



AUTORIDADE CERTIFICADORA DE DEFESA

EMISSÃO SIMPLIFICADA

- DXToken

Outubro 2024

Sumário

Glossário.....	3
1. Introdução	4
2. Preparação do Ambiente.....	5
2.1. Softwares necessários.....	5
2.2. Inicialização do Token DXToken.....	7
3. Processo de emissão.....	9
3.1. Passo 1 - Busca dos dados e solicitação.....	9
3.2. Passo 2 - Verificação e Aprovação.....	10
3.3. Passo 3 - Geração do par de chaves e instalação do certificado.....	12
4. Conclusão	13

Glossário

Autorizador designado: Autorizador local ou Autorizador da AR Defesa;

Autorizador local: Homologadores do Sistema de Cadastro de Pessoal das Forças (atualmente somente SICAPEX), cadastrados na base de dados de pessoal do Exército para uma organização militar.

Autorizador da AR Defesa: Supervisores da Autoridade de Registro vinculada à AC Defesa (AR Defesa), atribuídos para atender casos excepcionais.

Driver: Software que permite que o sistema operacional ou um aplicativo interaja com um dispositivo de hardware específico.

ITI: Instituto Nacional de Tecnologia da Informação, Órgão regulador da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Log: Registro de um evento em arquivo ou banco de dados para consulta posterior (geralmente com data e hora do evento e detalhes que possam identificar o acontecido e/ou a finalidade).

Login: Ação de entrada de um usuário em um software (autenticação), onde o usuário faz tentativa de entrada e o sistema após verificar as credenciais, autoriza o acesso aos recursos que o usuário faz jus.

Par de Chaves: Duas chaves relacionadas, uma chave pública e uma chave privada, que são utilizadas para diferentes propósitos.

Token USB: Dispositivo criptográfico USB capaz de armazenar chaves públicas e privadas, bem como certificados digitais.

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).

Em agosto de 2017, através da instrução normativa nº 06 relacionada à DOC-ICP-05.02 em sua versão 1.4, o Instituto Nacional de Tecnologia da Informação (ITI) passou a validar a solicitação de certificados para servidores públicos da ativa e militares da União de forma simplificada, através de procedimentos específicos. Tal sistemática é chamada pelo ITI de Módulo Eletrônico de AR.

A AC Defesa é composta de uma Autoridade Certificadora Principal (ACP) em Brasília, uma Autoridade Certificadora Reserva (ACR) no Rio de Janeiro, uma Autoridade de Registro (AR) em Brasília e diversos postos de validação distribuídos em guarnições militares em todo o território nacional, na maior parte dos casos em grandes cidades. Devido à sua capilaridade, ao aumento da demanda de certificados digitais por parte de seu público-alvo e a distância de muitos militares dos postos de atendimento da AC Defesa, fez-se necessário pensar em uma solução para prestar um melhor serviço ao Ministério da Defesa e aos comandos de Forças. Neste sentido, no ano de 2022, nasceu o projeto de Emissão Simplificada, nome dado à implementação de um Módulo Eletrônico de AR no âmbito da AC Defesa.

Este guia visa orientar os solicitantes de certificados digitais da AC Defesa a empregar o sistema de emissão simplificada de certificados digitais para a emissão de certificados digitais empregando o DXToken.



Observação: Os passos abaixo descritos consideram o emprego do **sistema operacional Windows**.

2. Preparação do Ambiente

2.1. Softwares necessários

Para a execução dos passos descritos no item 3 – Processo de geração do par de chaves e instalação do certificado no token DXToken – é **necessária a configuração do computador que será empregado pelo solicitante**. Deverão ser instalados dois softwares específicos, a saber:

1. Driver do Token (“Instalador DXSafe Middleware – 1.0.30”);
2. SDK-Desktop (versão 1.0.36 ou superior).

Ambos aplicativos podem ser encontrados na área de download do site da AC Defesa (<https://www.acdefesa.mil.br/index.php/downloads>).



