Certificados SSL

- Instalar certificados do ICPEdu

Instalar certificados do ICPEdu

1. Introdução

A Infraestrutura de Chaves Públicas para Ensino e Pesquisa (AC ICPEdu) é o serviço de certificação digital oferecido pela RNP, que provê infraestrutura pronta para a emissão de certificados digitais e chaves de segurança.

A modalidade adotada pelo IFPE é a “Certificado Corporativo”, onde as instituições clientes emitem gratuitamente certificados digitais qualificados pela GlobalSign, uma das maiores autoridades certificadoras do mundo. Isso fortalece a confiança dos usuários, que têm a garantia de estar fazendo negócios com uma instituição idônea.

Este documento visa a orientar a configuração do certificado emitido através do Sistema de Chamados do IFPE nos servidores web Apache e NGinx.

Observe que todos os passos são obrigatórios.

2. Utilizando os arquivos

Neste ponto devemos ter os seguintes arquivos disponíveis:

- ***dh-4096.pem***

  Arquivo contém os parâmetros Diffie-Hellman usado para fortalecer o canal criptografado e dificultar ataques que interceptam o tráfego criptografado.

- ***icpedu-chain.crt***

  Arquivo contém a cadeia de autoridades de certificação que inclui a CA do ICPEdu e as da Globalsign, usado para permitir que o cliente confira a validade dos certificados.

- ***globalsign-ca.crt***

Arquivo contém o certificado da CA raiz da Globalsign, usado para permitir que o cliente confira a validade dos certificados.

- ***CEPO171124239914-chain.crt***

  Arquivo inclui a cadeia de certificados que inclui o do ICPEdu, os da Globalsign, e o certificado gerado para o dispositivo final ou aplicação. É ele que será apresentado aos navegadores dos usuários.

- ***CEPO171124239914.key***

  Arquivo inclui a chave privada do certificado gerado para o dispositivo final ou aplicação. Ele será usada para compor o fluxo criptografado, juntamente com o certificado, aos navegadores dos usuários.

A seguir estão instruções de como utilizar os arquivos gerados nos servidores HTTP Apache e NGinx, instalados nos sistemas operacionais Linux Debian (os comandos são também válidos para Ubuntu) e Centos.

2.1. O diretório dos arquivos

Para seguir os passos definidos neste documento, copie os arquivos para o diretório "***/etc/ssl/private/***".

```
[usuario@linux /tmp]$ sudo mkdir -p /etc/ssl/private
[usuario@linux /tmp]$ sudo cp *.crt *.key *.pem *.pfx /etc/ssl/private
```

> Os passos a seguir não funcionarão se os arquivos não estiverem no diretório "/etc/ssl/private/".

2.2. Configuração com Apache

> Por padrão, os arquivos de configuração dos sites do Apache **no Debian e Ubuntu ficam localizados em *"/etc/apache2/sites-available/"*** . Caso esteja instalado **no Centos, ficam em *"/etc/httpd/conf.d"***

No arquivo de cada host, dentro da sessão "*<VirtualHost>*" onde o SSL esteja habilitado inclua as definições de modo que se pareça com o que é mostrado a seguir:

> Para identificar qual VirtualHost possui SSL habilitado, observe se uma linha com o conteúdo "***SSLEngine On***" existe

Caso a versão do apache seja inferior a 2.3.6

```
<VirtualHost <server_name>:443>
  Listen 443
  SSLEngine on
  ServerName <server_name>:443
  ...

  # Certificados
  SSLCertificateFile /etc/ssl/private/CEPO171124239914-chain.crt
  SSLCACertificateFile /etc/ssl/private/globalsign-ca.crt
  SSLCertificateKeyFile /etc/ssl/private/CEPO171124239914.key
  SSLCertificateChainFile /etc/ssl/private/icpedu-chain.crt
  ...
</VirtualHost>
```

