AUTORIDADE CERTIFICADORA DE DEFESA

- Geração de par de chaves
- Importação do Certificado A1

Guia de instruções

Agosto 2024

Índice

Glossário 3
1. Introdução 4
2. Preparação do ambiente 5
3. Gerando o par de chaves 6
4. Importação do Certificado A1 12
5. Utilização do Certificado A1 em outra máquina: 17

Glossário

Certificado Digital - é uma forma de identificar pessoas e empresas em sistemas e documentos digitais. Ele funciona como uma identidade virtual, apresentada por meio de sistemas de validação. Permite fazer diversas atividades de forma mais segura e simples.

Certificado A1 – certificado armazenado em software com validade de 1 ano.

Chave Privada – em posse do proprietário do certificado, permite fazer criptografias que podem ser validadas com seu certificado.

Exemplo: assinaturas digitais

Par de Chaves - é um conceito fundamental na criptografia assimétrica, também conhecida como criptografia de chave pública. Nesse tipo de criptografia, são utilizadas duas chaves distintas: uma chave pública e uma chave privada.

Keyutils - aplicação para geração do par de chaves e expedição do certificado.

Extensão .pfx / .p12 - é o formato de arquivo para armazenamento de certificado do tipo A1/S1.

Extensão .csr – sigla significa Certificate Signing Request, é um arquivo de texto, gerado pelo servidor web, contendo as informações para a solicitação do seu certificado, usada para gerar um certificado assinado digitalmente.

1.Introdução

A Autoridade Certificadora do Ministério da Defesa (AC Defesa) tem como missão emitir e fornecer certificados digitais para o Ministério da Defesa (MD), bem como para as três Forças: Marinha do Brasil (MB), Exército Brasileiro (EB) e Força Aérea Brasileira (FAB).

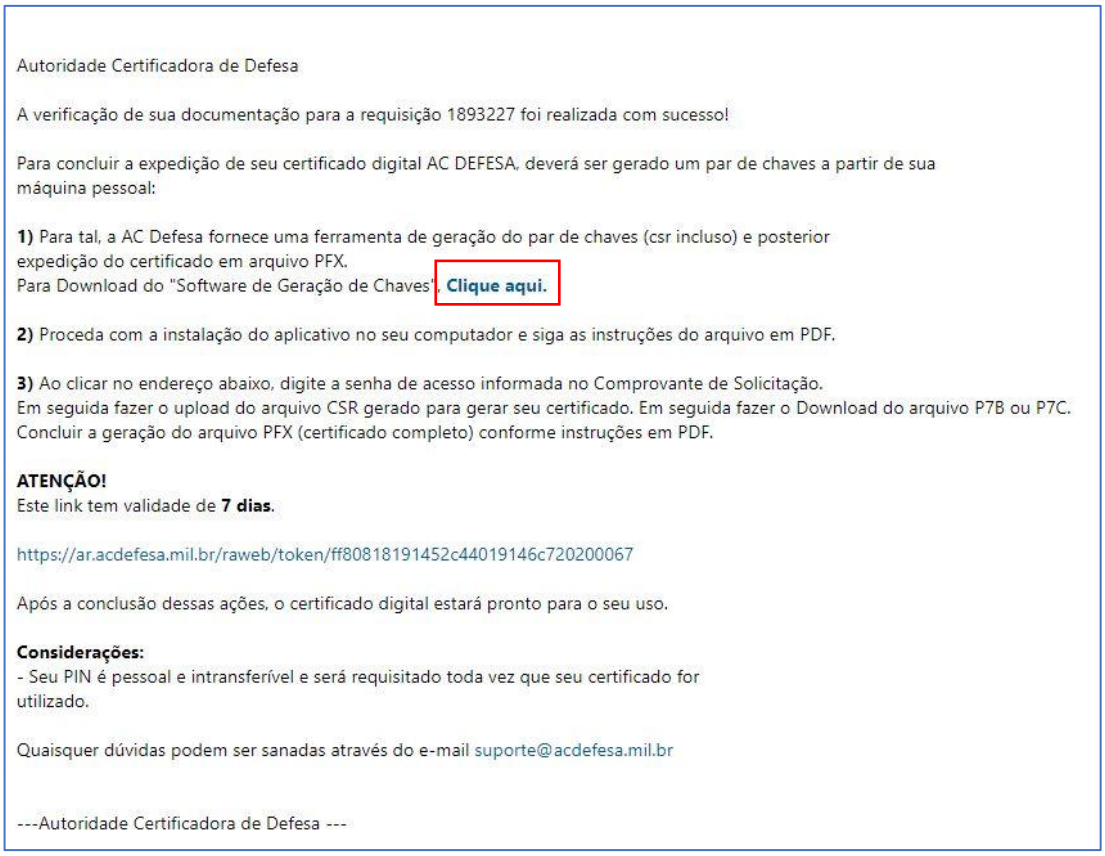
O presente manual tem como objetivo orientar o usuário no processo de emissão do certificado A1, desde a instalação do software de geração de par de chaves até a importação do certificado para o computador.

O certificado A1 é utilizado em aplicações para autenticação de usuário (confirmação de identidade) e para assinatura de documentos eletrônicos com verificação da integridade de suas informações. Utiliza chave criptográfica de 2048 bits, é armazenado no computador do usuário e deverá ser protegido por senha de acesso, tendo validade de 01 ano. Para emissão do certificado A1, o militar deverá comparecer presencialmente em um posto de identificação munido de identidade e comprovante de residência.

2. Preparação do ambiente

Instalação/execução do software KeyUtils:

2.1 Clique no link do item 1: “Software de geração de par de chaves” recebido no email que informou sobre a os procedimentos para conclusão da expedição do certificado digital (exemplo abaixo) para baixar o arquivo ou acesse https://repositorio.acdefesa.mil.br/Gerar_Par_de_Chaves/Windows/



Autoridade Certificadora de Defesa

A verificação de sua documentação para a requisição 1893227 foi realizada com sucesso!

Para concluir a expedição de seu certificado digital AC DEFESA, deverá ser gerado um par de chaves a partir de sua máquina pessoal:

1) Para tal, a AC Defesa fornece uma ferramenta de geração do par de chaves (csr incluso) e posterior expedição do certificado em arquivo PFX.
Para Download do "Software de Geração de Chaves", **Clique aqui.**

2) Proceda com a instalação do aplicativo no seu computador e siga as instruções do arquivo em PDF.