Importante: A instalação do software SDK-Desktop deve ser realizada da seguinte forma:

Passo 1: Baixar o arquivo “sdk-desktop-v1.0.36.zip” da página de downloads da AC Defesa;

Passo 2: Extrair o arquivo compactado para uma pasta no computador;

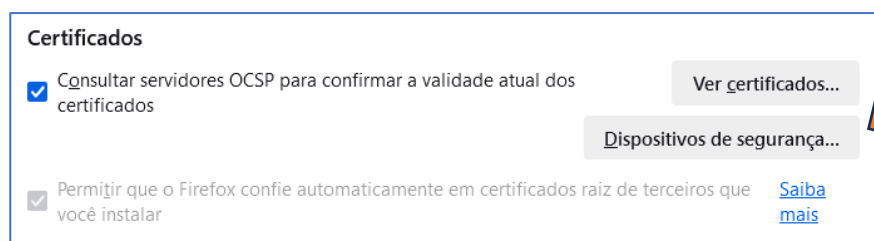
Passo 3: Clicar com o botão direito sobre o arquivo “sdk-desktop-install.bat” e selecionar a opção “Executar como administrador”.



Atenção: Caso esteja utilizando o navegador **Firefox**, após baixar e instalar as aplicações é necessário o carregamento de uma biblioteca chamada DXSafePKCS11.dll. Para isso, siga os seguintes passos:

Passo 1: digitar o endereço “<about:preferences#privacy>” na barra de endereços do navegador e em seguida digitar enter;

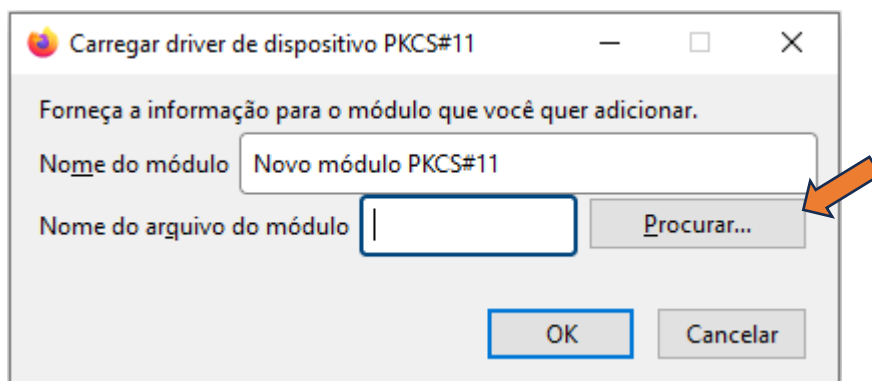
Passo 2: descer até o final da página e selecionar a opção “Dispositivos de segurança”;



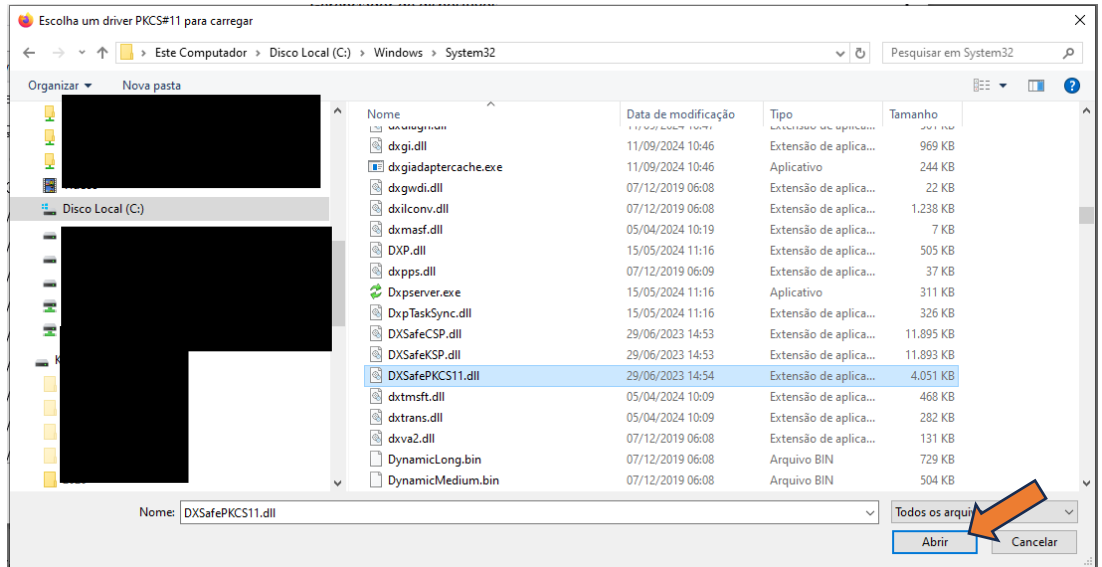
Passo 3: na janela que se abrir (“Gerenciador de Dispositivos”), clique em “Carregar”



