RNP
REDE NACIONAL DE ENSINO E PESQUISA

Especificações Técnicas do Servidor de Chaves PGP

Introdução

Em 1991, o pesquisador do Massachusetts Institute of Technology (MIT) Phillip Zimmermann criou um software que trouxe o mundo da criptografia para usuários comuns. Após vencer a barreira da exportação de criptografia dos Estados Unidos, o PGP ganhou o mundo e se tornou um padrão para criptografia pessoal.

Atualmente a criptografia consiste em uma série de fórmulas matemáticas, em que se utiliza um segredo (chamado de chave) para cifrar e decifrar a informação. Este segredo pode ser o mesmo para as duas operações (criptografia simétrica), ou pode haver segredos diferentes, um para cifrá-la e outro para decifrá-la, ou vice-versa (criptografia assimétrica).

Por meio de um software especial e um par de chaves, um usuário pode então utilizar essa tecnologia, para proteger suas informações pessoais.

O par de chaves possui as seguintes características:

Chave pública - disponível para qualquer usuário que queira se comunicar de forma segura;

Chave privada - chave secreta, que somente o dono do par de chaves conhece.

Através de software e um par de chaves, um usuário pode:

Assinar digitalmente um documento (garantir que o documento não foi alterado após a assinatura e que o mesmo foi assinado pelo dono do par de chaves que foi usado);

Cifrar um documento, de modo que só o dono do par de chaves destino seja capaz de ler a informação cifrada;

Assinar e cifrar um documento.

Infelizmente, o uso do software apenas garante que o dono do par de chaves realizou as operações, e não que o par de chaves em questão pertence realmente a uma pessoa. Não existe nenhum mecanismo que impeça a um usuário gerar um par de chaves com o nome de outro usuário. Para resolver esse problema, utilizam-se técnicas como certificação digital (versão eletrônica para os já conhecidos cartórios) e web-of-trust, que consiste em criar uma cadeia de confiança entre diferentes chaves. Este conceito será visto, adiante, com mais detalhes.

RNP
REDE NACIONAL DE ENSINO E PESQUISA

PGP e GnuPG

O PGP surgiu inicialmente como um produto gratuito, disponível para diversas plataformas. Entretanto, a partir de 2004 o PGP deixou de ser gratuito, o que fez com que muitos usuários de tecnologia migrassem para outros produtos, como o GnuPG (gpg), que é uma versão software livre do PGP, disponível para diversas plataformas. O gpg e o pgp são compatíveis, de modo que, a partir de um dos programas, é possível cifrar, decifrar, assinar e verificar assinaturas entre eles.

Teia de confiança (Web of Trust)

Conforme foi dito, anteriormente, existe um problema em se certificar que uma determinada chave realmente pertence a um usuário, site ou empresa. Essa dificuldade não é relativa apenas ao PGP, mas a qualquer sistema que use criptografia. Uma das soluções mais comuns consiste na compra de um certificado de uma entidade certificadora, que funciona como um cartório digital, atestando que uma determinada chave realmente pertence a um usuário específico.

Como no PGP, a idéia é disponibilizar criptografia para o público em geral, sem custos. Para isso, foi criado um método alternativo para se verificar se uma chave pertence a uma determinada pessoa, chamado web-of-trust. Neste método, a confiança vai sendo estabelecida através de uma rede de transitividade, onde se A confia em B e B confia em C, então A confia em C. Essa rede é construída por meio de uma relação pessoal entre dois indivíduos, constatação da identidade da chave, e assinatura da chave pública de um usuário pelo outro. Essas etapas acabam por gerar um laço de confiança. Essas relações de confiança convertem-se, então, em uma rede de confiança, como pode ser visto abaixo.

Teia de confiança Cais

Após a verificação da identidade do par de chaves, o próximo passo é a publicação desta chave num servidor de chaves, de modo que qualquer um que queira se comunicar possa obter facilmente a chave pública deste usuário. Quando uma chave é publicada, as assinaturas das pessoas que confiaram nesta chave também são publicadas, de modo que basta ao usuário confiar em uma das assinaturas da chave para que passe a confiar na chave.

Servidor de Chaves

Um servidor de chaves consiste em um software especial que possui uma interface via web, ou via e-mail, capaz de cadastrar, buscar e invalidar chaves públicas de usuários em qualquer parte do mundo. Estes servidores normalmente formam uma rede, de forma que, se um usuário publicar uma chave em um servidor na Espanha, por exemplo, esta atualização seja propagada para todos os servidores participantes da rede.

