Safra

Tradição Secular de Segurança

Serviços Web para Clientes

Procedimento para Obtenção de Certificado Digital

Conteúdo

Versão 1.2
Fevereiro/2018

1. Objetivo

As instruções a seguir descrevem como gerar uma requisição de certificado (CSR) para assinatura pela autoridade certificadora do Banco Safra. O certificado do tipo cliente assinado digitalmente permite autenticação e criptografia durante a comunicação com os serviços web do Banco Safra.

2. Preparação para geração do pedido de certificado

Você deve instalar o OpenSSL em seu servidor. Este é um pacote comum e está disponível em todas as principais distribuições Linux através dos instaladores de pacotes. Também é possível obter um pacote do OpenSSL para a Windows.

Caso você já possua o OpenSSL instalado, vá direto ao item 3.

Linux

Para verificar se o pacote OpenSSL está instalado em um sistema que usa yum (como CentOS ou Red Hat Enterprise Linux), execute o seguinte comando:

```
rpm -qa | grep -i openssl
```

O comando anterior deve retornar os seguintes pacotes ou similares:

```
openssl-1.0.1e-48.el6_8.1.x86_64
openssl-devel-1.0.1e-48.el6 8.1.x86_64
openssl-1.0.1e-48.el6_8.1.i686
```

Se esses pacotes não forem retornados, instale o OpenSSL executando o seguinte comando:

```
yum install openssl openssl-devel
```

Para verificar se o OpenSSL está instalado em um sistema Debian ou Ubuntu, execute o seguinte comando:

```
dpkg -l | grep openssl
```

Você deve receber uma saída similar a esta:

```
ii    libgnutls-openssl27           GNU TLS library - OpenSSL wrapper
ii    openssl                       Secure Sockets Layer toolkit
```

Se você não tiver o resultado esperado, instale o OpenSSL, executando o seguinte comando:

```
apt-get install openssl
```

Windows

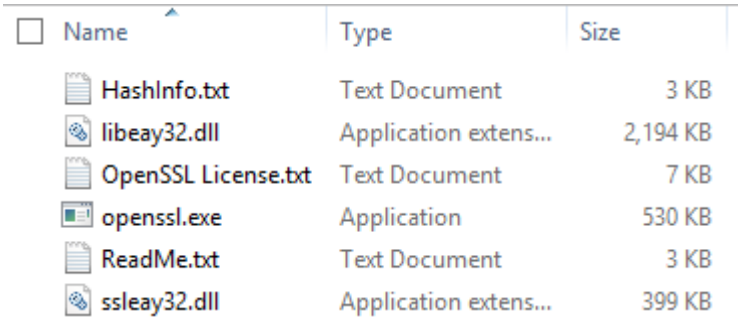
Em um sistema Windows, baixe o pacote *OpenSSL for Windows pre-compiled* no endereço https://wiki.openssl.org/index.php/Binaries.

Third Party OpenSSL Related Binary Distributions

Product	Description	URL
OpenSSL for Windows	Works with MSVC++, Builder 3/4/5, and MinGW. Comes in form of self-install executables.	https://slproweb.com/products/Win32OpenSSL.html
OpenSSL for Windows	Pre-compiled Win32/64 libraries without external dependencies to the Microsoft Visual Studio Runtime DLLs, except for the system provided msvcrt.dll.	https://indy.fulgan.com/SSL/
OpenSSL for Solaris	Versions for Solaris 2.5 - 11 SPARC and X86	http://www.unixpackages.com/
OpensSSL for Windows, Linux and OSx	Pre-compiled packages at conan.io package manager: *Windows* x86/x86_64 (Visual Studio 10, 12, 14) *Linux* x86/x86_64 (gcc 4.6, 4.8, 4.9 and 5.2) *OSx* (Apple clang)	https://www.conan.io/search?q=OpenSSL

Faça o download do pacote 32 ou 64 bit de acordo com a versão do Windows.

Extraia o pacote e execute openssl.exe a partir do Prompt de Comando ou PowerShell.



3. Geração e submissão do pedido de certificado

AVISO: Os passos a seguir descrevem o procedimento para o ambiente de homologação. Para o ambiente de Produção, basta repeti-los, substituindo o sufixo *HML* por *PRD*.