Passo 4: na janela que se abrir (“Carregar driver de dispositivo PKCS#11”), clique em “Procurar”



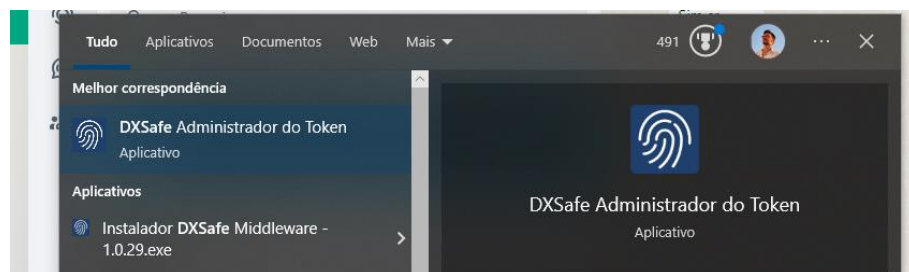
Passo 5: na janela que se abrir deverá ser selecionado o arquivo DXSafePKCS11.dll na pasta C:\Windows\System32\ e clicar em abrir.



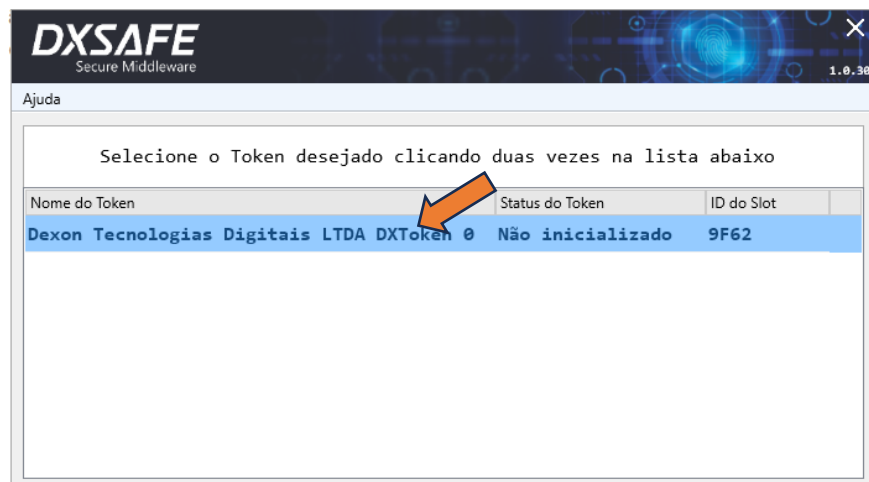
2.2. Inicialização do Token DXToken

Antes de se iniciar o processo no sistema de emissão simplificada, deve-se realizar a inicialização do token DXToken. Para isso, realize os seguintes procedimentos:

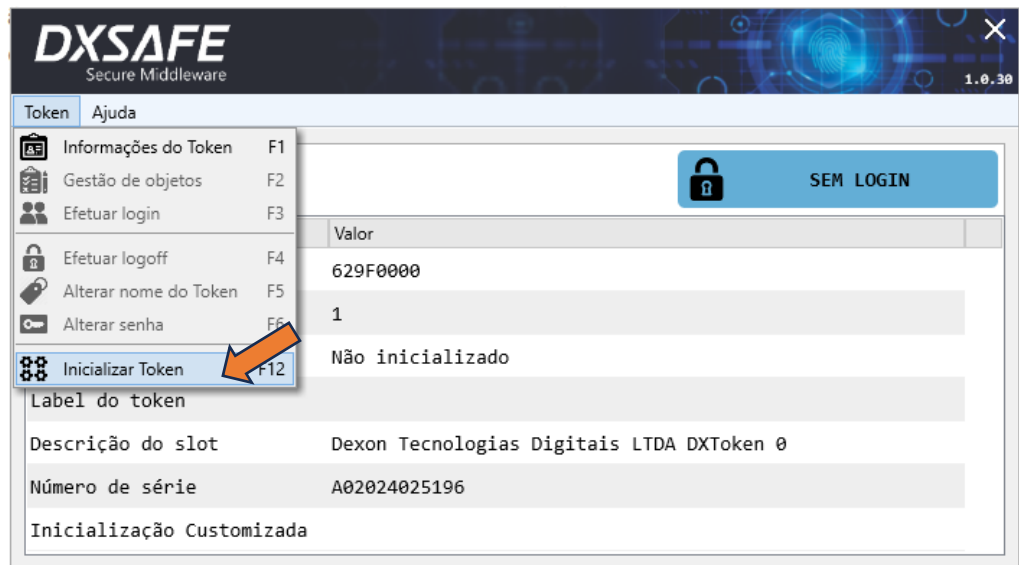
1. Insira o token DXToken em uma interface USB do computador;
2. Inicie o aplicativo **DXSafe Administrador do Token**