Caso a versão do apache seja superior a 2.3.6 e inferior a 2.4.8

```
<VirtualHost <server_name>:443>
  Listen 443
  SSLEngine on
  ServerName <server_name>:443
  ...
  # OCSP Stappling
  SSLUseStapling On
  SSLStaplingCache "shmcb:/tmp/stapling-cache(150000)"

  # Certificados
  SSLCertificateFile /etc/ssl/private/CEPO171124239914-chain.crt
  SSLCACertificateFile /etc/ssl/private/globalsign-ca.crt
  SSLCertificateKeyFile /etc/ssl/private/CEPO171124239914.key
  SSLCertificateChainFile /etc/ssl/private/icpedu-chain.crt
  ...
</VirtualHost>
```

Caso a versão do apache seja a 2.4.8 ou superior

No arquivo de cada host, dentro da sessão "*<VirtualHost>*" onde o SSL esteja habilitado inclua as definições (da linha 6 até a 14) de modo que se pareça com o que é mostrado a seguir:

```
<VirtualHost <server_name>:443>
  Listen 443
  SSLEngine on
```

```
    ServerName <server_name>:443
    ...
    # OCSP Stappling
    SSLUseStapling On
    SSLStaplingCache "shmcb:/tmp/stapling-cache(150000)"

    # Certificados
    SSLOpenSSLConfCmd DHParameters /etc/ssl/private/dh-4096.pem
    SSLCACertificateFile /etc/ssl/private/globalsign-ca.crt
    SSLCertificateFile /etc/ssl/private/CEPO171124239914-chain.crt
    SSLCertificateKeyFile /etc/ssl/private/CEPO171124239914.key
    ...
</VirtualHost>
```

Após realizar a configuração mostrada é preciso aplicar as alterações.

Procure por erros de configuração:

```
[usuario@linux ~]$ sudo apache2ctl -t
```

Se tudo correu bem, reinicie o serviço (no Debian/Ubuntu/Centos):

```
[usuario@linux ~]$ sudo apache2ctl -k restart
```

> Para que as alterações entrem em vigor é necessário reiniciar o serviço

2.3. Configuração com NGinx

> Utilize o comando **nginx -v** para saber a versão do nginx atualmente instalada. **Para este documento, é necessário que versão seja igual ou superior a 1.3.7.**

> Por padrão, os arquivos de configuração dos sites do **NGinx no Debian e Ubuntu ficam localizados em *"/etc/nginx/sites-available/*"** . Caso esteja instalado **no Centos, ficam em *"/etc/nginx/conf.d"***

No arquivo de cada host, na sessão "*server*" onde o SSL esteja habilitado inclua as definições (da linha 4 até a 13) de modo que se pareça com o que é mostrado a seguir:

> Para identificar qual VirtualHost possui SSL habilitado, observe se uma linha com o conteúdo "***listen 443 ssl***" existe

```
server {
  listen 443 ssl;
  ...
  # OCSP Stappling
  ssl_stapling on;
  ssl_stapling_verify on;
  resolver 208.67.220.220 208.67.222.222 valid=600s;

  # Certificados
  ssl_dhparam /etc/ssl/private/dh-4096.pem;
  ssl_certificate /etc/ssl/private/CEPO171124239914-chain.crt;
  ssl_certificate_key /etc/ssl/private/CEPO171124239914.key;
  ssl_trusted_certificate /etc/ssl/private/icpedu-chain.crt;
  ...
}
```

Após realizar a configuração mostrada é preciso aplicar as alterações.

Procure por erros de configuração:

```
[usuario@linux ~]$ sudo nginx -t
```

Se tudo correu bem, reinicie o serviço (no Debian/Ubuntu e Centos):

```
[usuario@linux ~]$ sudo nginx -s reload
```

> Para que as alterações entrem em vigor é necessário reiniciar o serviço

2.4 Outros sistemas

Caso haja a necessidade de instalar o certificado em outros oftwares (como MS IIS, MS Exchange e CPanel), acesse a documentação de instalação disponibilizada pela Globalsign clicando neste link.