

Certificação Digital ICPEdu (SSL) no Servidor Linux

Procedimento de solicitação e instalação da certificação digital RNP/ICPEdu em um servidor web Apache no ambiente Linux.

- [Introdução](#)
- [1. Conceitos e ferramentas utilizadas](#)
- [2. Geração da requisição de certificado](#)
- [3. Envio a requisição de certificado para a Reitoria](#)
- [4. Hierarquia da certificação e download dos arquivos do certificado digital](#)
- [5. Exemplo da instalação da certificação no servidor web Apache](#)
- [Instalação do certificado SSL](#)

Introdução

O serviço ICPedu (Certificado Corporativo da Infraestrutura de Chaves Públicas para Ensino e Pesquisa) oferecido pela RNP (Rede Nacional de Ensino e Pesquisa) provê segurança e confiabilidade no acesso aos serviços de TIC de suas Instituições membro. Através da emissão de certificados digitais do tipo SSL (Secure Socket Layer) o serviço garante autenticidade na comunicação cliente-instituição através da web, fortalecendo a confiança dos usuários, que têm a garantia de estar acessando serviços de uma Instituição idônea.

A solicitação, configuração e administração dos certificados é de responsabilidade da Instituição requerente, que deve, a princípio, gerar uma Requisição de Certificado e uma Chave Privada, para que então a certificação possa ser registrada junto a RNP. A Instituição deve então instalar o certificado validado pela Rede Nacional de Pesquisa em seus servidores. Com isso, os usuários então passarão a acessar os serviços em um ambiente criptografado e certificado.

A Reitoria do Instituto Federal do Sertão Pernambucano atua como intermediadora no registro dos certificados junto a RNP. Logo, os Campi devem solicitar a Reitoria o registro dos seus certificados. Para tanto, esse documento apresenta os passos a serem seguidos.

Mais informações podem ser obtidas na wiki do projeto ICPedu em <https://wiki.rnp.br/display/GI>.

1. Conceitos e ferramentas utilizadas

Uma conexão utilizando o protocolo para conexões seguras SSL é sempre iniciada pelo cliente. Quando um usuário solicita a conexão com um site seguro, o navegador web (Firefox, Microsoft Edge, Opera, Chrome, etc.) solicita o envio do Certificado Digital e verifica se:


- O certificado enviado é confiável;
- O certificado é válido;
- O certificado está relacionado com o site que o enviou.

Uma vez que as informações acima tenham sido confirmadas, o navegador envia sua chave pública e as mensagens podem ser trocadas. Uma mensagem que tenha sido criptografada com uma chave pública somente poderá ser decifrada com a sua chave privada (simétrica) correspondente. Analogamente, a mensagem seria uma fechadura que possui duas chaves, umas para trancar (criptografar) e outra para destrancar (decifrar) a porta.

[prototolo SSLCPEdu.jpg](#)

Um servidor web protegido pelo protocolo SSL utiliza o protocolo HTTPS (Hyper Text Transfer Protocol Secure), possuindo uma URL que começa em “https://”, onde o S significa “secured” (seguro, protegido).

Os algoritmos de criptografia abaixo utilizam o protocolo SSL:

- DES e DAS - algoritmo de criptografia usado pelo governo americano;
- KEA - usado para a troca de chaves pelo governo americano;
- MD5 - muito usado por desenvolvedores de software para que o usuário tenha certeza que o aplicativo não foi alterado;
-  RSA - Algoritmo de chave pública para criptografia e autenticação;
- SHA-1 - também usado pelo governo americano.

A versão 3.0 do SSL exige a autenticação de ambas as partes envolvidas na troca de mensagens.

Ou seja, tanto cliente quanto servidor deve fazer autenticação e afirmar que são que dizem ser.

O projeto ICPEdu recomenda a ferramenta OpenSSL para a geração da Requisição de Certificado Digital. Para tanto, este guia utiliza a ferramenta OpenSSL na versão 1.1.1, versão estável presente nos repositórios padrões das distribuições Linux Debian 10 e CentOS 8.