3) Ao clicar no endereço abaixo, digite a senha de acesso informada no Comprovante de Solicitação.
Em seguida fazer o upload do arquivo CSR gerado para gerar seu certificado. Em seguida fazer o Download do arquivo P7B ou P7C.
Concluir a geração do arquivo PFX (certificado completo) conforme instruções em PDF.

ATENÇÃO!
Este link tem validade de **7 dias**.

https://ar.acdefesa.mil.br/raweb/token/ff80818191452c44019146c720200067

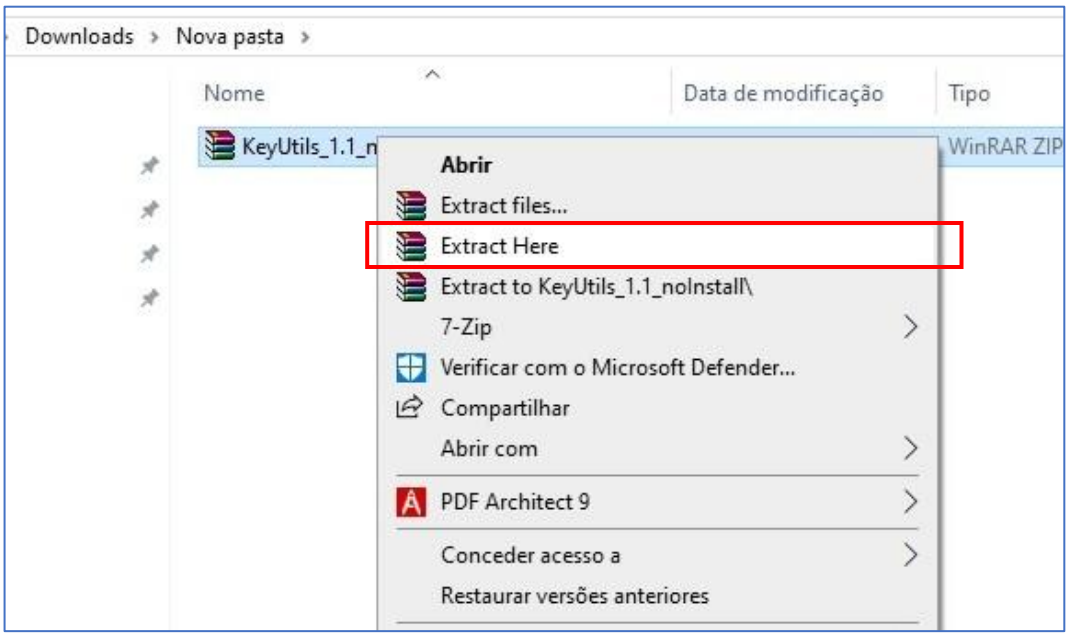
Após a conclusão dessas ações, o certificado digital estará pronto para o seu uso.

Considerações:
- Seu PIN é pessoal e intransferível e será requisitado toda vez que seu certificado for utilizado.

Quaisquer dúvidas podem ser sanadas através do e-mail suporte@acdefesa.mil.br

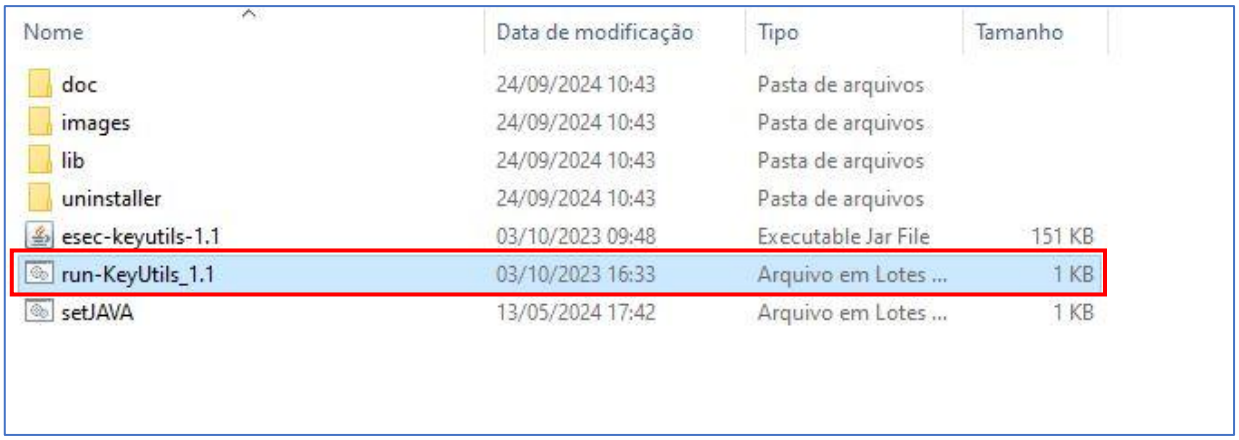
---Autoridade Certificadora de Defesa ---

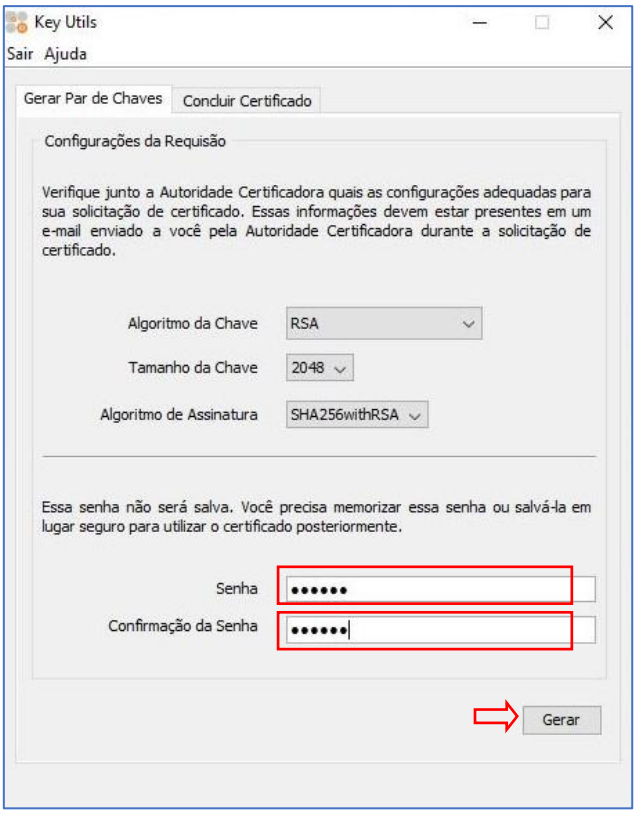
2.2 Extraia o arquivo **keyUtils_1.1_noInstall**:



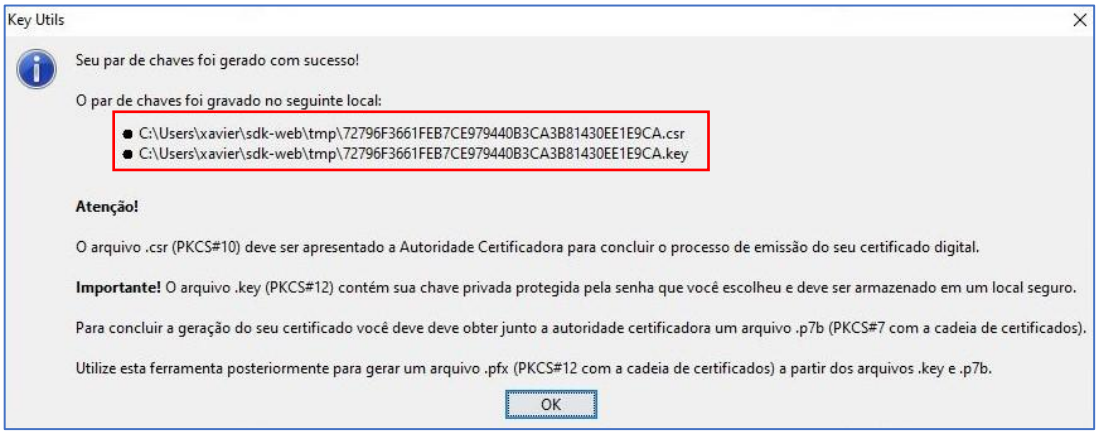
3. Gerando o par de chaves

3.1 Entre na pasta descompactada e execute o arquivo “run-keyutils-1.1”:





Obs: Fique atento ao caminho onde foram salvos os arquivos: O arquivo "********.csr" será utilizado para gerar o certificado que será utilizado posteriormente na aba **Concluir Certificado**.



3.3 Acesse o email recebido e clique no link de acesso ao sistema de emissão do certificado:

Autoridade Certificadora de Defesa

A verificação de sua documentação para a requisição 1893227 foi realizada com sucesso!

Para concluir a expedição de seu certificado digital AC DEFESA, deverá ser gerado um par de chaves a partir de sua máquina pessoal:

1) Para tal, a AC Defesa fornece uma ferramenta de geração do par de chaves (csr incluso) e posterior expedição do certificado em arquivo PFX.
Para Download do "Software de Geração de Chaves", **Clique aqui.**

2) Proceda com a instalação do aplicativo no seu computador e siga as instruções do arquivo em PDF.

3) Ao clicar no endereço abaixo, digite a senha de acesso informada no Comprovante de Solicitação.
Em seguida fazer o upload do arquivo CSR gerado para gerar seu certificado. Em seguida fazer o Download do arquivo P7B ou P7C.
Concluir a geração do arquivo PFX (certificado completo) conforme instruções em PDF.

ATENÇÃO!
Este link tem validade de **7 dias**.

https://ar.acdefesa.mil.br/raweb/token/ff80818191452c44019146c720200067

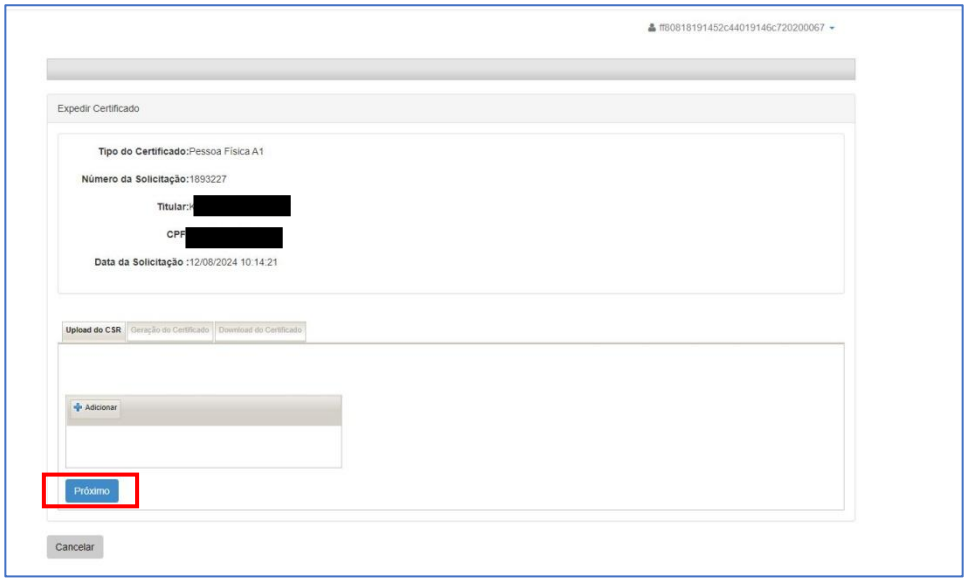
Após a conclusão dessas ações, o certificado digital estará pronto para o seu uso.

Considerações:
- Seu PIN é pessoal e intransferível e será requisitado toda vez que seu certificado for utilizado.

