

Converter certificados para utilizar no Monsta

No mundo da segurança digital, os certificados SSL/TLS são a espinha dorsal da comunicação segura na web (HTTPS), garantindo a autenticidade e a criptografia dos dados trocados entre usuários e servidores.

Este guia foi criado para auxiliar você um passo a passo, como utilizar a ferramenta padrão da indústria, **OpenSSL**, para converter certificados e chaves privadas de formatos comuns (como `.pfx` ou `.key` e `.crt`) para o formato PEM, garantindo que você tenha os componentes necessários – a **chave privada RSA** (`.pem`) e o **certificado público** (`.pem`) – prontos para serem utilizados no Monsta.

Certificados .crt e .key em formato PEM

Ao trabalhar com certificados digitais para segurança, você invariavelmente encontrará dois tipos de arquivos principais, geralmente com as extensões `.crt` e `.key`. Eles funcionam juntos, como um par, mas têm propósitos muito diferentes e um deles exige muito cuidado no manuseio.

O que é cada arquivo

certificado.crt: É a sua **Chave Pública**, uma longa sequência de caracteres que pode ser compartilhada livremente. Qualquer pessoa pode usá-la para criptografar mensagens que apenas o servidor HTTP do Monsta (com sua chave privada) poderá ler.

certificado.key: É sua **Chave Privada**, uma longa sequência de caracteres, matematicamente ligada à chave pública no seu arquivo `.crt`. Apenas esta chave privada pode descriptografar as mensagens que foram criptografadas usando a chave pública correspondente (do seu arquivo `certificado.crt`). É assim que seu servidor lê dados enviados de forma segura por um visitante.

Como importá-los no Monsta

Certifique-se de que os arquivos estão em formato PEM, ou seja, o início e o final do arquivo devem estar no formato informado abaixo:

```
-----BEGIN PRIVATE KEY-----
```

```
Texto da chave  
...  
...  
-----END PRIVATE KEY-----
```

Uma vez que as chaves estão nesse formato, basta renomear os arquivos para .pem, como abaixo:

```
chave_publica.pem
```

```
chave_privada.pem
```

Após esse procedimento, no Monsta, acesse o menu "Configuração" e selecione o item "Certificado TLS". Na tela que aparecer, selecione a opção "Certificado Próprio" e faça o upload de seus arquivos conforme exemplo abaixo:

Certificado TLS

Método

Certificado Próprio

Public Key

chave_publica.pem

Private Key

chave_privada.pem

Salvar

Fechar

Certificados .pfx

O certificado em arquivo `[.pfx]` é um formato de arquivo **contêiner**. Ele é projetado para **agrupar vários itens criptográficos** importantes em um único lugar. Dentro desse arquivo, você normalmente encontrará:

1. A **Chave Privada**;
2. O **Certificado Público** correspondente;
3. **(Opcional, mas comum)** A **Cadeia de Certificados Intermediários/Raiz** (os certificados da Autoridade Certificadora que validam o seu certificado).

Quase sempre, um arquivo `[.pfx]` é **protegido por uma senha**. Essa senha é crucial, pois ela criptografa o conteúdo do pacote, protegendo especialmente a chave privada que está lá dentro. Você precisará dessa senha para abrir o "cofre" e acessar os arquivos internos.

Para extrair os arquivos necessários pelo servidor HTTP do Monsta, será necessário o auxílio do programa openssl. O procedimento abaixo apresentado deve ser feito em um servidor Linux.

Para esses exemplos, faça o upload dos seus arquivos para um servidor Linux de sua escolha.

Instalar o openssl

Certifique-se de que o seu servidor Linux possui o software openssl. Caso necessite instalá-lo, utilize os comandos abaixo:

Fedora

```
yum install -y openssl
```

Ubuntu/Debian

```
apt-get install -y openssl
```

Extrair a chave pública e privada para arquivos

Execute os comandos abaixo para extrair as chaves pública e privada do seu certificado .pfx.

Caso seu arquivo esteja protegido por senha, a mesma será solicitada durante a execução dos comandos. Se você não possua a senha, contate a entidade que gerou seu certificado para maiores informações.

Chave Pública

```
openssl pkcs12 -in certificado.pfx -clcerts -nokeys -out chave_publica.pem
```

Chave Privada

```
openssl pkcs12 -in certificado.pfx -nocerts -nodes -out chave_privada.pem
```

Caso ocorra algum erro como este:

Global default library context, Algorithm (RC2-40-CBC : 0), Properties ()

Provavelmente seu certificado utiliza um algoritmo de critpografia fraco ou antigo. Para resolver esse problema, adicione o parâmetro "-provider legacy" ao final da linha de comando do openssl, por exemplo:

```
openssl pkcs12 -in certificado.pfx -nocerts -nodes -out chave_privada.pem -provider legacy
```

Importar os certificados no Monsta

Após esse procedimento, copie os arquivos `chave_publica.pem` e `chave_privada.pem` para seu computador. Dentro do Monsta, acesse o menu "Configuração" e selecione o item "Certificado TLS". Na tela que aparecer, selecione a opção "Certificado Próprio" e faça o upload de seus arquivos conforme exemplo abaixo:

Certificado TLS

Método

Certificado Próprio

Public Key

chave_publica.pem

Private Key

chave_privada.pem

Salvar

Fechar

Ao final, clique em "Salvar" para ativar seu novo certificado.

Os certificados TLS possuem uma data de validade. Certifique-se de renovar os certificados antes que eles expirem para evitar interrupções na comunicação segura.

Contato

Monsta Tecnologia Ltda

Site: <http://www.monsta.com.br>

Downloads: <http://www.monsta.com.br/download.html>

E-mail: contato@monsta.com.br



Revision #12

Created 10 April 2025 13:52:22 by Monsta Tecnologia

Updated 11 April 2025 18:41:04 by Eduardo