

Criação de certificado .p12 sem o uso do Mac

O certificado .p12 é necessário para configurar tasks no pipeline, portanto foi buscada uma maneira de criá-lo sem a necessidade de se utilizar um Mac. Nessa documentação abordarei o passo à passo de como realizar este procedimento.

O Que será necessário?

- Uma máquina com o sistema operacional Windows.
- O Microsoft Visual C++ 2008 Redistributable Package, que pode ser obtido pelo link:
<https://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=29>
- O Openssl versão light, que pode ser obtido pelo link:
<http://slproweb.com/products/Win32OpenSSL.html>

***Obs:** O Openssl deve ser da mesma arquitetura da máquina, ou seja caso sua máquina tenha a arquitetura 64bits, deve ser instalado o Openssl Light 64bits, caso a máquina seja de 32 bits deve-se escolher o Openssl de maneira análoga.

Passos após as instalações

Primeiramente navegue até o diretório onde o openssl foi instalado, caso tenha deixado o caminho padrão ele irá estar na pasta "Program Files" para arquiteturas de 64 bits, e na pasta "Program Files (x86)" em arquiteturas de 32 bits.

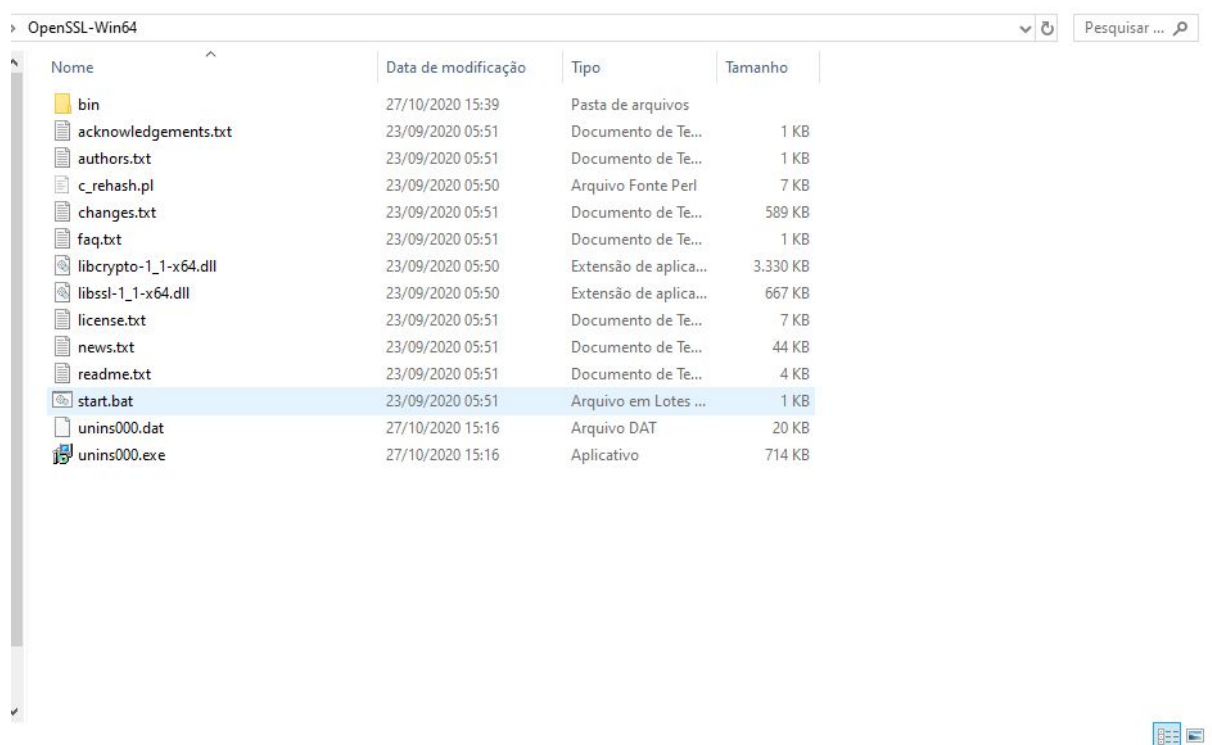


Figura 1 - Diretório do Openssl

Em seguida acesse a pasta bin, e digite no campo de pesquisa “cmd” e dê um enter.