A ferramenta OpenSSL é livre para a implementação de protocolos para Conexões Seguras SSL (Secure Sockets Layer) e Transporte Seguro TLS (Transport Layer Security) de dados em uma rede, possibilitando a criação de certificados, chaves sumarizadas, chaves públicas e privadas e a criptografia de arquivos.

Como os certificados SSL são comumente utilizados em servidores de hospedagem web para proteção de sites corporativos, será exemplificada a instalação final dos certificados digitais em um servidor web Apache versão 2.4 em ambiente Linux Debian 10 e CentOS 8. Essa versão do Apache também está presente nos repositórios padrões de ambas as distribuições.

2. Geração da requisição de certificado

O Certificate Signing Request (CSR) é um arquivo de texto criptografado contendo as informações para a solicitação do Certificado Digital. O CSR contém as informações da Instituição (nome, departamento, cidade, estado, país) e a URL onde o certificado SSL será utilizado (Common Name).

Para obter certificados digitais para os serviços computacionais é necessário:

- Chave Privada RSA 2048 bits;
- Uma requisição de certificado CSR;
- Compatibilidade com SHA-256.

A ferramenta OpenSSL é usada para criar a Chave Privada (arquivo .key) e a Solicitação de Assinatura de Certificado (arquivo .csr). Ambas devem ser geradas conforme os comandos abaixo.

- Geração da chave privada:

```
openssl genpkey -algorithm RSA -out exemplo.ifsertao-pe.edu.br.key -pkeyopt rsa_keygen_bits:2048
```

- Geração da requisição de certificado CSR:

```
openssl req -new -key exemplo.ifsertao-pe.edu.br.key -out exemplo.ifsertao-pe.edu.br.csr
```

O comando anterior requisitará as informações da Instituição para a Solicitação de Assinatura de Certificado. Os campos devem ser preenchidos conforme o servidor que receberá a certificação, no caso do exemplo abaixo, um servidor web identificado pelo domínio **exemplo.ifsertao-pe.edu.br** (campo Common Name):

```
Country name (2 letter code) [xx]: BRState or province name (full name) []: Pernambuco
Locality name (eg, City) [Default City]: CidadeOrganization Name (eg, company) [Default
Company Ltd]: IFSertaoPE
```

```
Organizational Unit Name (eg, section) [ ]: CampiCommon Name (eg your name or your server's
hostname) [ ]: exemplo.ifsertao-pe.edu.brEmail Address: [ ]: email.solicitante@ifsertao-
pe.edu.br
A challenge password [ ]:An optional company name [ ]:
```

Observar o seguinte no preenchimento dos campos anteriores:

- Os seguintes caracteres não são aceitos: < > ~ ! @ # \$ % ^ * / \ () ? . , &;
- O campo “Common Name” deve ser o nome completo (o domínio) do serviço cadastrado no DNS, ou seja, a exata URL onde o certificado vai ser utilizado;
- O campo “Organization Name” deve ser o nome oficial da Instituição, igual ao existente no cartão do CNPJ;
- Os campos “A challenge password” e “An optional company name” podem ficar em branco.

O arquivo .csr será gerado, sendo possível conferir os dados informados na requisição utilizando o comando:

```
openssl req -inform PEM -in exemplo.ifsertao-pe.edu.br.csr -text
```

É recomendado armazenar os arquivos **exemplo.ifsertao-pe.edu.br.key** e **exemplo.ifsertao-pe.edu.br.csr** em um local seguro, mantendo backup deles.

3. Envio a requisição de certificado para a Reitoria

O arquivo **exemplo.ifsertao-pe.edu.br.csr** gerado na sessão anterior deve ser enviado a Gerencia de Rede da Reitoria, informando o domínio do servidor e a funcionalidade dele. Para tanto, é necessário abrir um chamado na central de serviços do SUAP.

O arquivo **exemplo.ifsertao-pe.edu.br.key**, também gerado na sessão anterior, não deve ser enviado a Reitoria, devendo ser preservado em local seguro para posterior instalação nos servidores a serem protegidos.

A Reitoria então retornará o arquivo correspondente a certificação final. Dúvidas podem ser tratadas pelo e-mail redes@ifsertao-pe.edu.br.