3. Clique duas vezes no nome do token na janela que abrir.

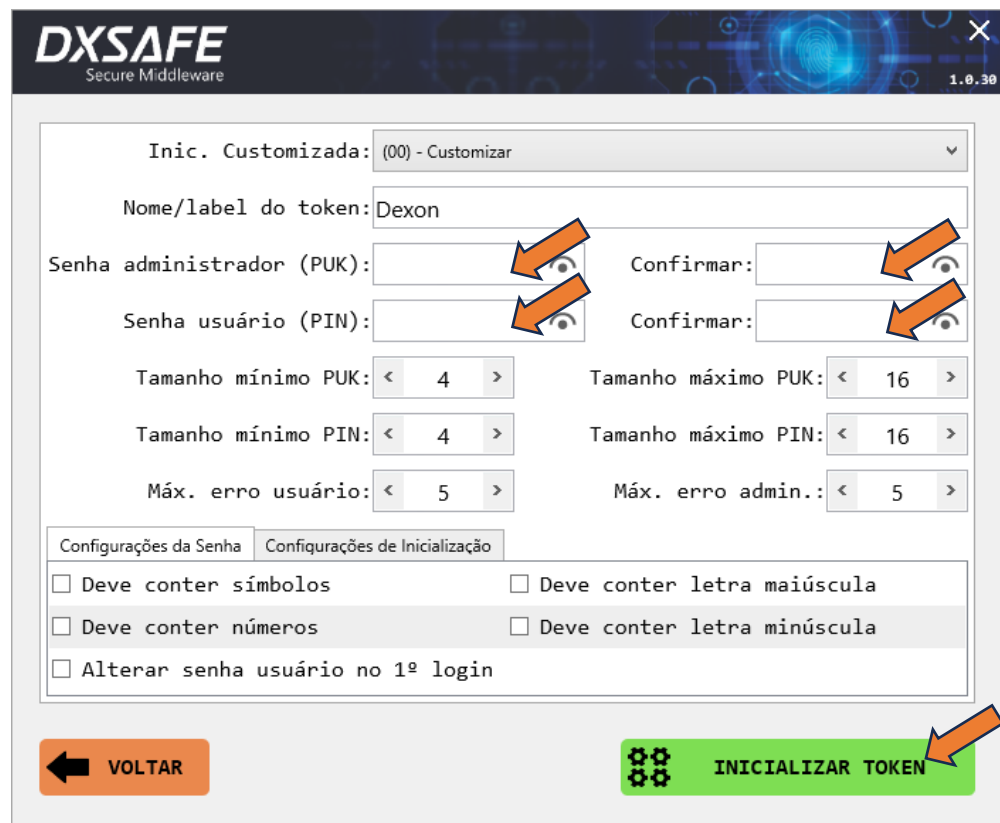


4. No menu da janela que abrir, clique em “Token > Inicializar Token”



5. Na janela que abrir, preencha os campos abaixo e clique em “inicializar token”.

- Nome/label do token** – nome para identificar o token. Pode ser qualquer nome a sua escolha;
- Senha administrador (PUK)**: senha de administração. De 4 a 16 caracteres;
- Senha de usuário (PIN)**: senha de uso do token. De 4 a 16 caracteres;



3. Processo de emissão

A emissão de um certificado digital AC Defesa através da Emissão Simplificada ocorre em 3 passos básicos:

1. Busca dos dados e Solicitação;
2. Verificação e Aprovação; e
3. Geração do par de chaves e Instalação do certificado.

3.1. Passo 1 - Busca dos dados e solicitação

Para solicitar um certificado, o militar interessado (futuro dono do certificado) deve acessar um dos módulos da aplicação (Módulo de Solicitação) que irá acessar a base de dados pessoais e biométricos da respectiva Força Singular e, caso todos os dados necessários estejam presentes, disponibilizar funcionalidade de realizar uma nova solicitação.

