

BANCO DO BRASIL S.A.

INTERNALIZAÇÃO DE CERTIFICADOS

PORTAL DEVELOPERS

DITEC/UOS/GESEC – APIS E PARCERIAS

O que são Certificados?

- Os **certificados digitais** são documentos eletrônicos que atestam a identidade de uma pessoa, empresa ou sistema. Eles são usados para garantir a autenticidade, integridade e confidencialidade das informações transmitidas pela internet.
- No contexto bancário, os certificados são essenciais para proteger transações financeiras, assinar contratos eletronicamente e garantir a segurança das operações.

1. Certificados para as APIs do Banco do Brasil

Em APIs, os certificados desempenham um papel crucial na segurança e na confiança entre sistemas. Vamos entender o que são os certificados da empresa, intermediários e raiz:

1.1. Certificados da Empresa:

- Também conhecidos como certificados de servidor, esses são emitidos especificamente para o domínio ou servidor de uma empresa.
- São usados para autenticar a identidade do servidor e criptografar a comunicação entre o cliente (por exemplo, navegador) e o servidor.
- Quando um cliente se conecta a um servidor, verifica se o certificado do servidor pertence ao domínio correto e se foi assinado por uma autoridade confiável.

1.2. Certificados Intermediários:

- São parte de uma cadeia de confiança que conecta o certificado do servidor (da empresa) ao certificado raiz.
- Os certificados intermediários são emitidos por uma autoridade de certificação (CA) e são usados para assinar os certificados do servidor.
- Eles garantem que os certificados do servidor sejam confiáveis e reconhecidos pelos navegadores e aplicativos.

1.3. Certificados Raiz:

- São os certificados de nível mais alto na hierarquia.
- Emitidos pelas autoridades de certificação raiz, como a GlobalSign, esses certificados são pré-instalados nos navegadores, aplicativos e dispositivos.
- Os certificados raiz não são usados diretamente para assinar certificados de servidor. Em vez disso, eles assinam os certificados intermediários.
- A cadeia de confiança é estabelecida quando o certificado do servidor é assinado pelo certificado intermediário, que, por sua vez, é assinado pelo certificado raiz.

Em resumo, os certificados da empresa são específicos para um domínio ou servidor, os certificados intermediários fazem a ponte entre os servidores e os certificados raiz são os pilares da confiança na infraestrutura de segurança. Essa estrutura garante a autenticidade e a criptografia segura nas comunicações via API.

Um **Certificado Digital A1** é um tipo de Certificado Digital usado para autenticação, assinatura e criptografia de informações eletrônicas. Ele é emitido por uma Autoridade

Certificadora (AC) e contém informações como nome, chave pública e número de série do Certificado.

Aqui estão alguns detalhes importantes sobre o Certificado Digital A1:

- Armazenamento: O Certificado A1 é um arquivo que fica armazenado no disco rígido do computador do usuário.
- Validade: Geralmente, ele tem validade de 1 ano.
- Utilização:
 - Serve para garantir a autenticidade e a segurança das transações digitais.
 - Pode ser usado para assinar documentos eletrônicos, realizar declarações e acessar sistemas como o portal da Receita Federal(e-CAC).
- Emissão e Instalação:
 - A Certisign, uma das maiores lojas de certificados digitais no Brasil, oferece orientações detalhadas sobre a emissão e instalação de Certificados A1.
 - O Certificado A1 é emitido e armazenado diretamente no computador do titular.

Portanto, o Certificado Digital A1 é uma ferramenta essencial para a segurança e a confiabilidade das operações online, permitindo que empresas e indivíduos realizem transações de forma protegida e autenticada.

Autenticação Mútua de Certificados

Para o consumo de algumas APIs do BB como as API PIX e API Pagamento em Lote é necessária a troca de certificados para Autenticação mTLS (*Mutual TLS authentication*).

É um tipo de autenticação que ambos, cliente e servidor, apresentam certificados digitais para serem validados pelo par. Ou seja, no caso da API de Pagamentos, para conseguir efetuar um *request* (seja ele de envio de remessa, consulta, cancelamento, etc.) ele deverá apresentar o seu certificado, que será validado pelo BB. Da mesma forma, o BB disponibilizará o seu certificado, que será validado pelo cliente. Em caso de confirmação de ambos, a autenticação será efetuada.

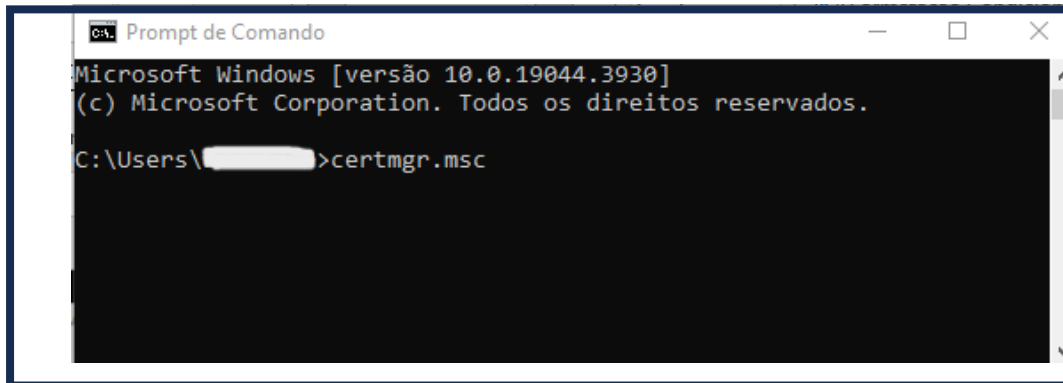
Os certificados autorizados pelo BB para a autenticação mútua são do tipo A1, em formato **.pem**, com a cadeia inteira (**Certificado > Intermediarias > Raiz**), emitidos por uma CA válida (exemplos: Digicert, Verisign, ICP Brasil).

2. Passo a passo para envio de certificado no **Portal Developers - Windows**

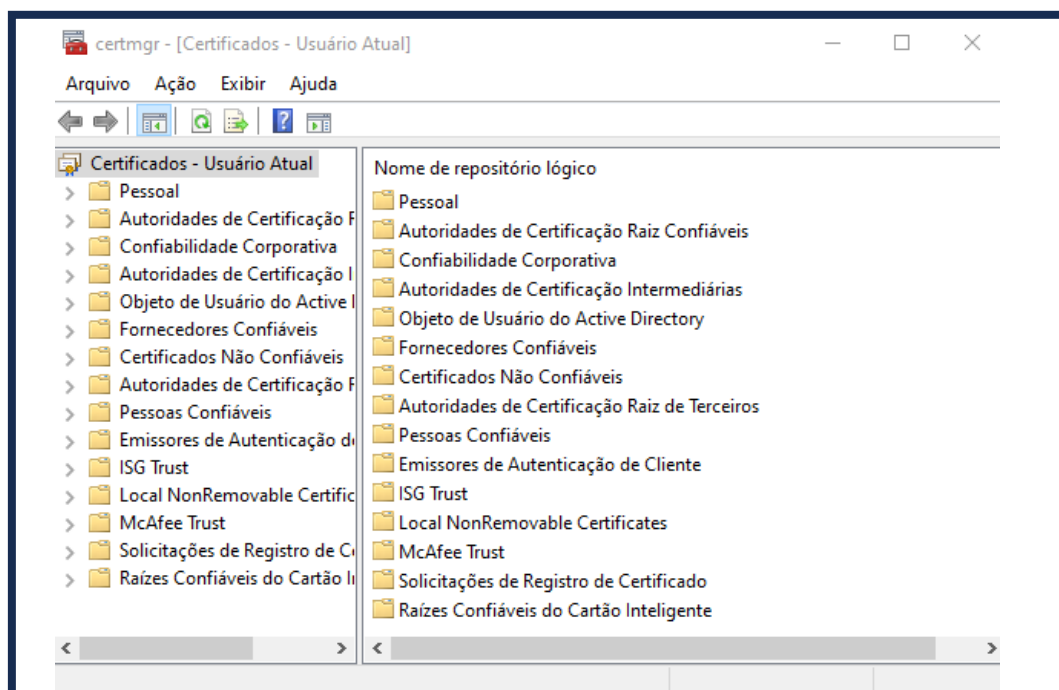
Caso já possua o certificado instalado em sua máquina, gentileza seguir o passo a passo indicado abaixo