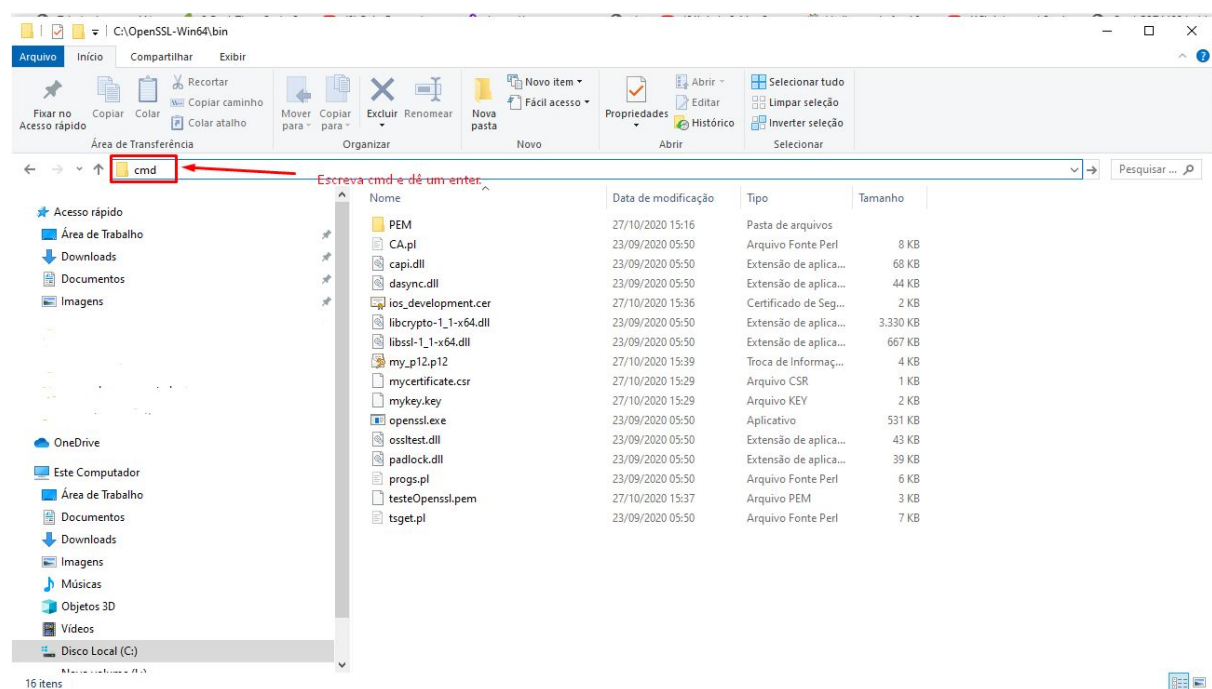


Figura 2 - Abrir o prompt já na pasta bin

isso fará com que o prompt de comando seja com o caminho da pasta.

