

SUORTE API
suorte.api@bradesco.com.br

EXTRAÇÃO CERTIFICADO PÚBLICO

2021

SUMÁRIO

1. ARQUIVOS .PFX, .P12 (PKCS#12).....	3
a. openssl.....	3
b. Sistema operacional.....	4
i. Windows.....	4
ii. macOS.....	7

Caso encontre dúvidas na execução dos passos, entrar em contato com suporte.api@bradesco.com.br

1. ARQUIVOS .PFX, .P12 (PKCS#12)

Os arquivos “.pfx” ou “.p12” são relacionados de maneira abrangente à arquivos que possuem o acesso à chave privada e pública de um certificado digital.

Para utilização das APIs somente se faz necessário o compartilhamento da chave pública, ao qual será transformada em um certificado X.509 para conceder permissão de acesso aos sistemas consumidores.

a. openssl

Executar o comando abaixo, substituindo os valores destacados conforme necessidade.

Quadro 01 PKCS#12, extração certificado X.509

Comando:

```
openssl pkcs12 -in [arquivo-keystore] -clcerts -nokeys -out [razaosocial].[cnpj].pem -password pass:[senha]
```

Exemplo (input = keyStore.pfx; output = parceiro.68423401000198.pem; senha = minhasenha)

```
openssl pkcs12 -in keyStore.pfx -clcerts -nokeys -out parceiro.68423401000198.pem -password pass:minhasenha
```

Ao abrir o arquivo como texto ele deve estar no seguinte formato.

Quadro 02 – X.509 base64 (.pem)