Roteiro para exportação de chave pública:

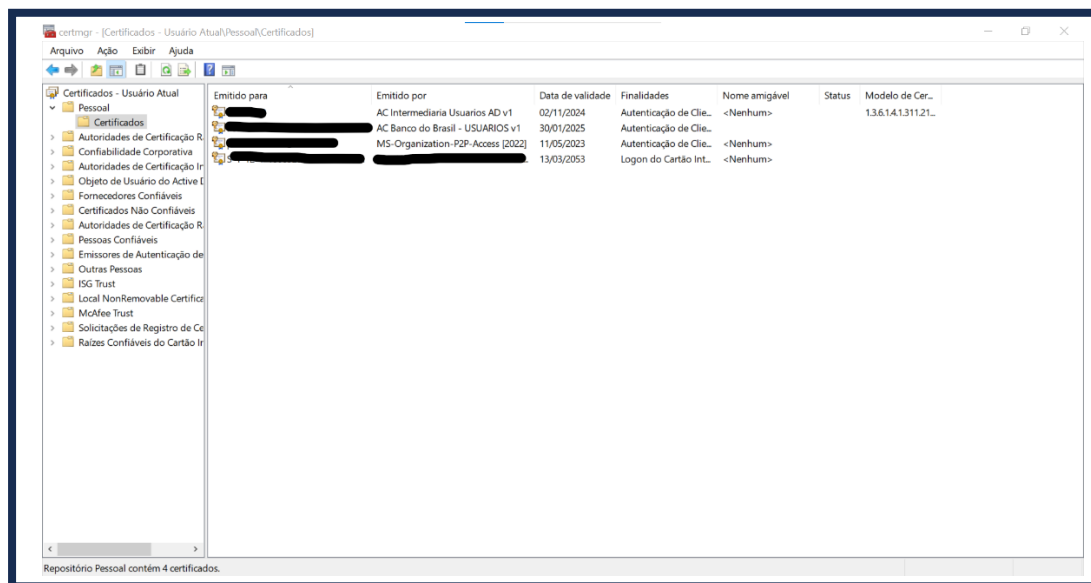
- a. No prompt do Windows digite: **certmgr.msc**