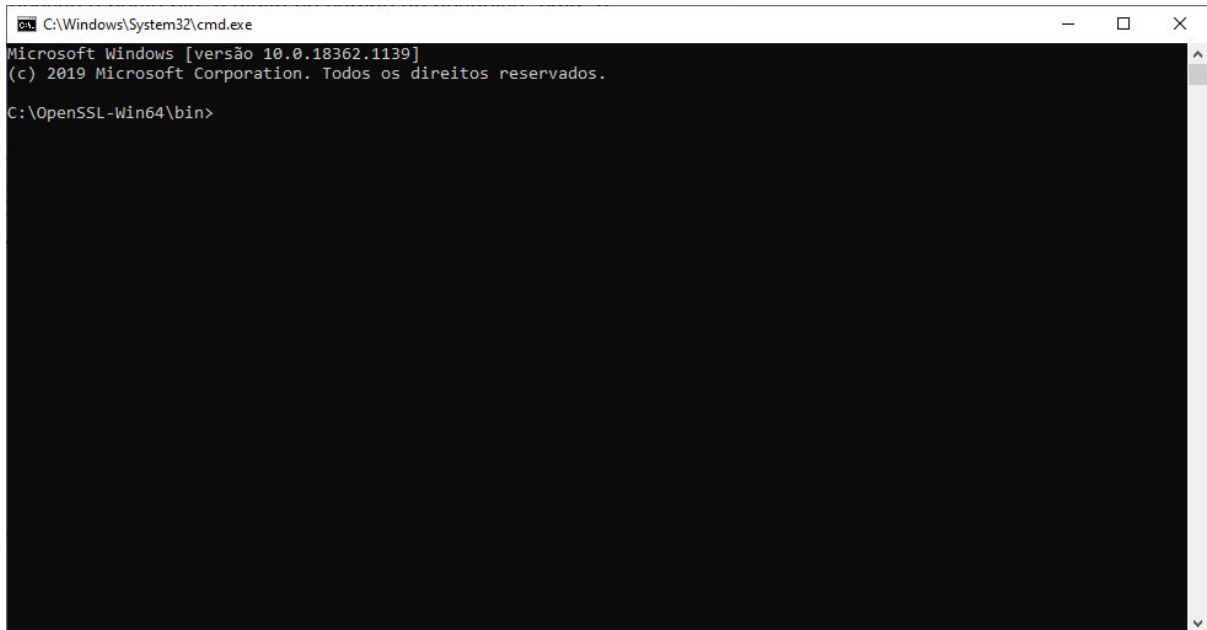


Figura 3 - Prompt aberto a partir da pasta

Agora para ter acesso a command line do openssl basta digitar openssl no prompt e dar um enter.