Para militares do Exército Brasileiro, o solicitante deverá acessar, a partir da EBNet, o endereço <https://certificadodigital.eb.mil.br/>



The screenshot shows the 'AC DEFESA' application interface. At the top, there is a navigation bar with 'Solicitações' and 'Nova Solicitação'. Below the navigation bar, the text 'as Solicitações' is visible. A warning message in yellow states: 'Atenção: O número da solicitação não é a senha. Caso você não tenha anotado ou perdeu sua senha, será necessário fazer uma nova solicitação.' Below the warning is a table with the following data:

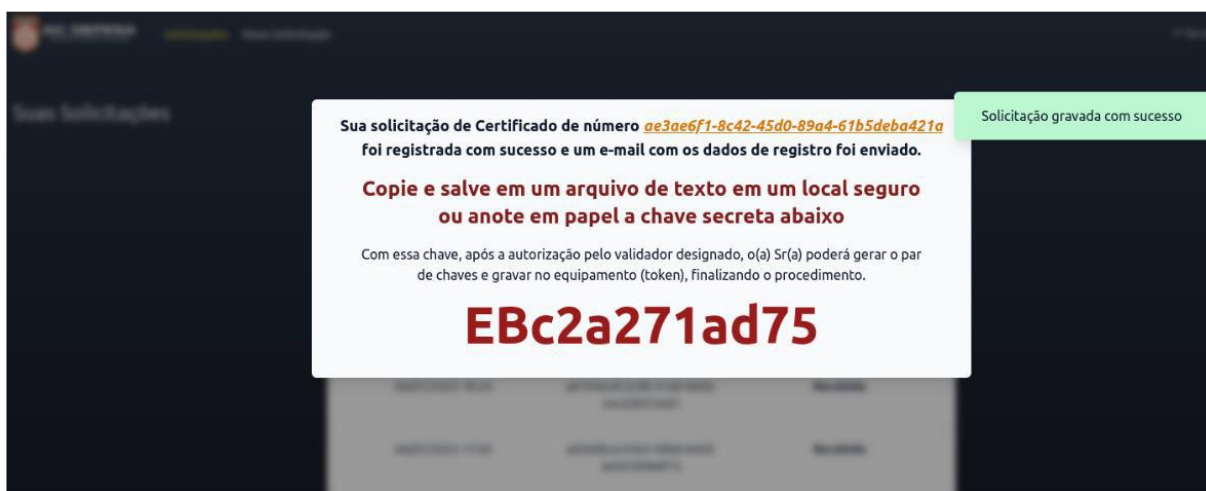
DATA	NÚMERO (NÃO É A SENHA)	STATUS
16/06/2023 14:38	c45ccc18-a3ac-4552-9476-9e3b512d8860	Revogada
20/06/2023 12:19	d51ede73-1f8a-438f-aae8-3a326592d18c	Emitida Solicitar Revogação
20/06/2023 15:30	feef431e-a4a3-4ef2-a048-b62503a8c70b	Recebida
20/06/2023 15:31	efe0ba0b-dc20-4720-aa9e-9176e602993b	Aprovada (Acessar Módulo 2)
20/06/2023 18:06	4fb423f9-e5ae-43a9-aede-944c857a5de4	Recebida

At the bottom of the table, there is a pagination control showing '1 2 3 >'.

Este módulo também disponibiliza a lista de solicitações anteriores e permite que o militar interessado revogue um certificado emitido pela Emissão Simplificada.

Após realizar a solicitação, o militar interessado recebe a informação de uma chave de acesso único. Neste momento, o militar deve tomar nota ou guardar a chave em armazenamento seguro, pois ela será utilizada no passo 3 (Emissão e Instalação).