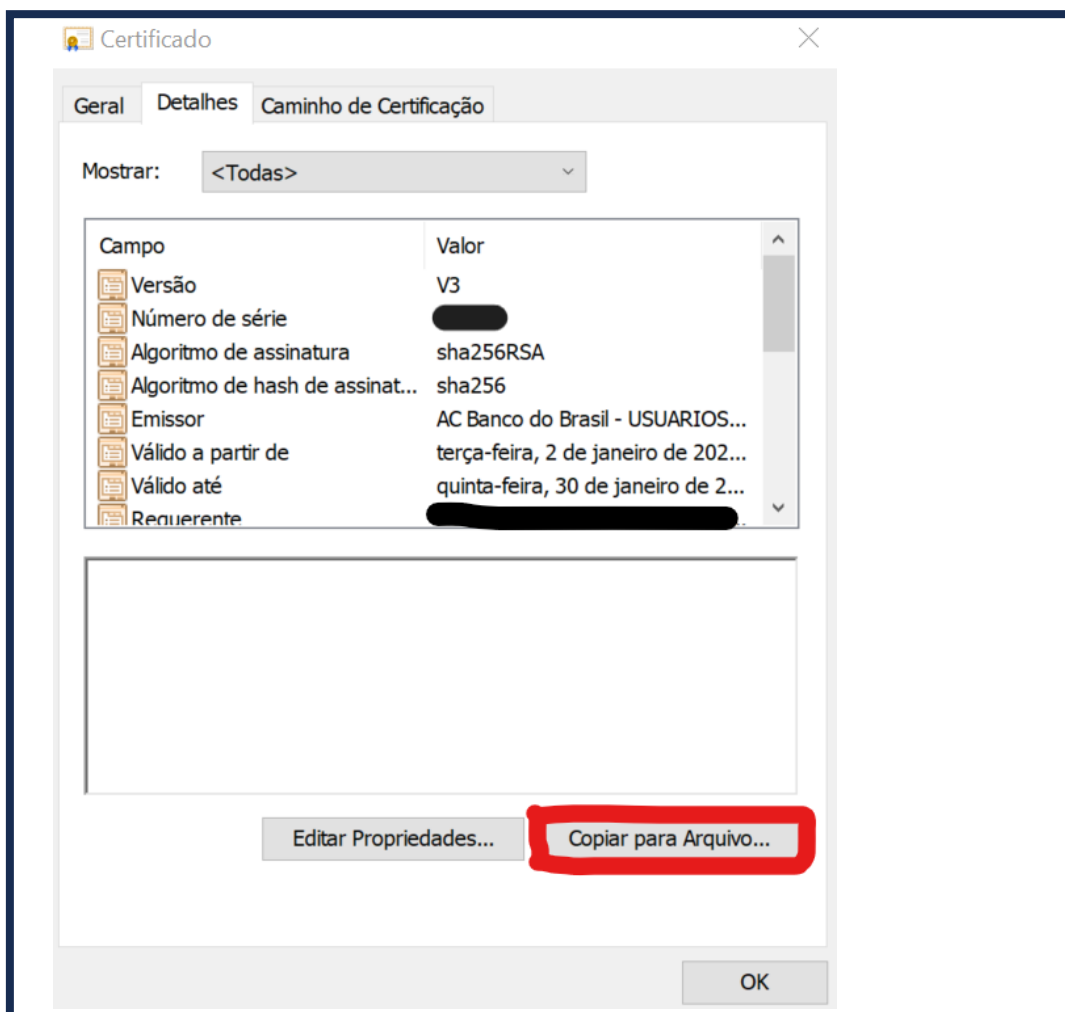
b. Será exibida a tela



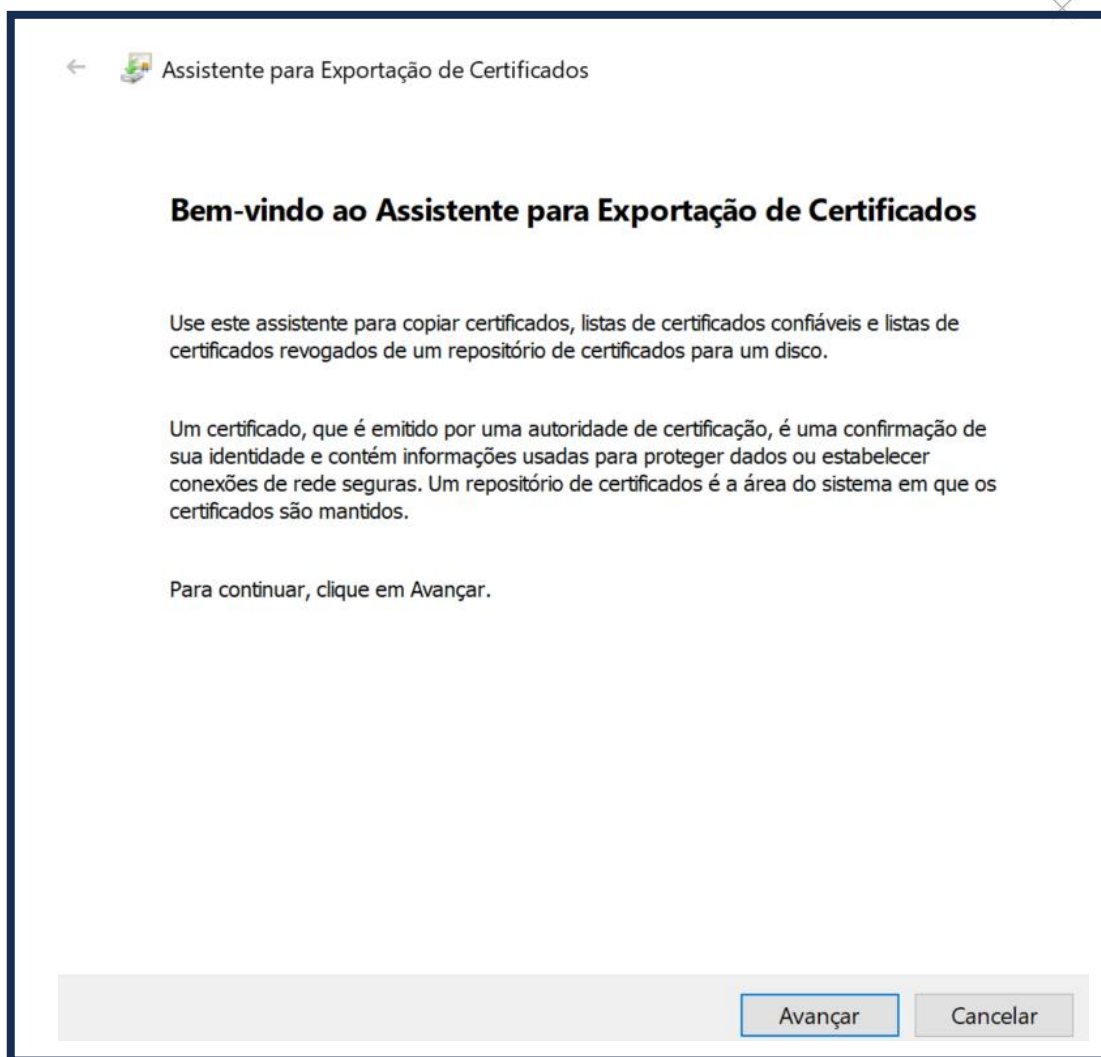
c. Clique na pasta **Pessoal** e, em seguida, na pasta **Certificados**

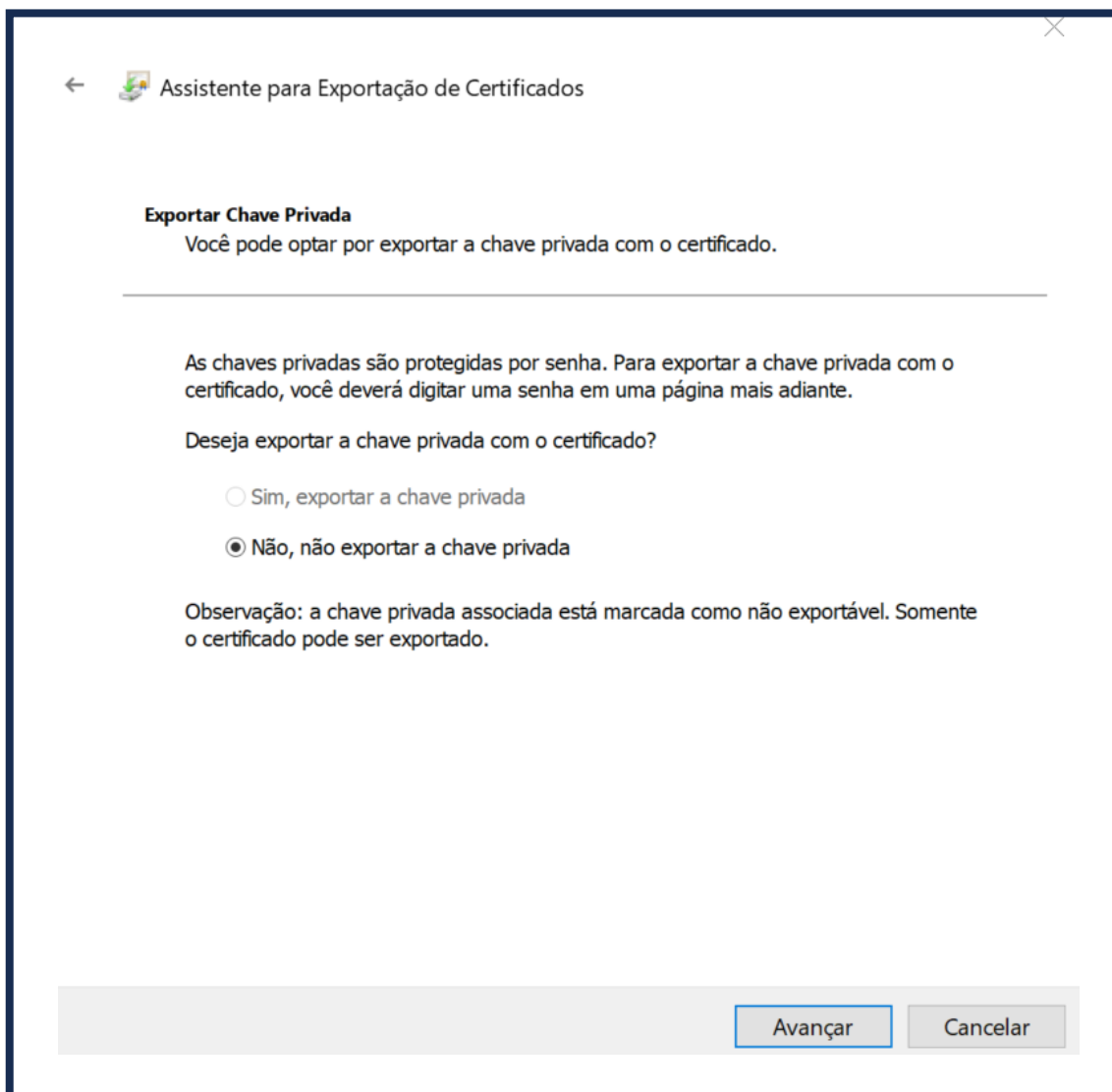


d. Clique com o botão esquerdo duas vezes sobre o certificado que deseja exportar e, na aba "Detalhes", selecione **Copiar para Arquivo ...**