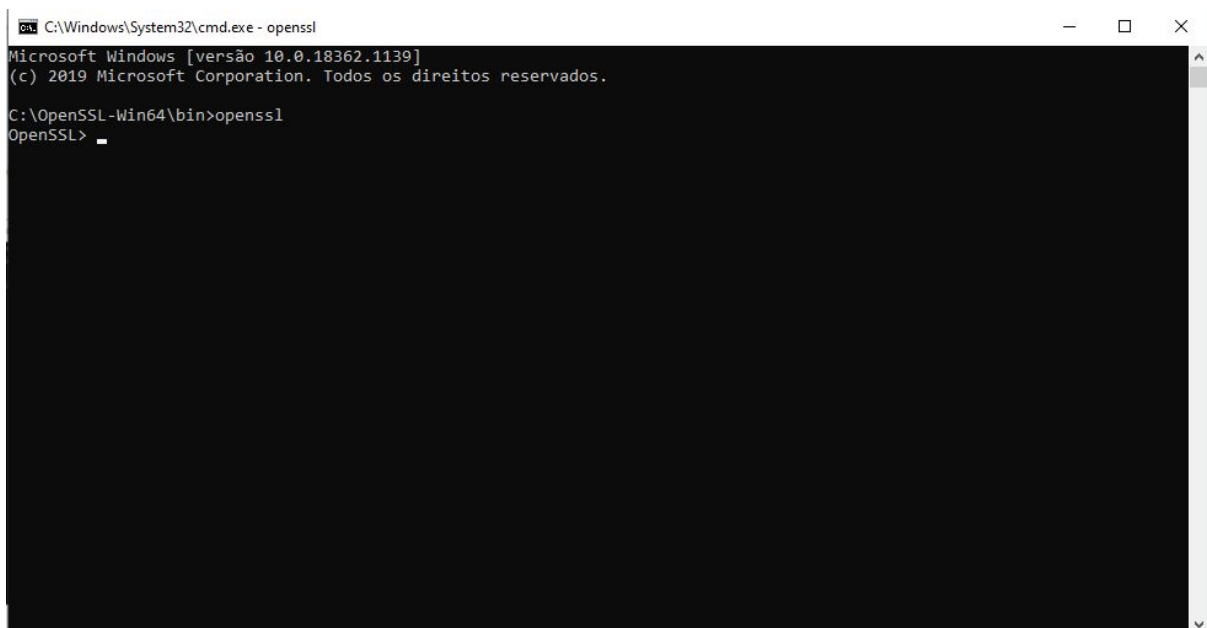
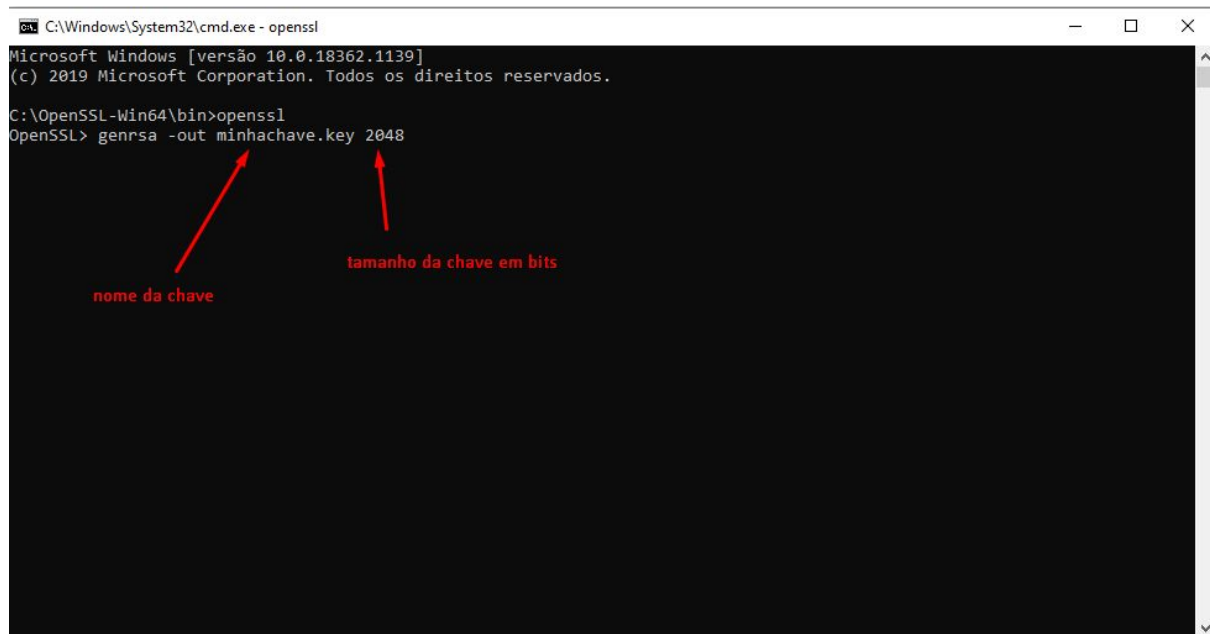


Figura 4 - Acionando o Openssl

Agora que temos acesso ao Openssl podemos gerar nossa chave. Para isso digite o comando: *genrsa -out minhachave.key 2048*