4. Hierarquia da certificação e download dos arquivos do certificado digital

Como exemplo, para um certificado emitido pelo serviço de **AC SSL Corporativa da ICPEdu** para o domínio ***.rnp.br**, a estrutura da cadeia de certificação será:

[hierarquia_ICPEdu.jpg](#)

Neste caso o certificado do domínio ***.rnp.br** possui:

Image not found or type unknown

- Os certificados *ICPEdu* e *Trusted Root CA SHA256 G2* como **certificados intermediários**;
- O certificado *GlobalSign* como o **certificado raiz** da cadeia de certificação.

Com a certificação final recebida da Gerência de Redes da Reitoria, a cadeia de certificados pode ser instalada em definitivo no servidor a ser protegido. Para tanto, é necessário realizar o download dos arquivos da cadeia da certificação, como segue:

- Baixar os certificados Raiz e Intermediário (**gs_root.pem e intermediate.pem**) disponível no link [\[link para download\]](#).
- Baixar o arquivo enviado pela Gerência de Redes da Reitoria, correspondente ao certificado emitido através da AC SSL Corporativa da ICPEdu, salvando-o com o nome <seudomínio>.crt (seguindo o exemplo deste guia, **exemplo.ifsertao-pe.edu.br.crt**).

5. Exemplo da instalação da certificação no servidor web Apache

De posse dos 3 arquivos anteriores (**gs_root.pem**, **intermediate.pem** e **exemplo.ifsertao-pe.edu.br.crt**), e da Chave Privada gerada na sessão 2 deste guia (**exemplo.ifsertao-pe.edu.br.key**), a cadeia de certificados pode ser instalada em definitivo no servidor que fará uso da certificação. No exemplo deste guia, o servidor a ser protegido é um Servidor Web identificado pelo domínio **exemplo.ifsertao-pe.edu.br**.

A instalação compreende basicamente a cópia dos arquivos para uma pasta específica do servidor, fazendo-se necessário ainda realizar algumas configurações para que os arquivos da certificação sejam localizados pelo serviço web e para que ele possa fazer uso do protocolo SSL através do HTTPS.

Por padrão o diretório `/etc/ssl/` é utilizado para armazenar os certificados do servidor. Contudo, este exemplo usa a pasta **<pasta_do_apache>/ssl/icpedu/**, devendo-se copiar os arquivos anteriores para ela. O CentOS utiliza a pasta `/etc/httpd/` como diretório padrão do serviço Apache, enquanto o Debian utiliza `/etc/apache2/`. Para tanto, os comandos abaixo podem ser utilizados:

```
mkdir <pasta_do_apache>/ssl/icpedu/  
cd <pasta_onde_os_arquivos_foram_baixados>cp *.pem *.crt *key <pasta_do_apache>/ssl/icpedu/
```

Por padrão, os arquivos de configuração dos sites do Apache no CentOS ficam em `/etc/httpd/conf.d`. No Debian, ficam localizados em `/etc/apache2/sites-available/`. Este exemplo considera que a pasta padrão no CentOS foi alterada para seguir o padrão do Debian, como segue:

- Criação dos diretórios:

```
mkdir -p /etc/httpd/sites-availablemkdir -p /etc/httpd/sites-enabled
```

- Edição do arquivo `/etc/httpd/conf/httpd.conf` para que o Apache enxergue o diretório criado `/etc/httpd/sites-enabled`, inserindo a seguinte linha no final do arquivo:

```
IncludeOptional sites-enabled/*.conf
```

Este exemplo habilita o SSL para o site “Site Exemplo” presente no diretório `/var/www/html/siteexemplo/`, com seu arquivo de configuração definido no arquivo `<pasta_do_apache>/sites-available/siteexemplo.conf` e habilitado pelo link correspondente em `<pasta_do_apache>/sites-enabled/siteexemplo.conf`. Para tanto, os seguintes comandos podem ser utilizados:

```
mkdir /var/www/html/siteexemplo
touch /var/www/html/siteexemplo/index.htmltouch <pasta_do_apache>/sites-
available/siteexemplo.conf
ln -s <pasta_do_apache>/sites-available/siteexemplo.conf <pasta_do_apache>/sites-enabled/siteex
```