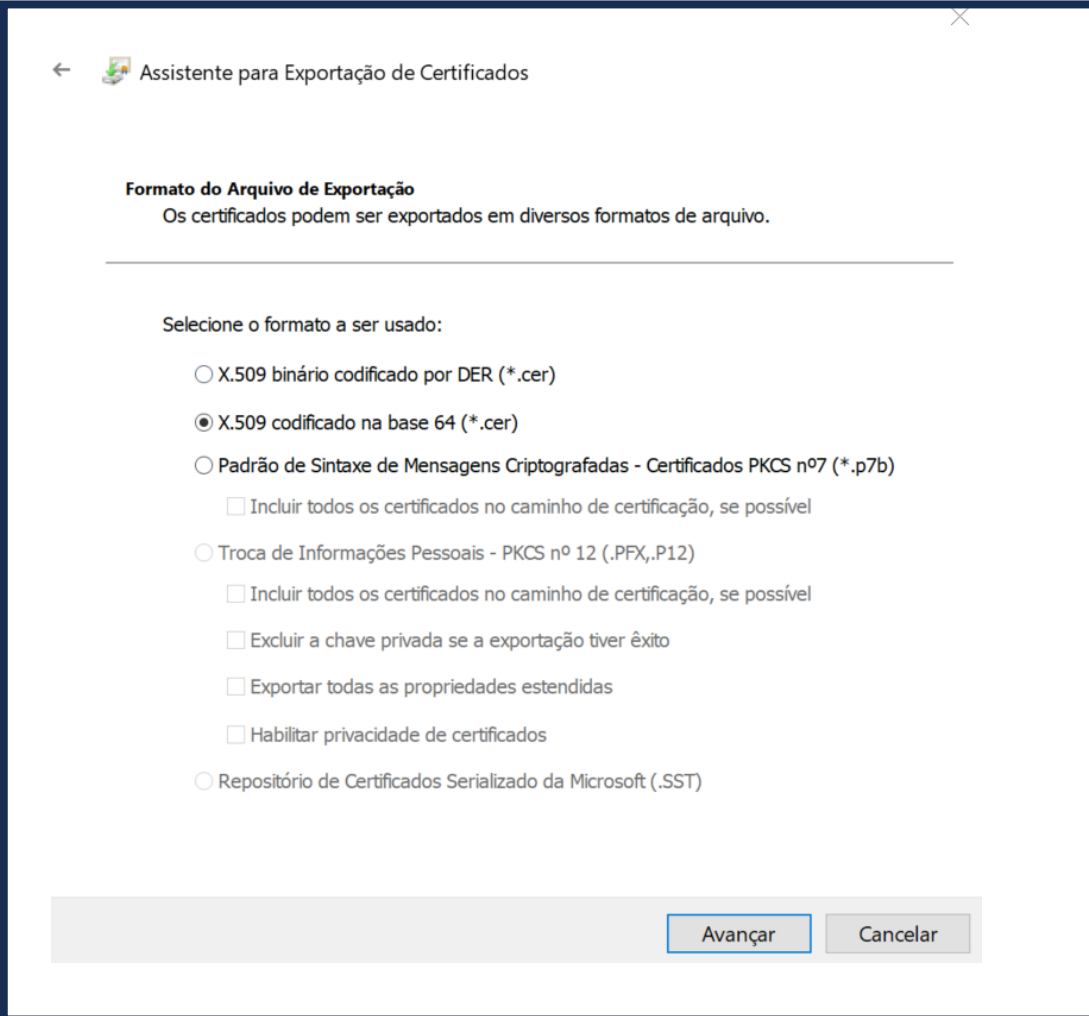



e. Clique em **Avançar** e, em seguida, novamente **Avançar**. Na tela a seguir mantenha a opção "**Não, não exportar a chave privada**".





f. Clique em **Avançar** e marque a **opção X.509 codificado no base 64 (*.cer)**



←  Assistente para Exportação de Certificados

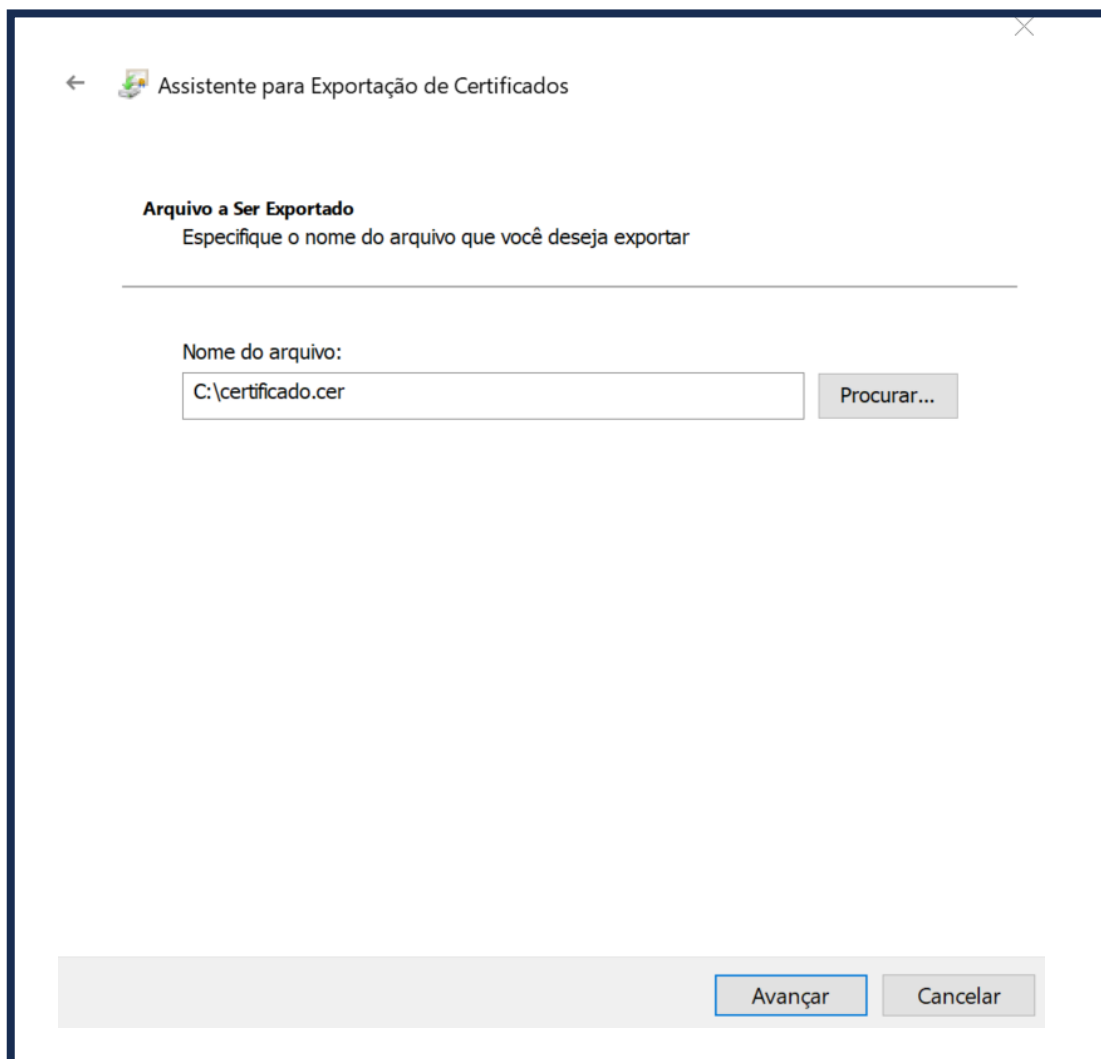
Formato do Arquivo de Exportação
Os certificados podem ser exportados em diversos formatos de arquivo.


Selecione o formato a ser usado:

- ☐ X.509 binário codificado por DER (*.cer)
- ☒ X.509 codificado na base 64 (*.cer)
- ☐ Padrão de Sintaxe de Mensagens Criptografadas - Certificados PKCS nº7 (*.p7b)
 - ☐ Incluir todos os certificados no caminho de certificação, se possível
- ☐ Troca de Informações Pessoais - PKCS nº 12 (.PFX,.P12)
 - ☐ Incluir todos os certificados no caminho de certificação, se possível
 - ☐ Excluir a chave privada se a exportação tiver êxito
 - ☐ Exportar todas as propriedades estendidas
 - ☐ Habilitar privacidade de certificados
- ☐ Repositório de Certificados Serializado da Microsoft (.SST)