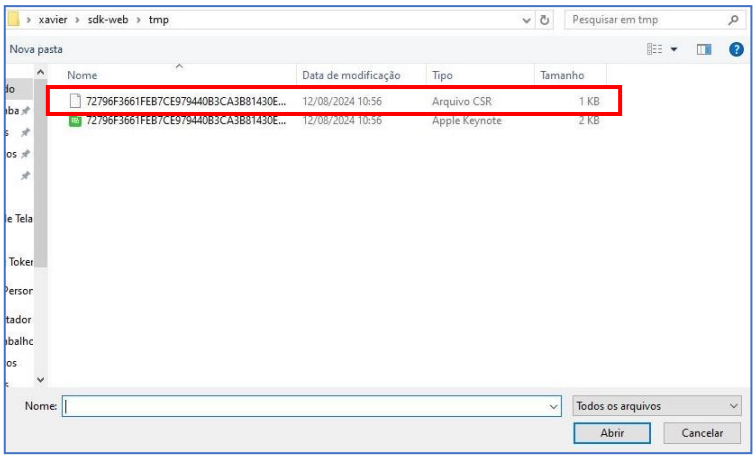
Quaisquer dúvidas podem ser sanadas através do e-mail suporte@acdefesa.mil.br

---Autoridade Certificadora de Defesa ---

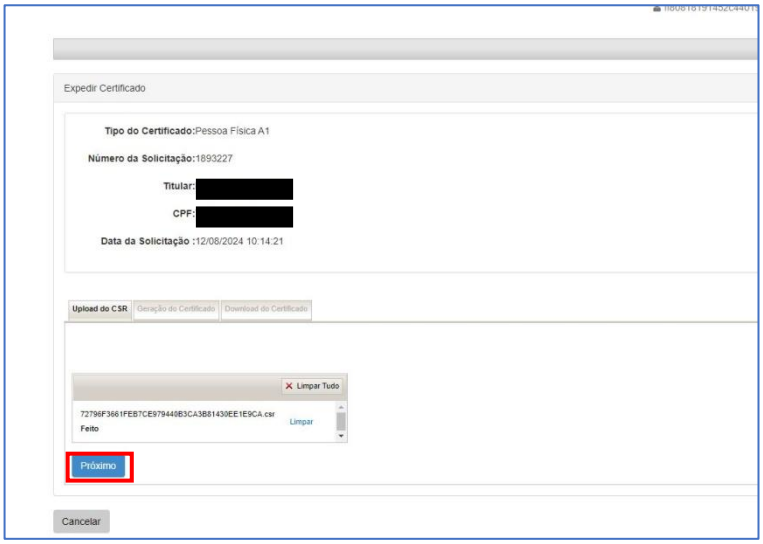
3.4 Clique em adicionar para fazer o upload do arquivo CSR:



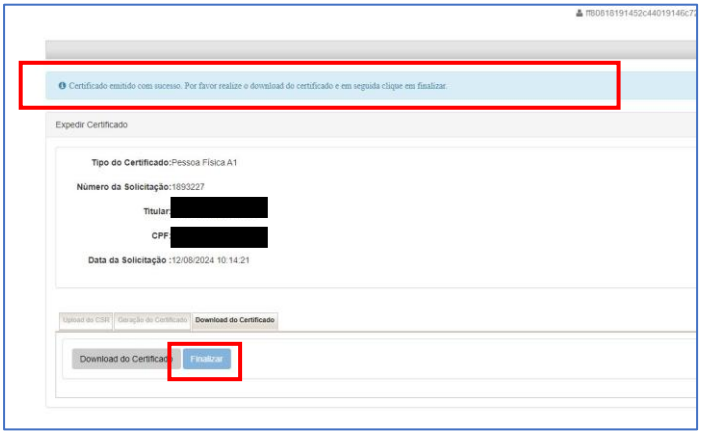
3.5 Clique no arquivo CSR gerado no caminho informado anteriormente:



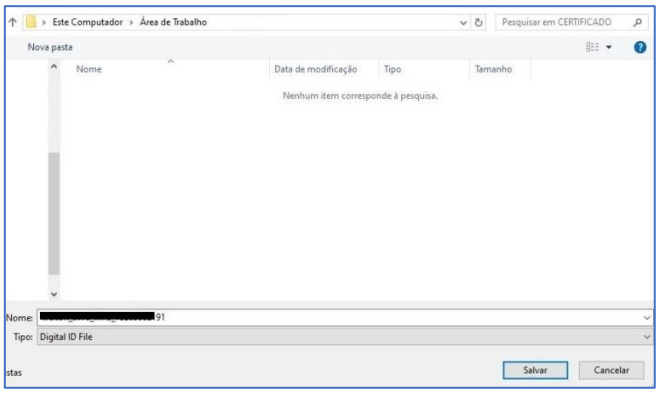
3.6 Clique em “próximo”:



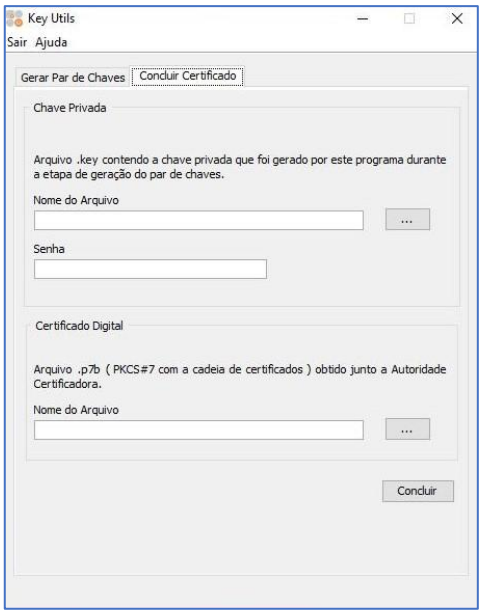
3.7 Realize o download do certificado e em seguida clique em “finalizar”:



Obs: O arquivo baixado será salvo na Área de trabalho e utilizado posteriormente para emissão do cerificado A1;