Onde 2048 representa o tamanho da chave em bits, *genrsa* representa o tipo de criptografia em que a chave será gerada, e *minhachave.key* representa o nome do arquivo que será gerado.



```
C:\Windows\System32\cmd.exe - openssl
Microsoft Windows [versão 10.0.18362.1139]
(c) 2019 Microsoft Corporation. Todos os direitos reservados.

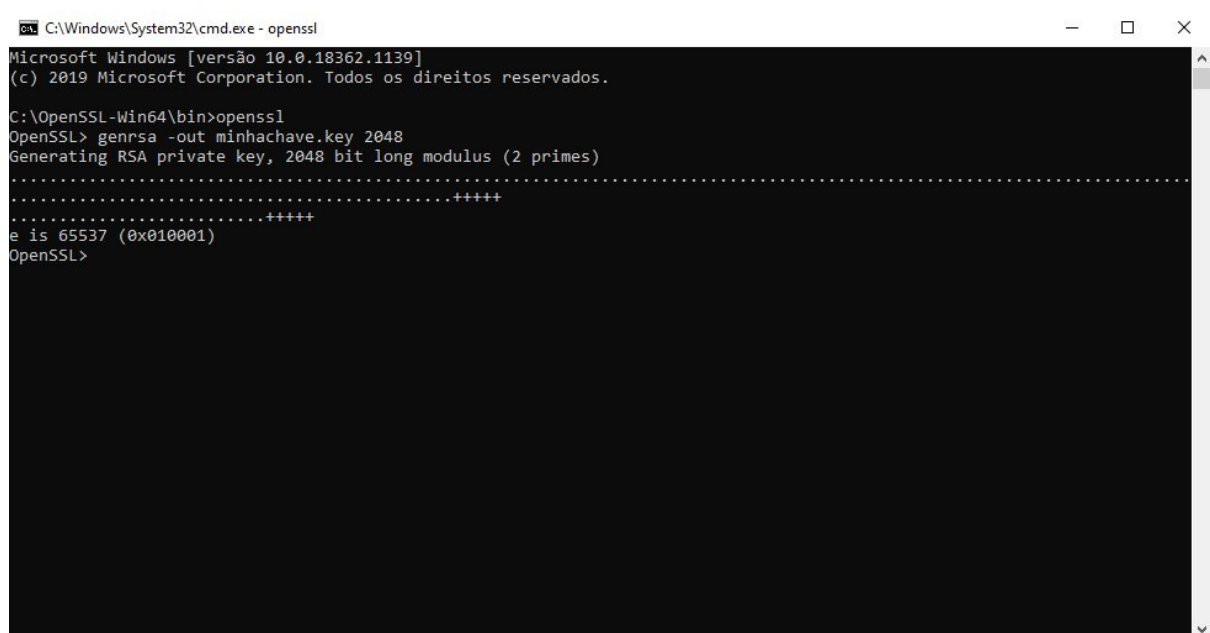
C:\OpenSSL-Win64\bin>openssl
OpenSSL> genrsa -out minhachave.key 2048
```

nome da chave

tamanho da chave em bits

Figura 5 - Gerando chave com criptografia RSA.

O resultado do comando deve ser semelhante ao mostrado na figura abaixo:



```
C:\Windows\System32\cmd.exe - openssl
Microsoft Windows [versão 10.0.18362.1139]
(c) 2019 Microsoft Corporation. Todos os direitos reservados.

C:\OpenSSL-Win64\bin>openssl
OpenSSL> genrsa -out minhachave.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
OpenSSL>
```

Figura 5 - Exemplo de saída após execução do comando de gerar chave.

A chave irá ser criada no diretório do openssl dentro da pasta bin.

Em seguida iremos realizar o comando:

```
req -new -key minhachave.key -out meucertificado.csr -subj  
"/emailAddress=seu@email.com, CN=SEU NOME, C=BR" -config  
"C:\ProgramFiles\CommonFiles\SSL\openssl.cnf"
```

Os campos destacados acima devem ser substituídos como desejar, mas o campo “minha chave” em especial deve conter o nome da chave criada no passo anterior.

Após executar o comando será criado um certificado com o nome [meucertificado].csr na pasta bin.