Avançar Cancelar

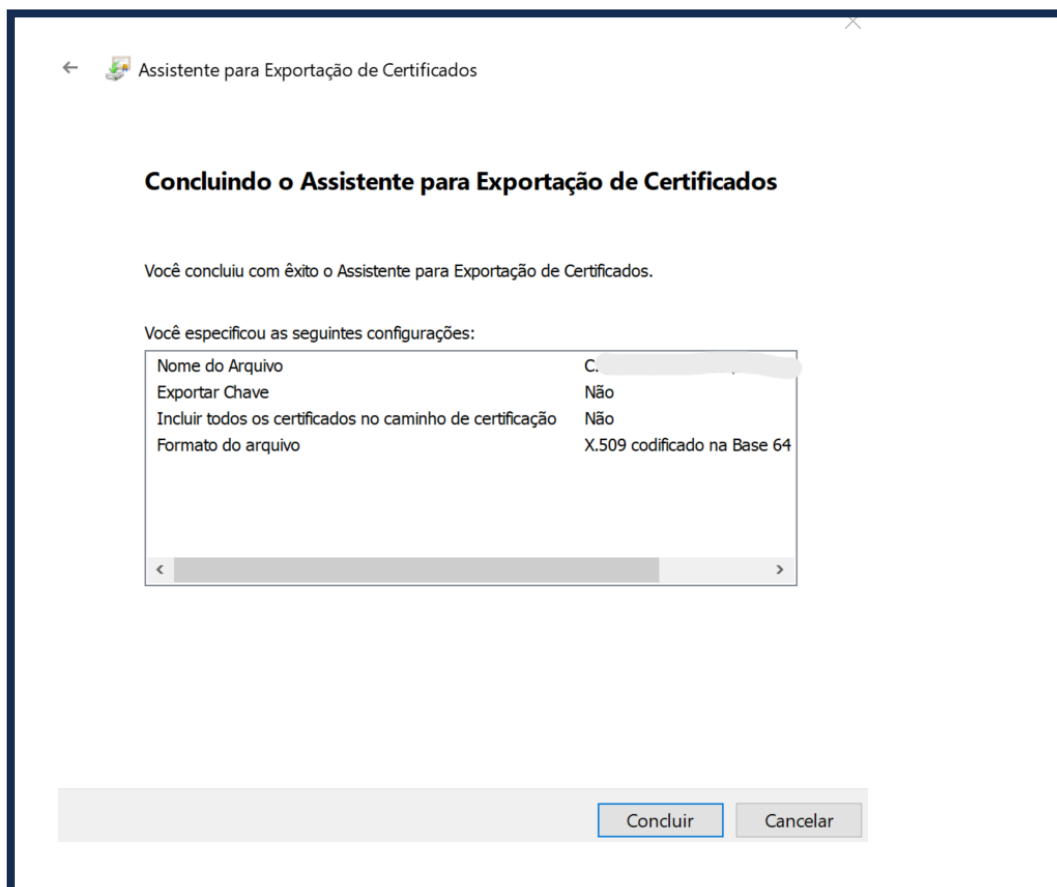
g. A seguir aparecerá uma tela para você escolher o local e o nome do arquivo .CER a ser exportado



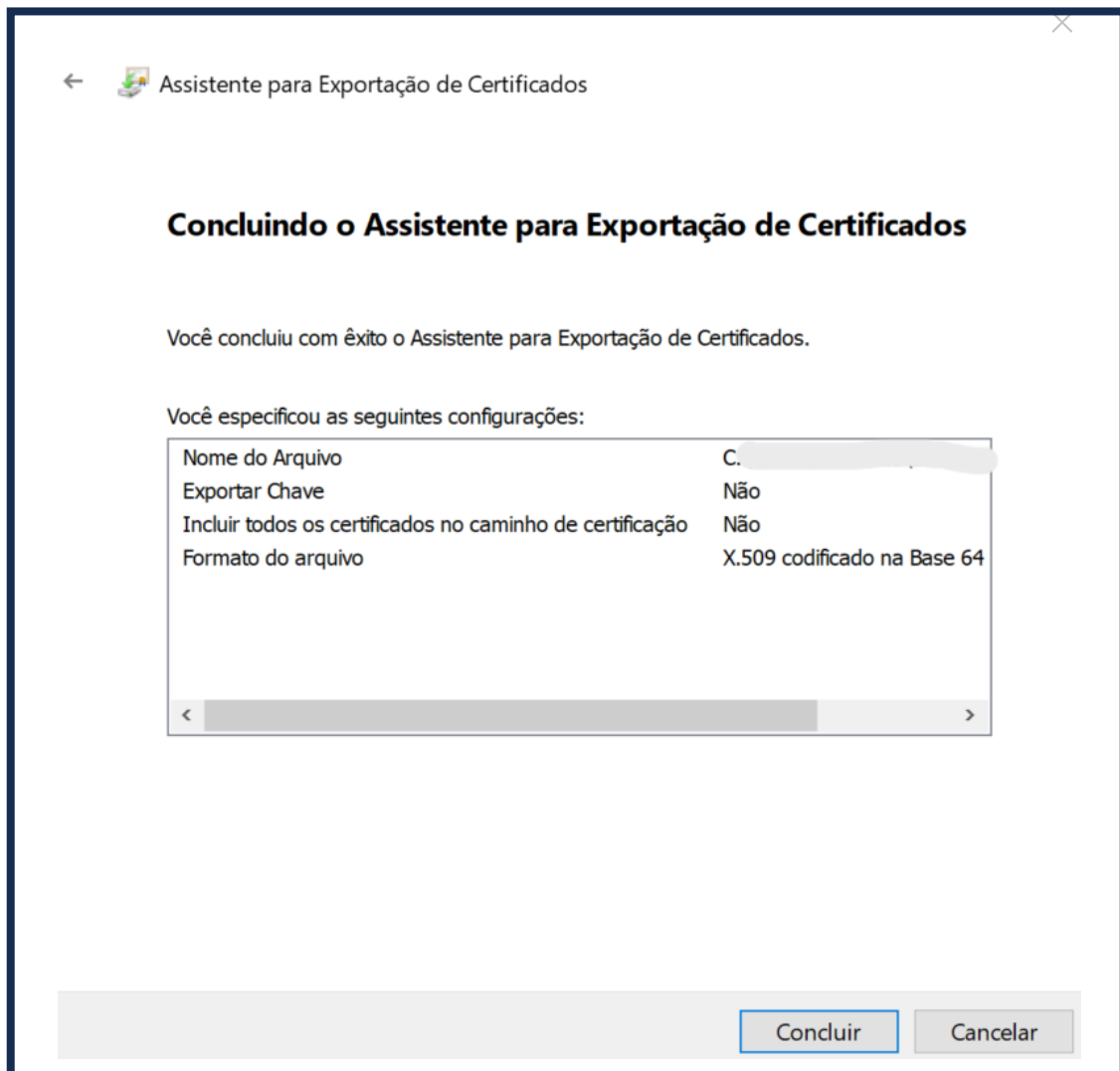
←  Assistente para Exportação de Certificados

Arquivo a Ser Exportado
Especifique o nome do arquivo que você deseja exportar

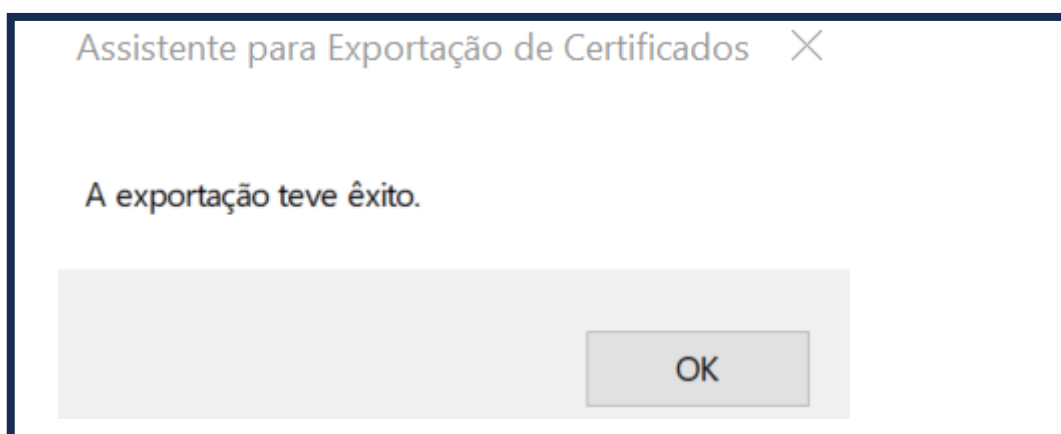
Nome do arquivo:



h. Clique em **Salvar** e, em seguida, clique em **Avançar**. Irá aparecer a tela a seguir