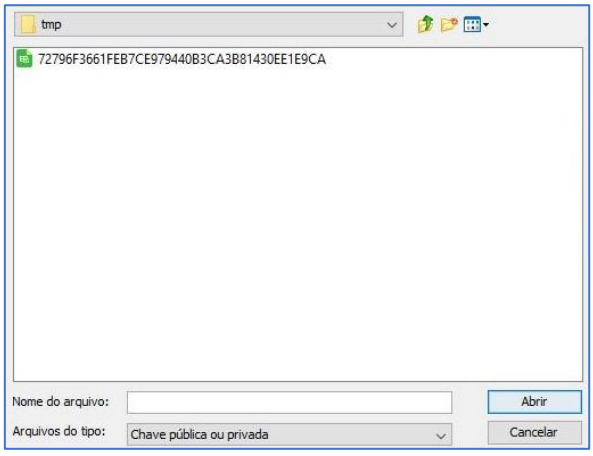


3.8 No aplicativo KeyUtils, clique na aba Concluir certificado:

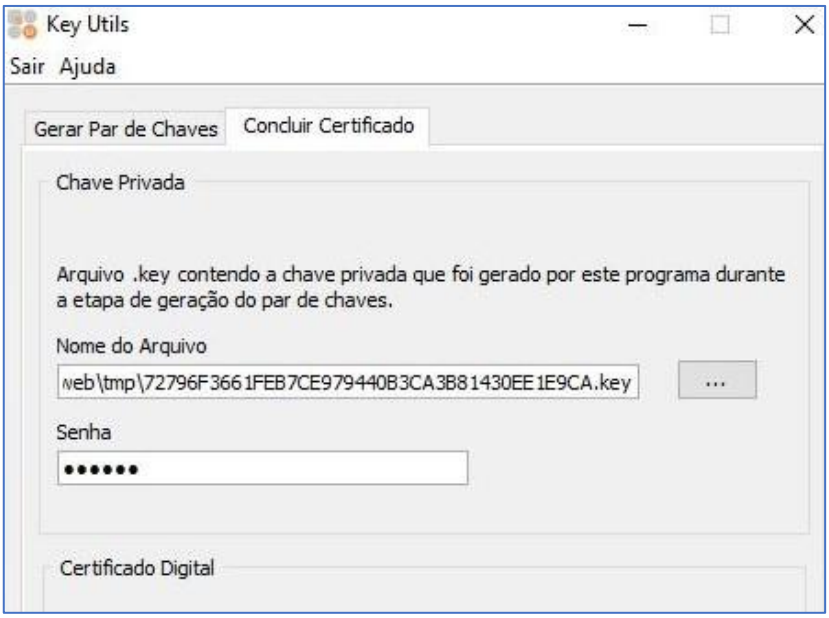


3.9 Painel Chave Privada

Clique no botão  para selecionar o arquivo da chave privada. Este arquivo deverá ter a extensão **.key**. Vá até o diretório onde encontra-se o arquivo, selecione-o, e clique no botão **Abrir**.



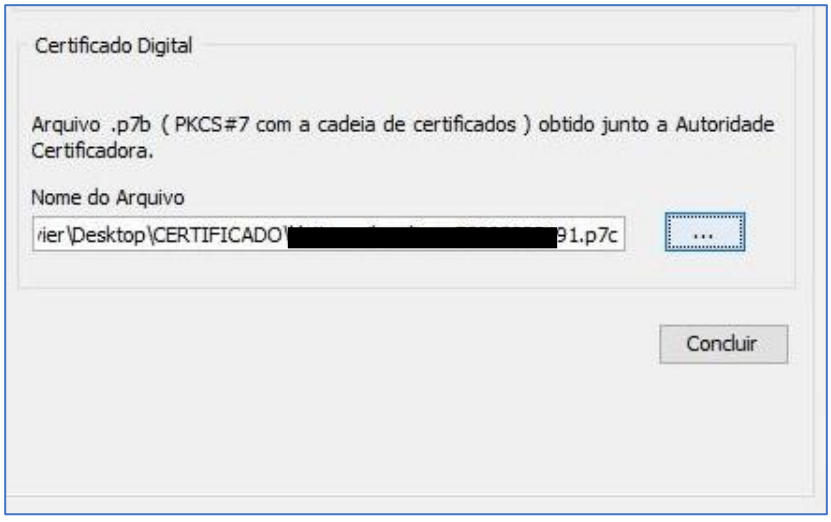
O sistema irá retornar para o aplicativo com o campo **Nome do arquivo** preenchido. Ainda no painel **Chave Privada**, digite a senha da chave privada.



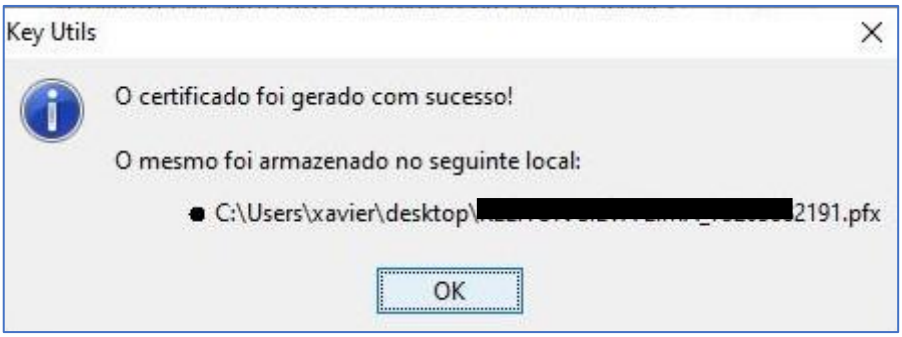
3.10 Painel Certificado Digital

3.10.1 Clique no botão ... para selecionar o arquivo da cadeia de confiança do certificado. Este arquivo deverá ter a extensão **.p7c**.

3.10.2 Execute os mesmos passos utilizados para selecionar o arquivo da chave privada, anteriormente descritos. Clique no botão Concluir.