Exemplo: parceiro.68423401000198.pem

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE-----
```

b. Sistema operacional

Para extração via interface do próprio OS é necessário a instalação prévia no computador.

i. Windows

1. Apertar **Windows** + R, irá abrir o “Executar”;
2. Digitar “certmgr.msc” e confirmar. Será aberto o gerenciador de certificados;

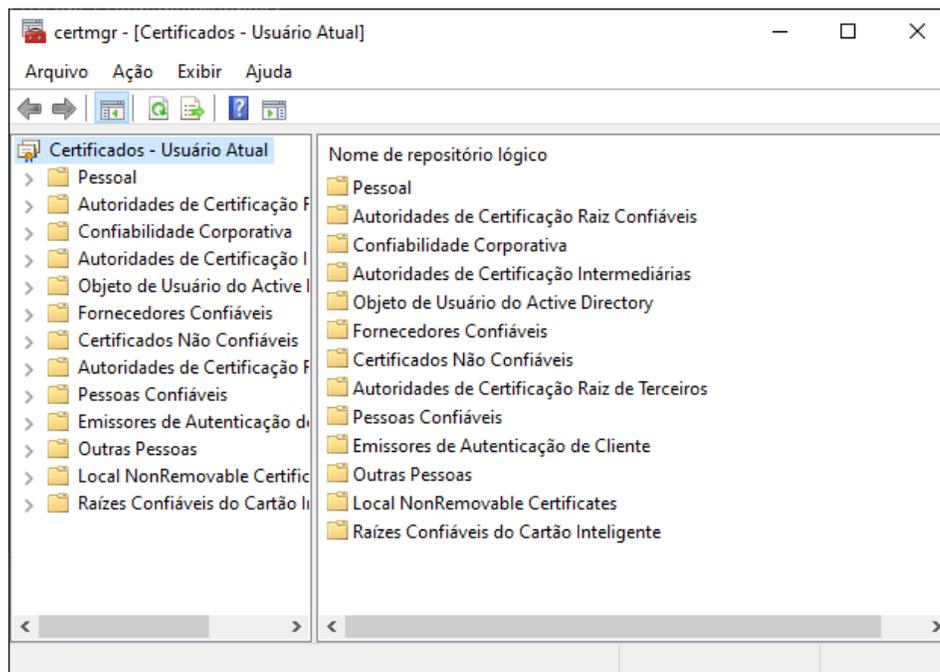


Figura 01. Gerenciador de certificados Windows

3. Selecionar a pasta “Pessoal” -> “Certificados”;
4. Irá aparecer a lista completa de certificados instalados na máquina;
5. Após selecionado com dois cliques, seguir com a exportação abaixo.
 - i. Abrir o certificado com o visualizador do Windows;

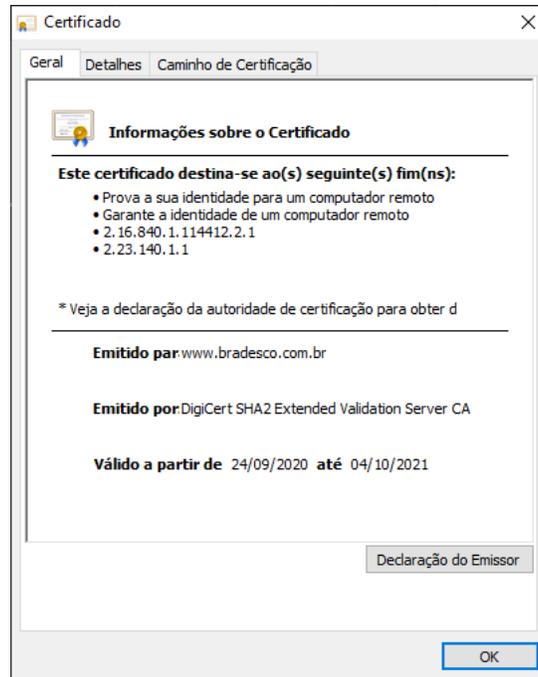


Figura 02. Visualizador de certificados Windows

- ii. Ir na aba “Detalhes” e no canto inferior direito clicar em “Copiar para Arquivo...”;

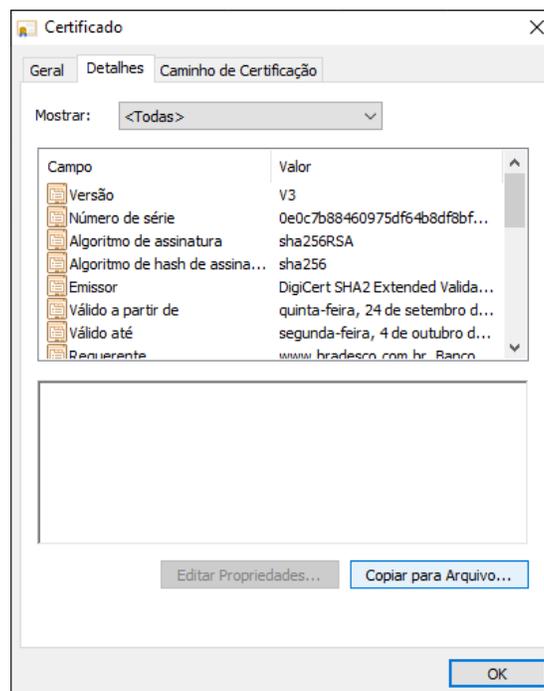


Figura 03. Visualizador detalhes certificado

- iii. Clicar em “Avançar”, selecionar “X.509 codificado na base 64 (*.cer)”;

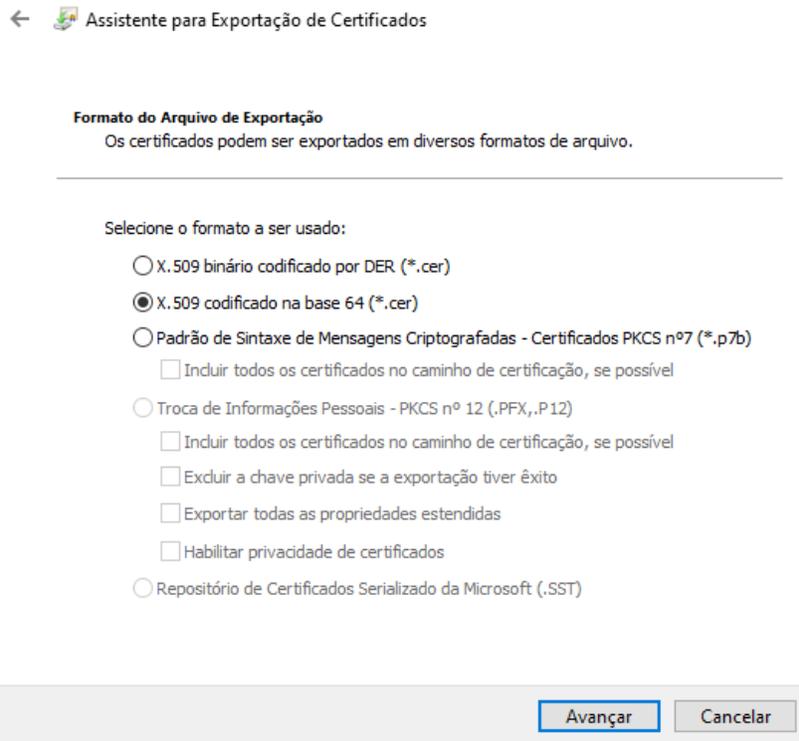


Figura 04. Exportar para X.509 base64

- iv. Clicar em “Avançar”, e depois em “Procurar” e exportar o arquivo com o nome abaixo.

<nomeParceiro>.<CNPJ>.pem

O próprio assistente irá criar o arquivo no diretório e nome escolhido. Recomenda-se a remoção da extensão “.cer” que o Windows insere por padrão, deixando somente como “.pem”.

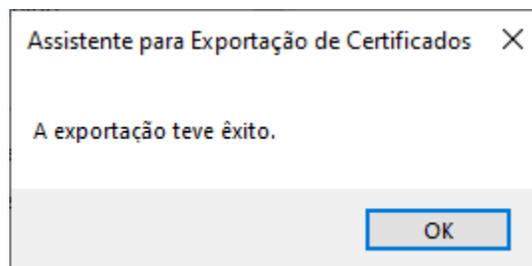


Figura 05. Finalização exportação

ii. macOS

1. No app Acesso às Chaves  do Mac, selecione os itens que deseja exportar na janela do Acesso às Chaves.
2. Escolha Arquivo > Exportar Itens.
Selecione a opção “Certificado (*.cer)” em “Formato de Arquivo”.
3. Selecione um local para salvar o certificado público.
4. Clique em Salvar.