i. Clique em **Concluir** para finalizar o procedimento

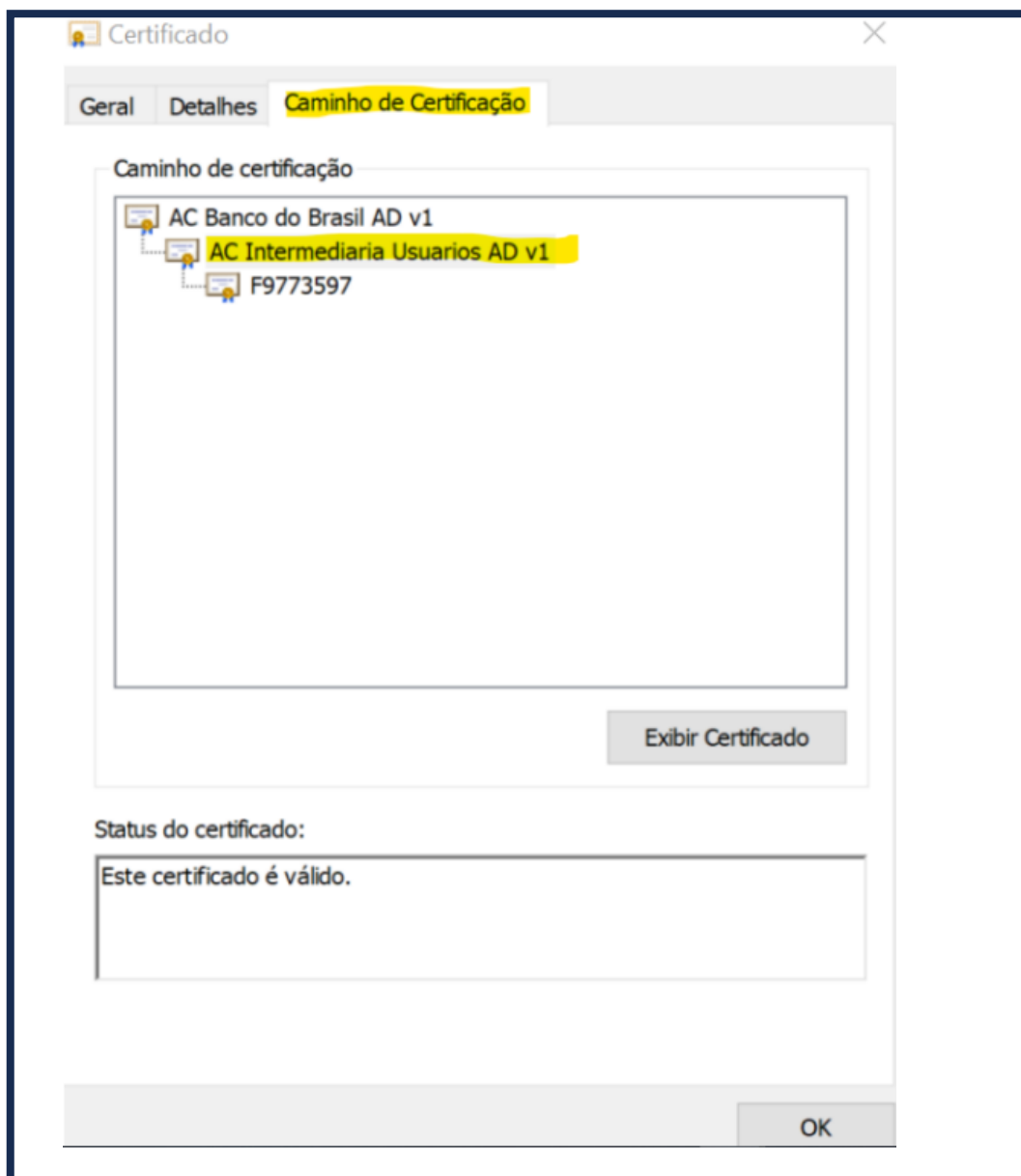


Salve o certificado com o nome Empresa para facilitar mais adiante.
Pronto, você exportou o certificado da Empresa a ser colado em campo específico no Portal Developers.
Exportar os demais certificados (Certificado intermediário e Raiz do Certificado)
Realizar os mesmos procedimentos acima.

Retorne ao certificado conforme orientado nos passos "a" a "c" anteriormente e vá em caminho de Certificação:

Selecione o Certificado intermediário exatamente seguinte a Raiz e depois realize os mesmos procedimentos realizados com Certificado da empresa.

Clique em **Exibir Certificado > Detalhes > Copiar para arquivo > Avançar > Selecione o formato x.509 codificado na base 64 (*cer)** e clique em **Avançar**.

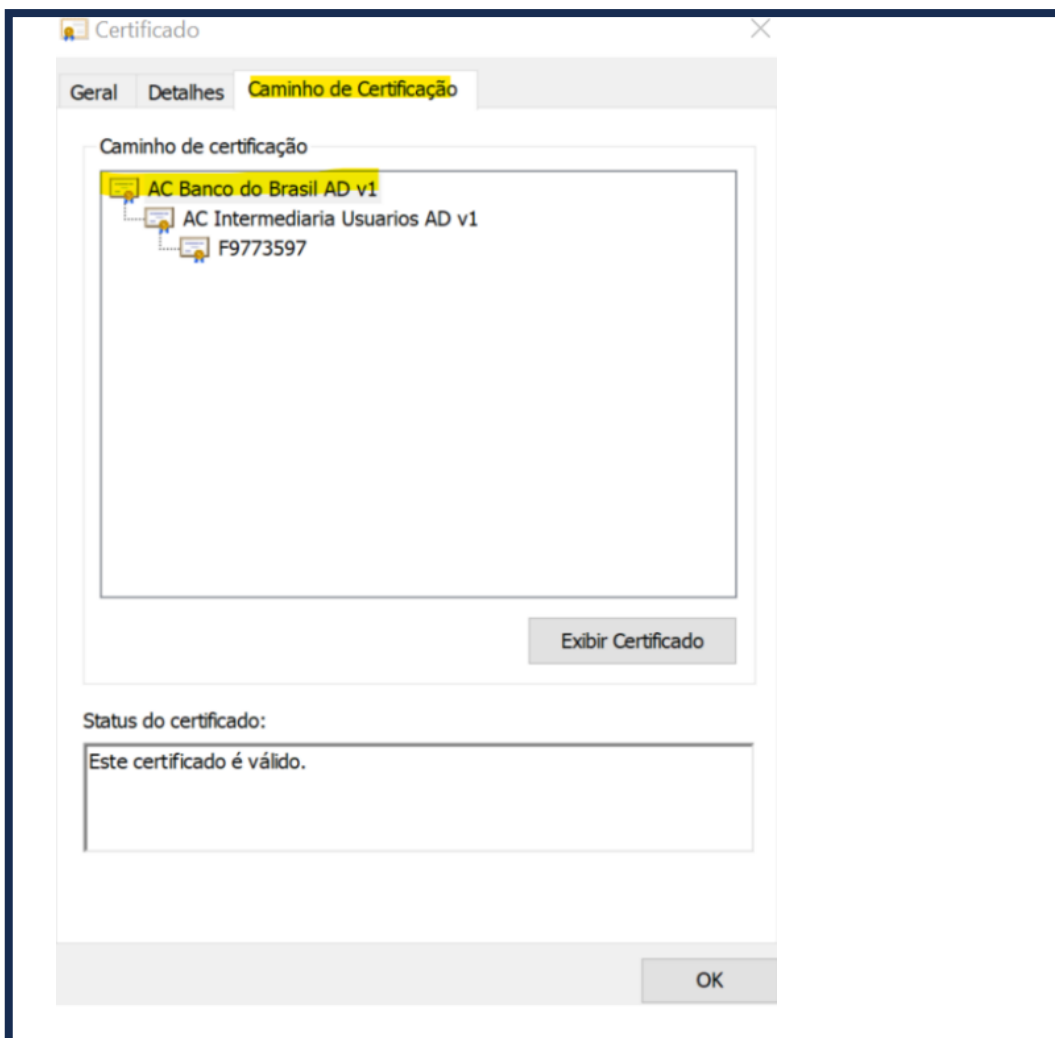


Salve o certificado com o nome Intermediário para facilitar mais adiante.

Dica! Se entre o primeiro certificado (raiz) e o último (certificado da empresa) existirem outros intermediários, repetir o procedimento para cada um deles, respeitando a ordem de cima pra baixo (intermediário1, Intermediário2 etc.).