3.10.3 O sistema gerará o arquivo **.pfx** e informará o local de armazenamento do mesmo:



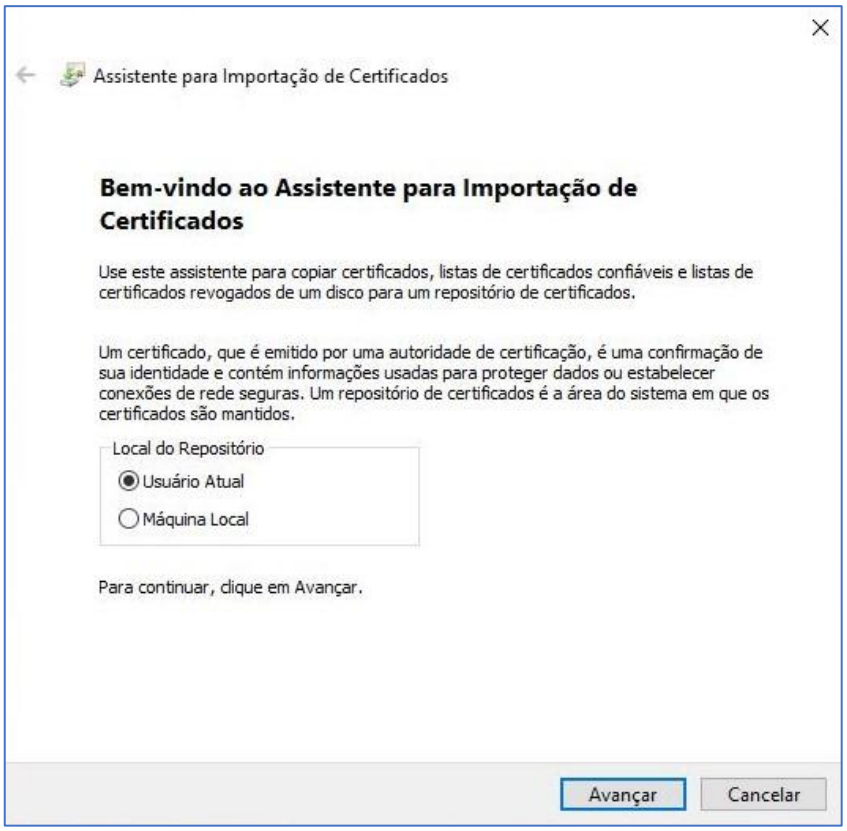
3.10.4 O arquivo ficará salvo conforme imagem abaixo:

4. Importação do Certificado A1:

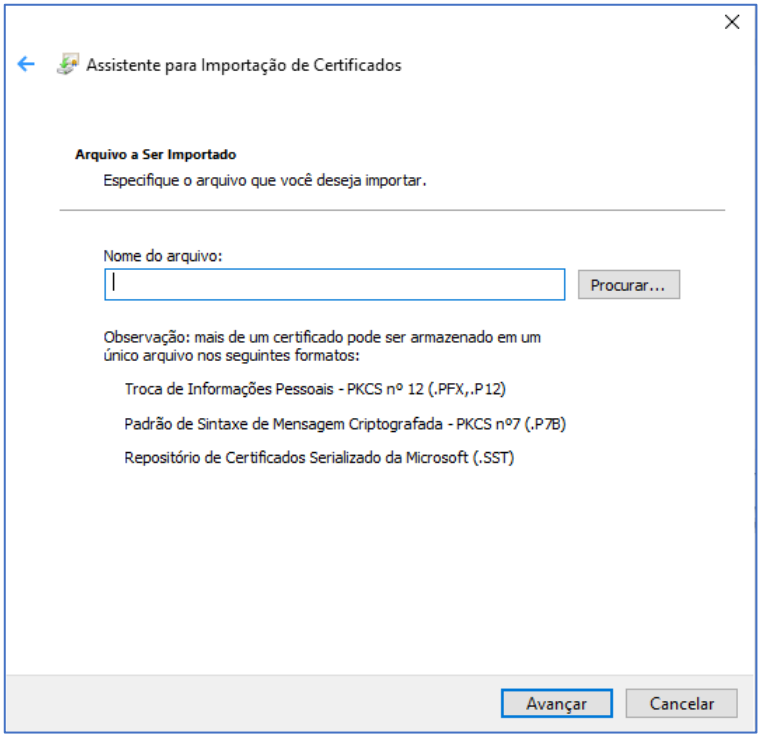
Para utilização do certificado A1 pelos navegadores, o arquivo do tipo PFX ou P12 contendo o certificado, deverá ser importado para o gerenciador de certificados do Windows:

4.1 Clique duas vezes no ícone :

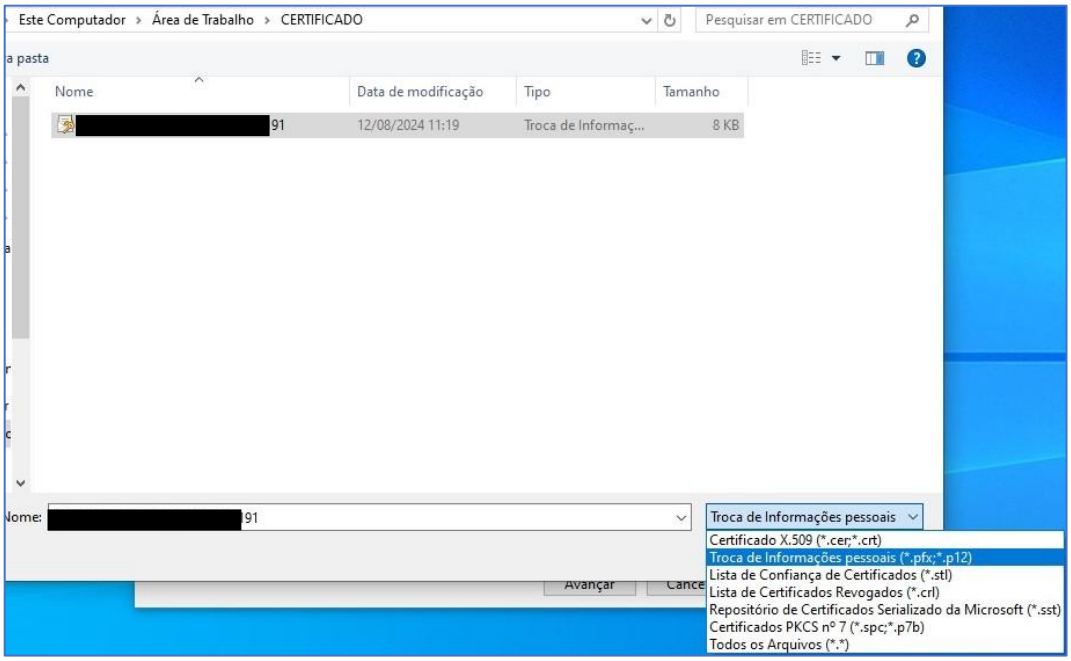
4.2 Na janela a seguir, o “Local do Repositório” é “Usuário Atual”:



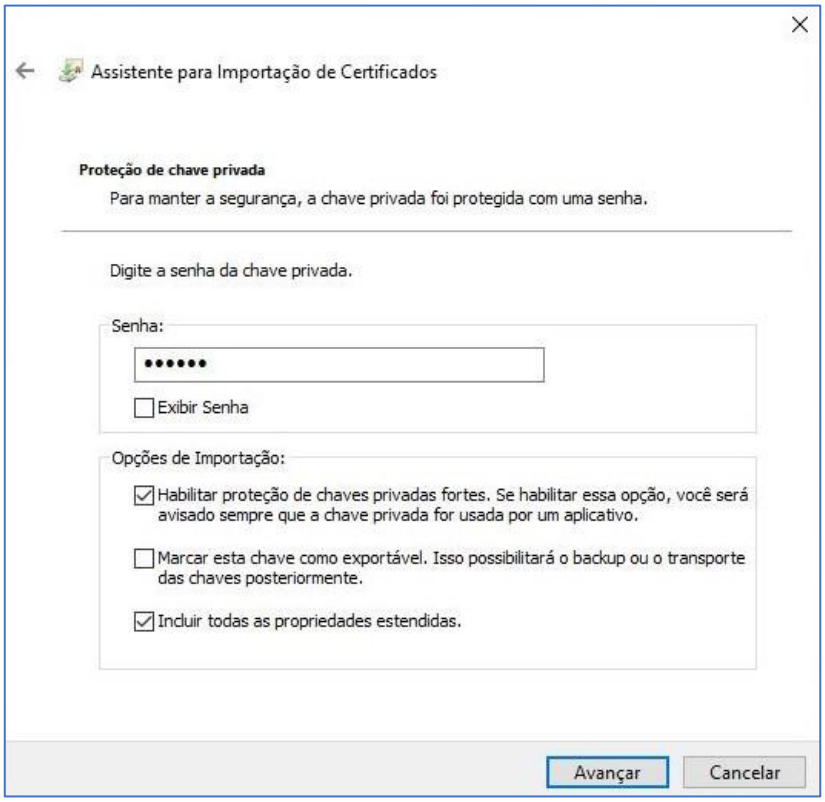
4.3 Clique em “Procurar…”.



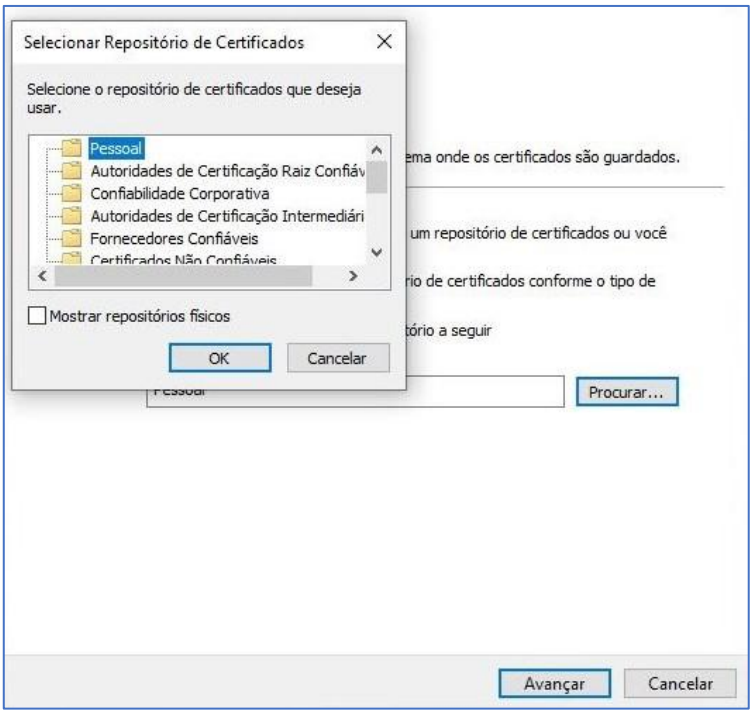
4.4 Na caixa de seleção do tipo de arquivo, selecione “Troca de informações pessoais (*.pfx, *.p12), em seguida selecione seu arquivo de certificado (Ex. certificado.pfx). Em seguida clique em “Avançar”.



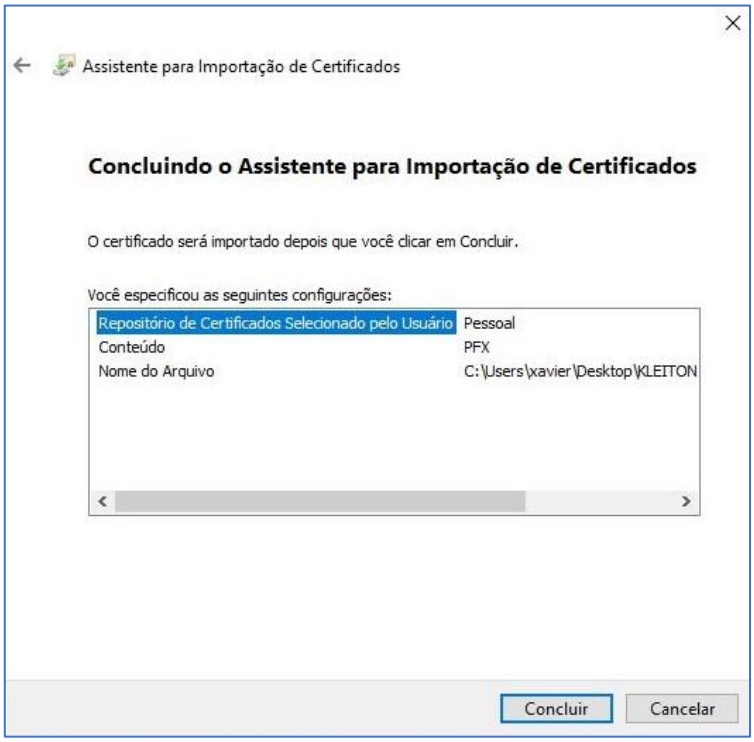
4.5 Digitar a senha do certificado e marcar a opção “Habilitar a proteção de chaves privadas fortes.”, em seguida avançar.



