# Manual de instalação e configuração OpenSSL [Windows]

Leandro Kümmel Tria Mendes

11 de setembro de 2013

# Sumário



# Lista de Figuras

# Lista de Tabelas

## 1 Pré-requisitos

Para a instalação e configuração do sistema que gera certificados digitais é necessária a instalação do OpenSSL[1]. A máquina alvo deverá conter a última versão do Apache (versão $\geq$ 2.2) **com módulo de ssl**[2]

## 2 Instalação e Gerar Certificado

I **Instalação**: A instalação do OpenSSL é básica, simples next-next-finish (NNF).**A instalação deverá, por padrão, ser realizada no diretório raiz C:/**. Após a instalação teremos a seguinte pasta: **C:/Openssl/**

II **Gerar certificado**: Para gerar um novo certificado devemos abrir o DOS (iniciar− >executar: digite "*cmd*" e enter) navegar até a pasta de instalação[I] entre em **/bin** e digitar os comando abaixo.

**Listing 1** Gerar chave e certificado

```
1:    # gerar arquivo com a chave privada.
2:    openssl genrsa -aes256 -out privada.key 2048
3:    # gerar a chave publica.
4:    openssl rsa -in privada.key -out publica.key
5:    # gerar o certificado digital utilizando a configuracao padrao do openssl.
6:    openssl req -new -x509 -nodes -sha1 -key publica.key \
7:    -out publica.crt -days 999 -config C:\Openssl\share\openssl.cnf
```

A chave pública e o certificado encontram-se em **C:/Openssl/bin/** publica.key e publica.crt, respectivamente.

[1] http://slproweb.com/products/Win32OpenSSL.html

[2] http://ftp.unicamp.br/pub/apache//httpd/binaries/win32/httpd-2.2.25-win32-x86-openssl-0.9.8y.msi

# 3 Configurar Apache + SSL

Nessa seção será necessário a cópia de alguns arquivos para a pasta **system32** do windows e a configuração de alguns arquivos do apache[3]

# 4 System 32

Navegue nas pastas até a instalação do Apache e procure na pasta **bin** as .dll **ssleay32.dll** e **libeay32.dll**. Copie as mesmas para a pasta **C:/Windows/system32**[4]

# 5 Apache

Para esse item é necessário lembrar a pasta de instalação do Apache, assim como sua pasta de configuração. A instalação, exemplo, está localizada em **S:/Apache/**.[5].
A cada conexão no Apache haverá a troca de certificados e chave pública entre o cliente e servidor. Para isso deveremos criar uma pasta localizada em **S:/Apache/conf/extra/**, nominada **ssl**. Resultando em um nova pasta **S:/Apache/conf/extra/ssl/**.
Lembrando o item I, temos a chave e certificado já gerados e presentes em **C:/Openssl/bin/**. Copie os arquivos criados (publica.key e publica.crt) para a nova pasta criada acima. Concluindo, ao navegar na pasta **/conf/extra/ssl/** do Apache, deveremos encontrar dois arquivos [II], um com extensão **.key** e o outro com **.crt**.

- **httpd-ssl.conf**: Arquivo localizado em **S:/Apache/conf/extra/**

**Listing 2** httpd-ssl.conf

```
1:    # Localize SSLSessionCache e troque seu conteudo por
2:    SSLSessionCache "shmcb:S:/Apache/logs/ssl_scache(512000)"
3:
4:    # Localize SSLCertificateFile e coloque o caminho do certificado
5:    SSLCertificateFile "S:/Apache/conf/extra/ssl/publica.crt"
6:
7:    # Localize SSLCertificateKeyFile e coloque o caminho da chave publica
8:    SSLCertificateKeyFil "S:/Apache/conf/extra/ssl/publica.key"
9:
10:   # Verifique se o SSLMutex esta como default
11:   SSLMutex default
12:
13:   # Localize <VirtualHost> e troque seu conteudo por
14:   DocumentRoot "S:/htdocs" # diretorio dos projetos
15:   ServerName engenheiro.cpo.unicamp.br:443 # servidor
16:   ServerAdmin admin@localhost # email do administrador
17:   ErrorLog "S:/Apache/logs/ssl_error.log" # log de erro
18:   TransferLog "S:/Apache/logs/ssl_access.log" # log de transferencia
```

[3]Lembre-se que a instalação do apache deverá ser feita com uma versão acima da 2.2 e com OpenSSL nativo.
[4]Esse caminho pode variar, dependendo da versão do S.O. e de sua instalação
[5]Vide: engenheiro.cpo.unicamp.br

```
19:
20:     # Localize a linha SSLOptions +StdEnvVars
21:     # Substitua por
22:     SSLOptions +StdEnvVars
23:     Options Indexes FollowSymLinks MultiViews
24:     AllowOverride All
25:     Order allow,deny
26:     allow from all
27:
28:     # Localze a linha CustomLog e troque seu conteudo por
29:     CustomLog "S:/Apache/logs/ssl_request.log" \
30:     "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

- **httpd.conf**: Arquivo localizado em **S:/Apache/conf/**

```
1:      Procure por mod_ssl.so e descomente a linha, caso esteja comentada.
2:      Ache a linha com extra/httpd-ssl.conf e tambem a descomente.
```

Reinicie o serviço do apache e pronto! Para testar acesse o DocumentRoot através de seu browser utilizando https:// ao invés de http://.