O servidor da RNP pertence à rede mundial, e, através dele, é possível consultar, adicionar e cancelar chaves na rede mundial de servidores. Para mais informações sobre o funcionamento específico do servidor de chaves, deve-se consultar a documentação incluída no endereço acima. Para outras informações a respeito de PGP e GPG, as referências podem ser consultadas na margem direita da página http://www.rnp.br/keyserver.php

Como funciona

Os servidores de chaves públicas (keyservers) PGP têm como único intuito ajudar o usuário a trocar chaves. De forma alguma, eles garantem a validade de uma determinada chave. Para avaliar a confiança de uma chave, é necessário o uso das assinaturas incorporadas à própria chave.

Os servidores de chaves públicas são acessíveis por e-mail ou pelo uso de uma interface web. O servidor RNP está disponível no endereço http://www.rnp.br/keyserver.

Há servidores de chaves públicas PGP distribuídos ao redor do mundo. Uma lista de alguns deles pode ser obtida em:

Currently functioning pgp.net servers http://keyserver.kjsl.com/~jharris/keyserver.html

Enviar uma chave pública para apenas um servidor é suficiente. Depois de processá-la, o servidor que recebeu a chave vai enviá-la para os outros servidores durante o processo de sincronização.

Guia do usuário

É fácil usar o servidor de chaves da RNP. Veja abaixo como fazer para submeter, procurar ou remover uma chave. Veja também como gerar um certificado de revogação.

1. Submetendo uma chave para o keyserver

Para submeter uma chave para o keyserver RNP, com o uso da interface web, você deve visitar o site do serviço e introduzir sua chave pública (em formato ASCII) no campo apropriado do formulário.

O envio de sua chave para apenas um servidor é suficiente. Depois de processá-la, o servidor a enviará para o restante dos servidores automaticamente. Se a chave

submetida já existir no servidor, ela é simplesmente atualizada pela adição de novas assinaturas ou identificadores associados a ela.

Tenha em mente que, uma vez submetida, a chave será distribuída para os demais servidores no mundo em pouco tempo. Portanto, certifique-se de que esta chave é valida.

Uma vez que a única maneira de remoção de uma chave do keyserver é feita por meio de um certificado de revogação de chave, recomendamos que você gere um certificado de revogação e o armazene em um local seguro, antes de submeter sua chave. A geração deste certificado requer que você tenha acesso à sua chave privada. Se você perder sua chave privada ou se esquecer de sua frase-chave (passphrase), você poderá usar o certificado de revogação e remover sua chave pública não mais válida.

2. Procurando chaves no servidor

Visite a página do Keyserver PGP da RNP e procure pela chave. A busca é possível usando-se o número-identificador (KeyID), parte do nome, e-mail ou qualquer campo de informação presente na chave.

3. Removendo uma chave do keyserver

É necessário um certificado de revogação de chave no processo de remoção de uma chave pública PGP do servidor.

Três casos distintos podem ocorrer:

- Você tem um certificado de revogação disponível, como recomendado na seção "Submetendo uma chave para o keyserver":

  - Visite a página web do keyserver e insira o certificado, usando o formulário apropriado. Depois clique no botão "Enviar".

- Você não tem o certificado de revogação disponível, mas tem acesso à sua chave privada:

- Gere um certificado de revogação e siga os passos descritos no item acima.

- Você não tem o certificado de revogação e perdeu sua chave privada ou esqueceu sua frase-chave (passphrase):

- Nesse caso, é completamente impossível remover sua chave do servidor, uma vez que você não pode oferecer provas confiáveis de sua identidade e direitos sobre a chave.

4. Gerando um certificado de revogação

A geração de um certificado de revogação depende da versão de PGP que você usa:

- PGP versão 2.6.3:
    1. Desative sua chave usando a opção -kd:
    2. `pgp -kd sua_chave`
    3. Responda "yes" para as questões sobre a revogação de sua chave.
    4. Uma vez revogada, gere uma versão de sua chave em formato ASCII:
    5. `pgp -kxa sua_chave`
- PGP versão 5.X:
    1. Desative sua chave usando a opção --revoke:
    2. `pgpk --revoke sua_chave`
    3. Responda "yes" para as questões sobre a revogação de sua chave.
    4. Uma vez revogada, gere uma versão de sua chave em formato ASCII:
    5. `pgpk -xa sua_chave`
- PGP versão 6.X:
    1. Desative sua chave usando a opção -kd:
    2. `pgp6 -kd sua_chave`
    3. Responda "yes" para as questões sobre a revogação de sua chave.
    4. Uma vez revogada, gere uma versão de sua chave em formato ASCII:
    5. `pgp6 -kxa sua_chave`
- GNU PGP:
    1. Gere um certificado de revogação usando a opção --gen-revoke:
    2. `gpg --gen-revoke sua_chave`

3. Responda "yes" para as questões sobre a revogação de sua chave.