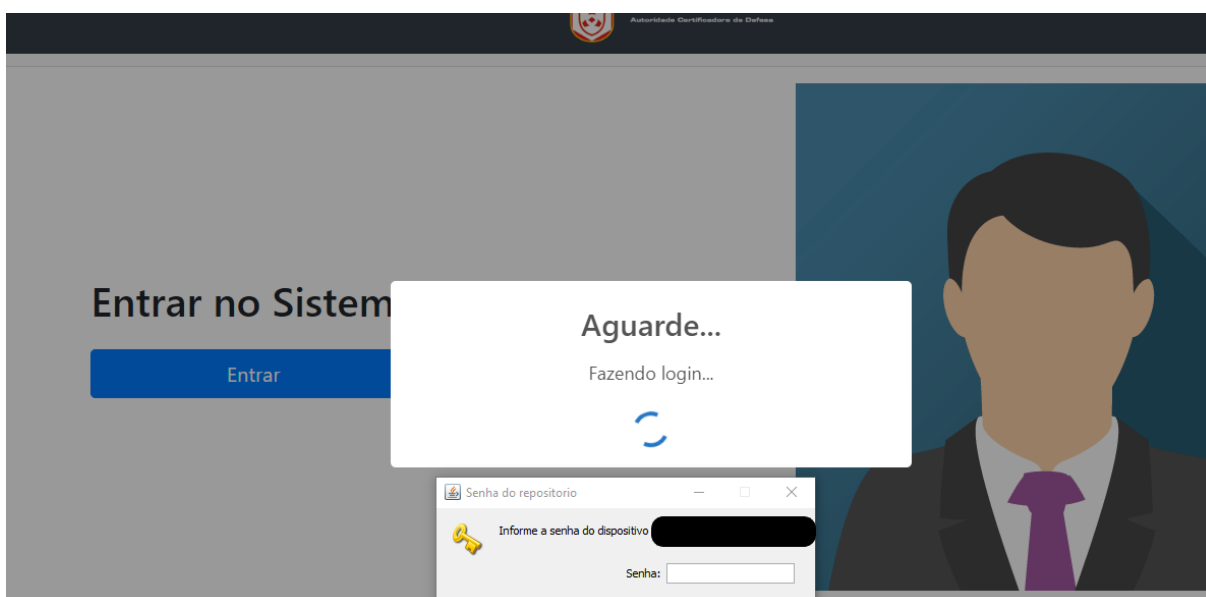
O Autorizador Designado para aquela solicitação, receberá uma mensagem via e-mail informando que há uma solicitação de certificado a ser tratada.



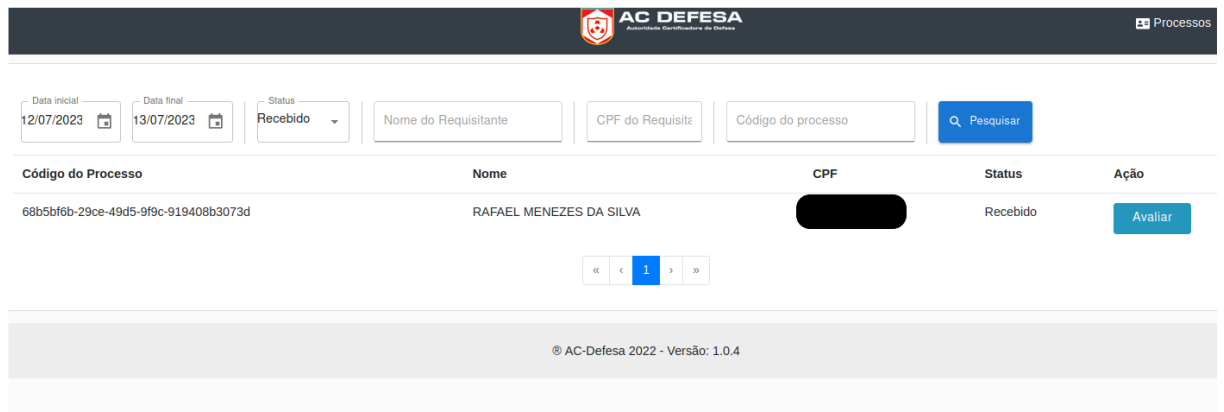
3.2. Passo 2 - Verificação e Aprovação

Neste passo, o Autorizador Designado visualiza as solicitações que deve tratar, realiza a conferência dos dados e pode aprovar ou rejeitar a solicitação. Para realizar o login e a aprovação ou rejeição, o Autorizador deverá utilizar seu certificado digital próprio. Dessa forma, a máquina utilizada pelo Autorizador deverá estar preparada para usar o seu certificado digital conforme descrito no **item 2.1** deste guia.