***Obs:** Note que o caminho utilizado:

C:\Program Files\Common Files\SSL\openssl.cnf

Equivale ao caminho do arquivo para uma máquina de arquitetura 64bits, caso sua arquitetura seja de 32 bits você deve ir na pasta “Common Files” do “Program Files(x86)”.

Após gerar o certificado devemos realizar o upload do mesmo no site da apple, então dirija-se ao site de desenvolvedores e configura para gerar um novo certificado, quando for pedido para fazer o upload do .csr basta selecionar o certificado gerado no passo anterior, e prosseguir.

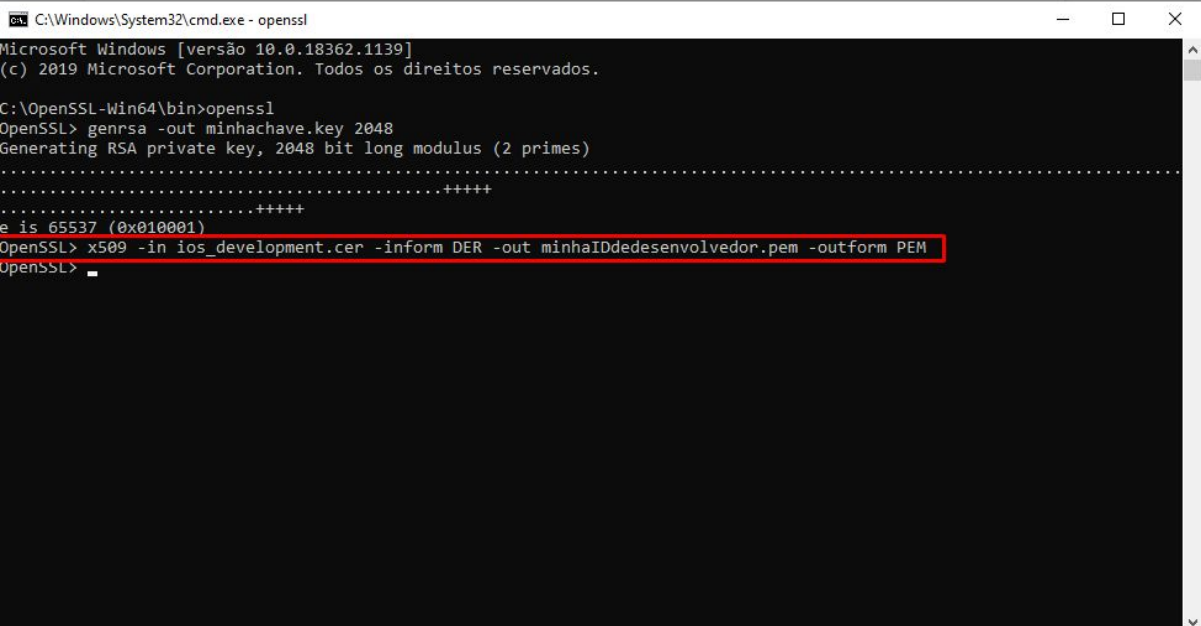
Quando a criação do certificado for finalizada no site da apple, ele te dará a opção de realizar o download do mesmo, baixe-o e o mova para a pasta *bin* do diretório do *openssl*.

Gerando a chave .p12

Com o certificado já baixado do site da apple agora devemos primeiramente gerar uma chave publica a partir dele, utilizando o comando:

```
x509 -in ios_development.cer -inform DER -out developer_identity.pem  
-outform PEM
```

Onde *ios_development.cer* é o nome do arquivo baixado do site da apple, e *developer_identity.pem* é o nome do arquivo que será gerado.



```
C:\Windows\System32\cmd.exe - openssl
Microsoft Windows [versão 10.0.18362.1139]
(c) 2019 Microsoft Corporation. Todos os direitos reservados.

C:\OpenSSL-Win64\bin>openssl
OpenSSL> genrsa -out minhachave.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
OpenSSL> x509 -in ios_development.cer -inform DER -out minhaIDdesenvolvedor.pem -outform PEM
OpenSSL>
```