Exportar o certificado raiz

O certificado **Raiz** é o primeiro da cadeia no Caminho de Certificação conforme exemplo abaixo:

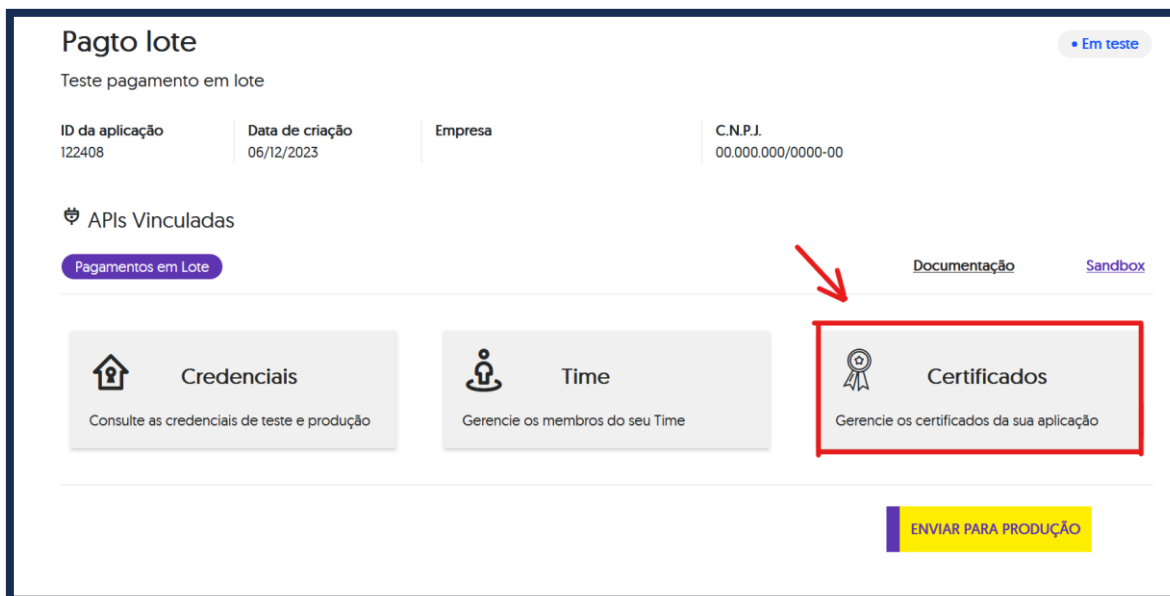


Selecione o Certificado Raiz, o primeiro de cima para baixo conforme indicado na imagem acima, e depois realize os mesmos procedimentos realizados com Certificado da empresa.

Clique em **Exibir Certificado > Detalhes > Copiar para arquivo > Avançar > Selecione o formato x.509 codificado na base 64 (*cer)** e clique em **Avançar**. Salve o certificado com o nome Raiz para facilitar mais adiante.

Acesse o [Portal Developers](#).

Selecione a API para a qual será encaminhado o certificado. Clique em **Certificados**.




Pagto lote • Em teste


Teste pagamento em lote


| | | | |
|---------------------------|-------------------------------|---------|--------------------------------|
| ID da aplicação 122408 | Data de criação 06/12/2023 | Empresa | C.N.P.J. 00.000.000/0000-00 |
|---------------------------|-------------------------------|---------|--------------------------------|

🔑 APIs Vinculadas

Pagamentos em Lote [Documentação](#) [Sandbox](#)

**Credenciais**
Consulte as credenciais de teste e produção

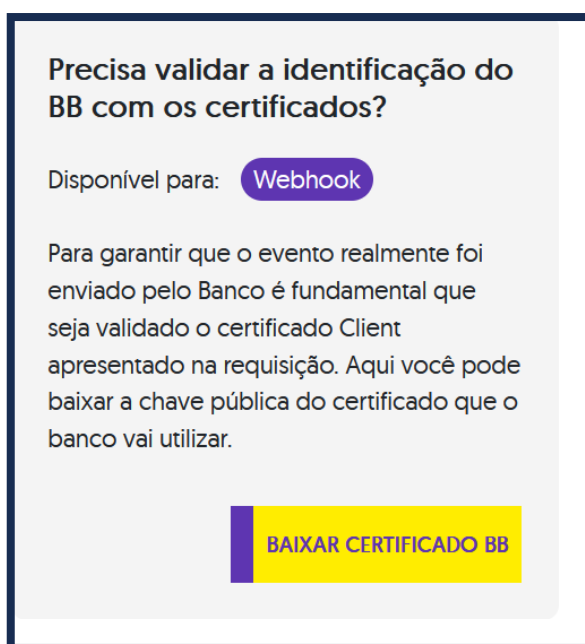
**Time**
Gerencie os membros do seu Time

**Certificados**
Gerencie os certificados da sua aplicação

ENVIAR PARA PRODUÇÃO

São duas opções disponíveis:

- A primeira sobre “Como obter os certificados e identificar as requisições feitas pelo BB?”, que possibilita baixar o Certificado BB.



Precisa validar a identificação do BB com os certificados?

Disponível para: **Webhook**

Para garantir que o evento realmente foi enviado pelo Banco é fundamental que seja validado o certificado Client apresentado na requisição. Aqui você pode baixar a chave pública do certificado que o banco vai utilizar.

BAIXAR CERTIFICADO BB

- A segunda opção é a que será usada para enviar os seus certificados obtidos por uma CA (organização responsável pela emissão de Certificados Digitais) para o BB. Clique em **Enviar Certificado**.

Você tem um certificado próprio obtido por uma CA.

Disponível para: **API** **Webhook**

Envie o arquivo do seu certificado com validade vigente. Para uso em APIs e Webhook basta enviar uma única vez.

ENVIAR CERTIFICADO

Você possui um serviço HTTPS em funcionamento.

Disponível para: **Webhook**

Vamos fazer uma tentativa para obtenção do certificado exposto e configurar para que seja confiável em nossos servidores.

LIBERAÇÃO AUTOMÁTICA

A tela apresentada mostra como adicionar a Cadeia de Certificados.

Cadeia de certificados

Certificado #1

Certificado #2

+ Adicionar certificado

Certificado #1

Adicione a cadeia de certificados do domínio que será utilizada para APIs mTLS e/ou Webhook. Devem ser incluídos o certificado raiz (AC), o certificado da sua empresa e os certificados intermediários (caso existam). Cada certificado que compõe o caminho de certificação deve ser incluído de forma isolada nas áreas correspondentes.

Em caso de dúvidas, consulte a [documentação](#).

IMPORTAR CERTIFICADO

Dica: Na maioria das vezes, existem 4 certificados. Um certificado da empresa, dois certificados intermediários e um certificado raiz. Clique duas vezes em **Adicionar certificado**, para incluir cada um deles no respectivo botão.

Cadeia de certificados

Certificado #1

Certificado #2


Certificado #3

Certificado #4

+ Adicionar certificado

IMPORTANTE:



NÃO clicar em  (Enviar), antes de inserir TODOS os certificados. O envio é feito somente ao final do processo.

São duas formas de inserção do certificado:

- fazendo a importação do certificado, clicando em **Importar Certificado**. É a melhor opção, pois o conteúdo do certificado é colado no campo respectivo, evitando alguma falha no processo de copiar/colar.



OU

- abrindo o certificado com um editor de texto (**Bloco de Notas, Notepad++** ou similar), copiando todo o conteúdo do certificado (**Ctrl+C**) e colando (**Ctrl+V**) no campo.