O Autorizador deverá acessar o endereço eletrônico na Internet <https://ar-eletronica.acdefesa.mil.br/> e clicar no botão “Entrar” já com o seu token contendo o seu certificado digital inserido no computador.




Ao efetuar o *login*, o Autorizador Designado irá encontrar uma lista de solicitações a serem tratadas por ele.



The screenshot shows the AC DEFESA web interface. At the top, there is a header with the logo and the text "AC DEFESA" and "Processos". Below the header, there is a search form with fields for "Data inicial" (12/07/2023), "Data final" (13/07/2023), "Status" (Recebido), "Nome do Requirante", "CPF do Requirite", and "Código do processo". A "Pesquisar" button is located to the right of the search fields. Below the search form, there is a table with the following columns: "Código do Processo", "Nome", "CPF", "Status", and "Ação". The table contains one row with the following data: "68b5bf6b-29ce-49d5-9f9c-919408b3073d", "RAFAEL MENEZES DA SILVA", a redacted CPF, "Recebido", and an "Avaliar" button. Below the table, there is a pagination control showing "1" of 1 items. At the bottom of the page, there is a footer with the text "© AC-Defesa 2022 - Versão: 1.0.4".

Clicando em avaliar ele tem acesso aos dados do usuário e deverá **confrontar esses dados com os constantes na base de dados pessoais** da Força Singular correspondente e se o solicitante faz jus ao certificado, de acordo com as regras específicas de cada Força.

Por fim, para autorizar será solicitada sua senha do token por duas vezes: uma para assinar o Termo de Titularidade a ser gerado para o solicitante e a outra para aprovar, de fato, a solicitação.



The screenshot shows a dialog box titled "Autorizar" with a question mark icon. The text inside the dialog box reads "Deseja autorizar o processo?". Below the text, there are two buttons: "Sim" (blue) and "Não" (red).

3.3. Passo 3 - Geração do par de chaves e instalação do certificado

Neste momento, o solicitante deve-se acessar o sistema de emissão simplificada a fim de gerar o par de chaves criptográficas no token DXToken e instalar o certificado digital no token. Para isso, ele deverá realizar os seguintes procedimentos:

1. Entrar no site de solicitação pela EBNET (<https://certificadodigital.eb.mil.br>) e clicar no botão “Acessar Módulo 2” ou acessar diretamente o link recebido no e-mail que informou sobre a autorização da solicitação.

Data	Número (não é a senha)	Status
12/09/2023	4f77f0aa-1f57-4d2e-a1d0-c07c01ea2304	Aprovada Acessar Módulo 2

OU

AC DEFESA
Autoridade Certificadora de Defesa

SOLICITAÇÃO APROVADA

Olá [nome], sua solicitação de certificado digital de número d51ede73-1f8a-438f-aae8-3a326592d18c foi **aprovada**. Para gerar seu certificado, acesse o endereço abaixo utilizando a **chave de acesso**, que você anotou ou imprimiu no momento da solicitação e siga as orientações (passo-a-passo) do sistema.

<https://ecds.acdefesa.mil.br:6443/issue/d51ede73-1f8a-438f-aae8-3a326592d18c/login>

2. Fazer o login com a chave de acesso única fornecida no momento da solicitação

Número do processo: 4f77f0aa-1f57-4d2e-a1d0-c07c01ea2304

Senha de acesso: [campo oculto]

Logar

Sua solicitação de Certificado de Acesso...
Para solicitar o par de chaves criptográficas, é necessário utilizar o token de segurança fornecido.
Digite e valide seu PIN do token de acesso no site de acesso do sistema em seguida a chave de acesso fornecida.
Caso não tenha, solicite a chave de acesso para o módulo de geração de chaves criptográficas no par de chaves criptográficas e equipamentos de acesso, disponibilizados no equipamento.

EBfec5e4053

3. Clicar em **Gerar Par de Chaves** - Será solicitado o PIN do token;
Observação: Será solicitado o PIN novamente para assinar o Termo de Titularidade;
4. Clicar em **Instalar Certificado** - Será solicitado o PIN do token.

4. Conclusão

Seguindo os passos descritos acima, o solicitante deverá ter o seu certificado digital gerado e instalado no token DXToken entregue.

Caso haja dúvidas ou problemas na execução desses passos, favor entrar em contato com a Autoridade de Registro da AC Defesa, por meio do endereço de correio eletrônico **suporte@acdefesa.mil.br**.