diretórios compartilhados, diretórios no servidor de backup da sua empresa, etc). Caso haja necessidade de uma cópia em disquete ou cd-rom, esconda-os em um local seguro de difícil acesso.

2. Usos dos certificados digitais

* Garantia de sigilo e privacidade na web - Ao visitar um site que está em um servidor WWW que implementa a certificação digital, o seu computador recebe o certificado contendo a chave pública do site que será utilizada para transmitir informações criptografadas entre as duas partes.

* Controle de acesso - Um servidor de aplicações pode solicitar um certificado digital do cliente, evitando o controle de acesso baseado no método tradicional: usuário e senha.

* Garantia de sigilo e privacidade - O sistema de correio eletrônico utilizado para troca de mensagens através da Internet não possui recursos nativos para impedir a violação da correspondência eletrônica. Com o uso

de certificados digitais, você pode selar a sua correspondência em um "envelope digital criptografado" e certificar-se de que apenas o destinatário será capaz de compreender seu conteúdo.

3. Ferramentas disponíveis no Linux

Podemos utilizar o "openssl" para gerar e gerenciar nossos certificados digitais. O openssl possui código-fonte aberto e é mantido por uma comunidade de desenvolvedores espalhados pela Internet.

4. Utilizando o openssl

Para utilizar o openssl basta fazer o download no site oficial www.openssl.org, descompactar, compilar e instalar.
Obs.: Não entraremos em detalhes sobre a instalação do openssl.

* Implementando a criptografia assimétrica utilizando o openssl

Para fixarmos os coneceitos, vamos imaginar um cenário real e quase comum (pelo menos desejado) por muitas organizações: criptografar documentos e criar o controle de acesso através das chaves públicas. O exemplo será realizado em quatro etapas:

Gerar uma chave privada de 2048 bits utilizando o algoritmo de criptografia 3DES
openssl genrsa -des3 -out chave_privada.key 2048

Criar uma chave pública utilizando a chave privada gerada anteriormente
openssl rsa -in chave_privada.key -pubout -out chave_publica.key

Criptografar o documento com nossa chave privada e gerar um arquivo criptografado texto_cifrado.des3
openssl rsautl -sign -inkey chave_privada.key -in texto.txt -out texto_cifrado.des3

Para que um indivíduo leia o arquivo criptografado, você deverá entregar-lhe a chave pública gerada anteriormente. Com a chave pública em mãos:
openssl rsautl -inkey chave_publica.key -in texto_cifrado.des3 -out texto.txt -pubin

Pronto! Acabamos de decriptografar o documento criptografado anteriormente texto.des3 (texto.txt criptografado).

*** Implementando a criptografia simétrica utilizando o openssl**

O processo envolve apenas duas etapas: gerar o conteúdo criptografado
openssl base64 -in arquivo.txt -out arquivo_cifrado.b64

decriptografar o conteúdo criptografado anteriormente
openssl base64 -d -in arquivo_cifrado.b64 -out arquivo.txt

Agora podemos começar a pensar em colocar em ação as boas práticas de segurança e principalmente conscientizar os usuários de que não há nada tão seguro que alguém não possa ver ou descobrir, mesmo utilizando a certificação digital e a criptografia ninguém pode garantir que você está seguro. A certificação digital aliada à criptografia são apenas agentes desencorajadores.