Para fazer uso dos certificados, o arquivo `<pasta_do_apache>/sites-available/siteexemplo.conf` deve ser editado como o exemplo abaixo:

```
<VirtualHost <server_name>:443>

    DocumentRoot "/var/www/html/siteexemplo"
    SSLEngine on
    ServerName <server_name>:443

    SSLCACertificateFile <pasta_do_apache>/ssl/icpedu/gs_root.pem SSLCertificateChainFile
<pasta_do_apache>/ssl/icpedu/intermediate.pem SSLCertificateFile
<pasta_do_apache>/ssl/icpedu/exemplo.ifsertao-pe.edu.br.crt SSLCertificateKeyFile
<pasta_do_apache>/ssl/icpedu/exemplo.ifsertao-pe.edu.br.key

    <Directory "/var/www/html/siteexemplo/">
        DirectoryIndex index.html
        Options FollowSymLinks
        AllowOverride All
        Require all granted
```

```
<Directory>
</VirtualHost>
```

Antes de testar o acesso, deve-se verificar se a porta HTTPS (443) está liberada no Firewall, caso o servidor faça uso de um. Pode ser necessário ainda habilitar o módulo SSL no servidor:

- No CentOS:

```
yum install mod_ssl
```

- No Debian:

```
a2enmod ssl
```

Para finalizar a instalação deve-se reiniciar os serviços com um dos comandos:

```
systemctl restart httpd
apache2ctl restartshutdown -r now
```

O acesso HTTPS pode ser testado em um navegador web com a url <https://exemplo.ifsertao-pe.edu.br/siteexemplo>. A página web “Site Exemplo” deve ser exibida, significando que a conexão está sendo encriptada e que o certificado foi reconhecido pelo navegador devido ao cadeado ao lado da url. A figura abaixo exemplifica o acesso ao site web do domínio *rnp.br protegido por seu certificado digital. [browser_https_rnp.jpg](#)

Instalação do certificado SSL

- Consultar no DNS qual a máquina responsável por redirecionar o serviço (VM própria ou *proxy*).

Na máquina do serviço a ter o certificado instalado:

- Acessar a pasta `/etc/nginx` e conferir no diretório `conf.d` os arquivos de configuração `serviço.conf` e onde estão localizados os certificados (geralmente `/etc/ssl/icpedu`);
- Acessar o diretório dos certificados e mover os agora expirados para uma pasta de "*antigos*":

```
sudo mv serviço.ifsertao* antigos/
```

- Criar arquivos *CSR*, *KEY*, *CRT* para cada nome de domínio (ex.: ifsertao-pe e ifsertaope):
 - CSR e KEY:
 - utilizar script `./gerar_csr.sh` para criar a requisição (`.csr`) e a chave (`.key`);
 - CRT:
 - emitir certificado no site da Global Sign e criar arquivo `serviço.crt` contendo o conteúdo do certificado.

NGINX:

- Criar arquivo `serviço.pem` concatenando três arquivos (para cada nome de domínio):
 - `serviço.crt`
 - root (`gs_root.pem`)
 - `intermediate.pem`

```
cat serviço.crt intermediate.pem gs_root.pem > serviço.pem  
caso retorne "Permissão negada":  
sudo bash -c "cat serviço.crt intermediate.pem gs_root.pem > serviço.pem"
```

- Testar arquivos de configuração em uso pelo NGINX:

```
nginx -t
```

- Reiniciar serviço do NGINX e verificar status:

```
systemctl restart nginx
```

```
systemctl status nginx
```

APACHE

- O apache utiliza de forma separada dois arquivos criados no processo (a chave .key e o certificado .crt).
- Testar arquivos de configuração em uso pelo Apache:

```
apachectl configtest
```

- Reiniciar serviço do Apache e verificar status:

```
systemctl restart httpd (apache)
```

```
systemctl status httpd (apache)
```

- Acessar página do serviço pelo navegador e verificar a validade do certificado.