Passo 1: Geração da chave RSA

Execute os seguintes comandos para criar um diretório a fim de armazenar sua chave RSA, substituindo o nome de diretório por um de sua escolha.

```
mkdir cert-hml
cd cert-hml
```

Execute o seguinte comando para gerar uma chave privada:

```
openssl genrsa -out client.key 2048
```

ATENÇÃO: O arquivo da chave privada deve ser tratado como uma informação confidencial em sua empresa. Armazene-o em um local seguro, com em um cofre virtual.

Passo 2: Criando um CSR

Digite o seguinte comando para criar um CSR com a chave privada RSA:

```
openssl req -new -sha256 -key client.key -out client.csr
```

Quando solicitado, insira as informações necessárias para criar um CSR usando as convenções mostradas na tabela a seguir.

AVISO: Não utilize acentuação ou caracteres especiais no preenchimento dos campos.

Campo	Descrição	Exemplo
Country	A abreviatura ISO de duas letras para o seu país.	BR
State or Province	O estado ou província onde sua organização está legalmente localizada. Não use uma abreviatura.	Sao Paulo
City or Locality	A cidade onde sua organização está localizada legalmente.	Sao Paulo
Organization Name	O nome legal exato da sua organização. Não abrevie o nome da sua organização.	Banco Safra SA
Organizational Unit	Seção da organização. Deve ser o departamento ou área responsável pela Segurança da Informação na sua organização.	Seguranca da Informacao

Common Name	O nome comum que identifica a sua organização junto ao Banco Safra. É um conjunto de informações separadas por dois pontos ":", sendo: ***HML*** ou ***PRD***: Indica o ambiente, se homologação ou produção. ***RAZAO SOCIAL***: Razão social da organização. ***PJ***: Fixo, sempre pessoa jurídica ***01234567890122***: CNPJ completo da sua organização, sem pontos ou traço.	HML:BANCO SAFRA SA:PJ:58160789000128
Email Address	Um endereço de e-mail para contato com sua empresa. Será usado para notificação quando o certificado estiver próximo da sua expiração.	certificados.si@safra.com.br

Deixe a senha de desafio em branco e o nome opcional da empresa (pressione Enter).

Passo 3: Verifique seu CSR

Execute o seguinte comando para verificar seu CSR:

```
openssl req -noout -text -in client.csr
```

Você deve receber uma saída como esta:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=BR, ST=Sao Paulo, L=Sao Paulo, O=Banco Safra SA,
OU=Seguranca da Informacao, CN=HML:BANCO SAFRA
SA:PJ:58160789000128/emailAddress=security@safra.com.br
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bb:40:73:de:d2:84:a1:ac:84:df:87:94:f2:cc:
:_
```

Passo 4: Envie o conteúdo do seu CSR para o Banco Safra

Você deve enviar o conteúdo do arquivo de requisição de certificado (CSR) para que o Banco Safra possa realizar o processo de assinatura. Em um sistema Windows, clique com o botão direito no arquivo .csr, selecione Abrir Com, e então escolha um editor de texto como o Bloco de Notas. No Linux copie a saída do comando:

```
cat client.csr
```

Cole todo o conteúdo do texto, incluindo `-----BEGIN CERTIFICATE REQUEST-----` e `-----END CERTIFICATE REQUEST-----`, no corpo de um e-mail e envie:

Para: certificados.si@safra.com.br
Assunto: Assinatura de Certificado Safra SV C2

Em até 3 dias úteis você deve receber uma resposta com certificado assinado.

4. Preparação do certificado assinado para instalação

Passo 1: Salve o certificado assinado

Após receber o certificado assinado pelo Banco Safra por e-mail, copie o conteúdo, incluindo *-----BEGIN CERTIFICATE-----* e *-----END CERTIFICATE-----*, para um novo arquivo texto com extensão cer. Em um sistema Windows você pode fazer isso com o Bloco de Notas, no Linux use o comando:

```
nano client.cer
```

ATENÇÃO: Respeite as quebras de linha do texto, caso contrário, o certificado poderá ficar inválido e não funcionar corretamente.

Passo 2: Una o arquivo CSR com o KEY

Se uma aplicação é executada em ambiente Linux, provavelmente será necessário um arquivo PEM. Para tanto execute o seguinte comando:

```
cat client.key client.cer > client.pem
```

Caso sua aplicação rode em ambiente Windows, tipicamente é necessário um arquivo PFX no formato PKCS#12. Para gerar esse arquivo use o comando:

```
openssl pkcs12 -export -in client.cer -inkey client.key -out client.pfx
```

Deixe a senha de desafio em branco (pressione Enter duas vezes para confirmar).