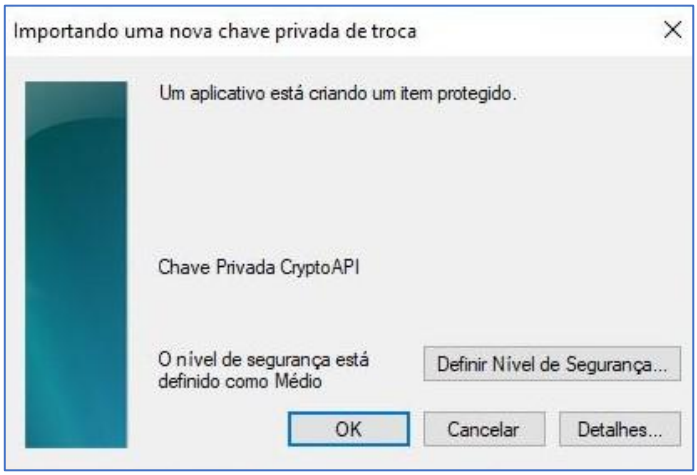
4.6 Escolher o repositório “Pessoal”. Caso não venha preenchido, clicar em “Procurar…” e selecionar o diretório “Pessoal”. Clique em “Avançar”.



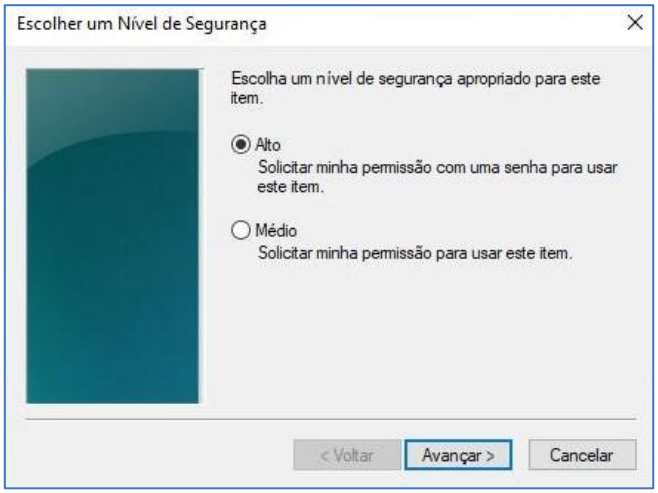
4.7 Conferido, clique em “Concluir”



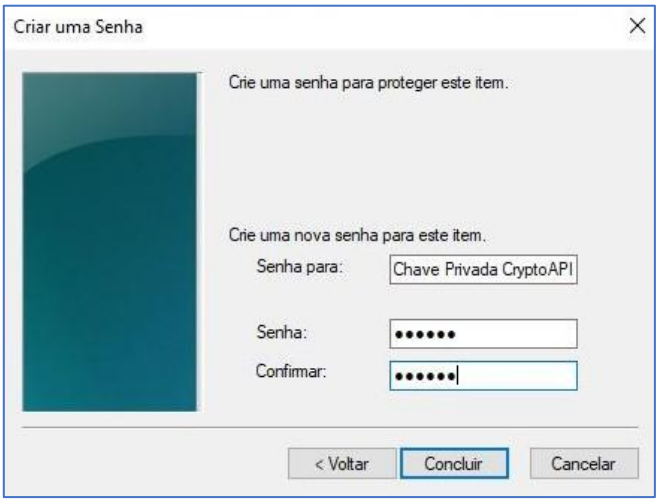
4.8 Após concluir, será aberta uma nova janela para definir a segurança da chave privada e uso do certificado. Recomenda-se o nível "Alto". Para tal, clique em "Definir Nível de Segurança…"



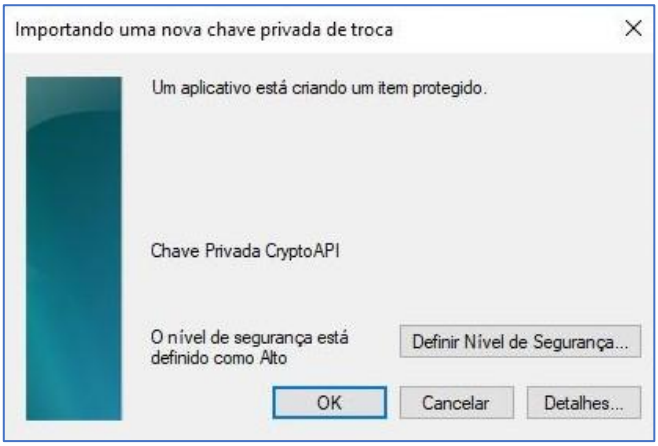
4.9 Selecione "Alto", em seguida Avançar.



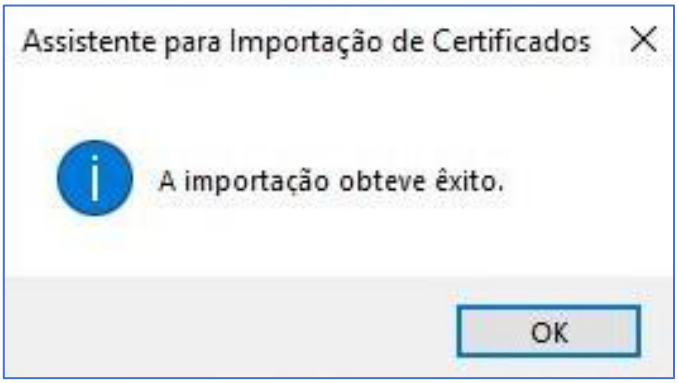
4.10 Crie e confirme a senha do seu certificado, em seguida clique em "Concluir".



4.11 Para finalizar, clique em “OK”;



4.12 Com esta mensagem a importação foi concluída e seu certificado pode ser utilizados por aplicações que utilizam o Microsoft CAPI no Windows.



5. Utilização do Certificado A1 em outra máquina:

Caso o usuário deseje utilizar o seu certificado em outra máquina, deverá copiar o certificado .pfx para a máquina destino e seguir o passo do item 3. Importação do Certificado A1.


AC DEFESA