Figura 6 - comando para gerar o .PEM

Com o .PEM criado na pasta bin, agora devemos exportá-lo para uma chave .P12, para isso basta executarmos o comando:

```
pkcs12 -export -inkey minhachave.key -in developer_identity.pem -out  
my_p12.p12
```

Onde *minhachave.key* é o nome da chave criada no início da documentação, *developer_identity.pem* é o arquivo criado no passo anterior, e *my_p12.p12* é o nome que você deseja para sua chave *.p12*.

Ao executar o comando, basta escolher a senha para a chave, e confirma-la então o arquivo será criado na pasta bin, como visto na imagem abaixo.

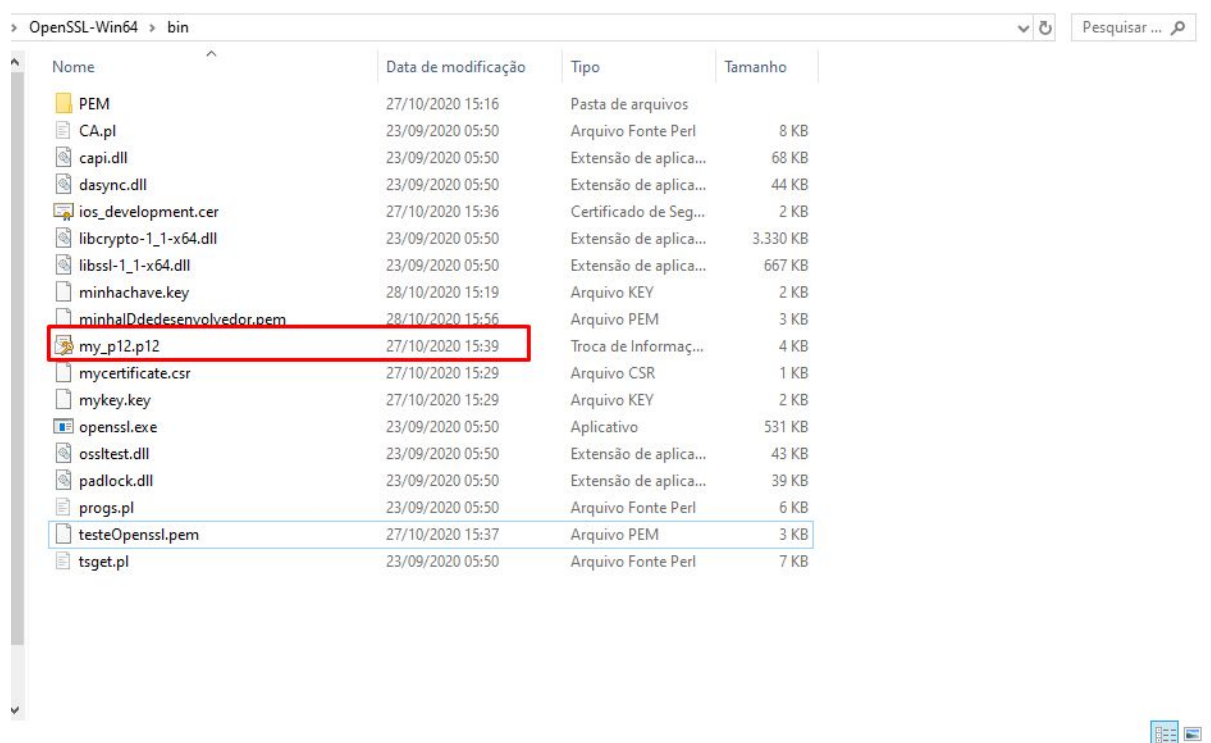


Figura 7 - chave .p12 gerada na pasta bin do diretório do openssl