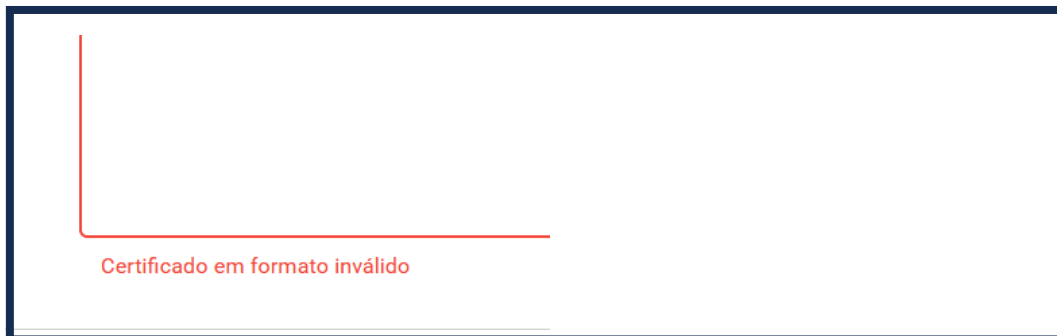
Exemplo de conteúdo do certificado em formato PEM:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzTCCAbUCAQAwYcxCAzA1BgNVBAYTAkdCMRYwFAYDVQQIEw11TdGFMzMyZHN0
aXJ1M1RwFQYDVQHQEw5TdG9rZS8vbiBUcmVudDEjMCEGA1UEChMaUmVkaIEt1c3Ry
ZWwGQ29uc3VsdGluZyBmDQGXjIjAgBgNVBAMTGXR1c3RjZjX0Lnl1ZGt1c3RyZWw
Y28udlwsggEiMA0GCQSqG5Ib3kDQEBAQAA1BDwAwgEKAoIUAQDVULw88TeAia3N
23R99i8174fhjef+tSTSGPgkFGBXj++tclKgk3MJE0iJd4PNaxGXUCUNLgn2R0yy
bm5sTmGzpEOD+1AAAYv+pLQoFNkHEFuudGqVM6XkPWfqaM2vKvdzUbPPC0X/MfDF
GPxc8AY3TUM385c9c9/WOIF6NUcAvAFIQf0zG7evzJZBqDb4enUnatMSLHmxRWmi
1JeHtFLINXhNihHewEQWgIB3j1xmh7CP05FeTb6HzQDxc+f7uMisY6s9J/Ph3GeO
LeIDooqU8jnfV5aEgEiIMH5CFMZjaJrNKF4DYK3YRYUI0K66+vK0iL0UntEs++M20
LhOn+VE9AgMBAAGGADANBgkqhkiG9w0BAQUFAAOCAQEAWUe7oBX3SLjYNNM53bsB0
lNGnsGAP1P1f1CPpEKaZGE0UJ2x0hZTsu1N1ZigKpWmiAAZxuoaag1R/ANM3jXp
vCLVBRv40AHCFsot9udrdCYjI43aDHAaYvLmT4/Pvpntcn0/7+g//e1AHhr9UIoo
MZwww6yom67Jwfw/be/g7Mae7mPHZ21sQTS02hEqqYynIRk2W9meQULrt+/atog
0mqJ3Bx0WswtH1i1tC+nxFPqRwFTEzVuPGCOVw7LmCFNmHNcKZVuRSJB/9MdLmrfw
chPI3NeTGSse+BZfs0tpt2/7j+bqeYKFu8B0stLoJBEnihxUoV18uZ0mOeuVuX1N6
nA==
-----END CERTIFICATE REQUEST-----
```

Importar Certificado:

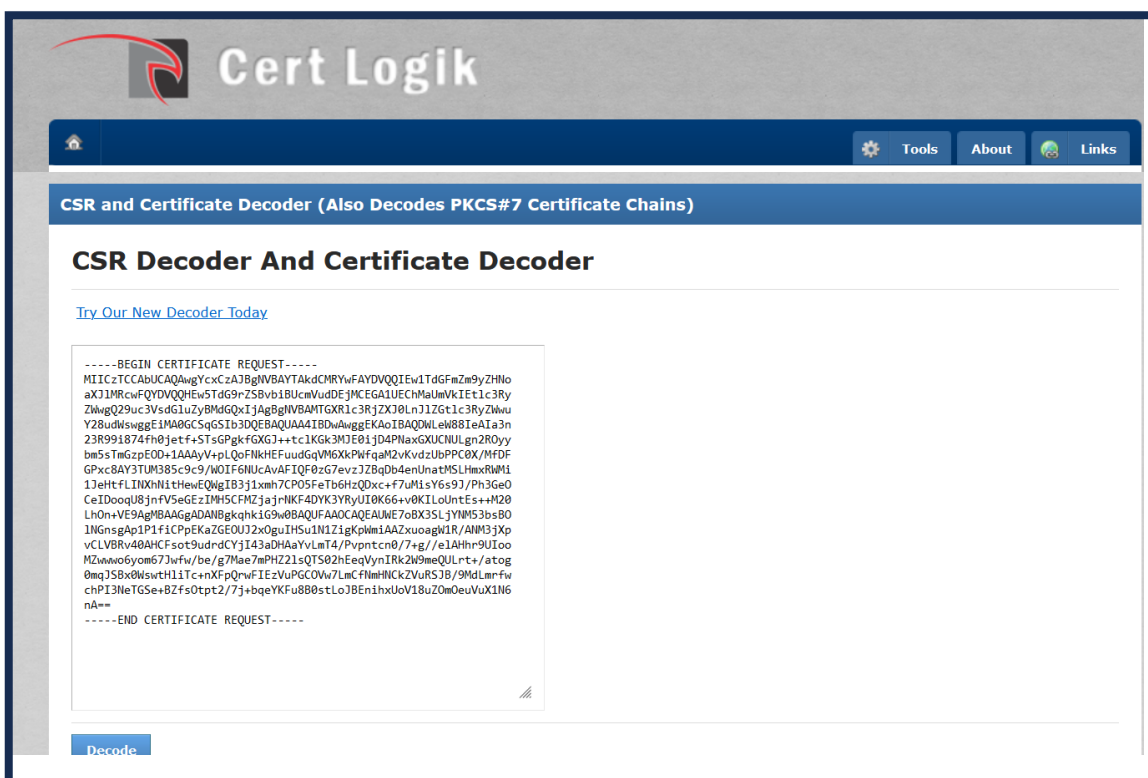
Podem ser importados os arquivos de certificados com extensão **.pem**, **.ctr**, **.cer** e **.cert**.

Se, durante a importação do certificado for mostrada a mensagem de erro “Certificado em formato inválido”, como abaixo:



verifique se há alguma inconsistência no arquivo, fazendo um teste na página

<https://certlogik.com/decoder/>



Este decodificador faz alguns ajustes na formatação do conteúdo. Experimente copiar o arquivo criado no decodificador e colar novamente no campo do certificado a ser enviado para o Banco do Brasil. Só isso já soluciona o problema de formato inválido.

Após adicionar todos os certificados separadamente, conforme os passos informados acima, clique em **Enviar**.

Será exibida rapidamente no canto superior direito a mensagem "Requisição feita com sucesso" e você será direcionado para a tela abaixo:

The screenshot shows a user interface for uploading certificates. It has two main sections at the top, each with a description, available options, instructions, and a button.

Left Section:

- Header:** Você tem um certificado próprio obtido por uma CA.
- Disponível para:** API, Webhook
- Text:** Envie o arquivo do seu certificado com validade vigente. Para uso em APIs e Webhook basta enviar uma única vez.
- Button:** ENVIAR CERTIFICADO

Right Section:

- Header:** Você possui um serviço HTTPS em funcionamento.
- Disponível para:** Webhook
- Text:** Vamos fazer uma tentativa para obtenção do certificado exposto e configurar para que seja confiável em nossos servidores.
- Button:** LIBERAÇÃO AUTOMÁTICA

Table: Solicitações de envio de certificados

| Ambiente | Número solicitação | Situação | Data envio | Data vencimento |
|----------|--------------------------------------|----------|------------------------|-----------------|
| Teste | 0857530b-2a47-4cbc-9aed-bc059918699f | Sucesso | 15/03/2024 19:11:14 | 13/12/2024 |

O campo **Número Solicitação** é a identidade da requisição. Ele deverá ser informado quando você precisar se referir ao envio do certificado.

O campo **Situação** passará para **Sucesso** assim que o certificado for internalizado, o que ocorre no mesmo dia.



Ficou alguma dúvida? Faça contato conosco:

suporte.openbanking@bb.com.br