AUTORIDADE CERTIFICADORA DE DEFESA

EMISSÃO SIMPLIFICADA

Guia de Orientações

Julho 2024

Índice

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.

Módulo 1: Módulo de Solicitação de Certificados

Módulo 2: Módulo de Aprovação e Emissão de Certificados

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.

2. Preparação do Ambiente

2.1 Softwares Necessários

Para a execução dos passos descritos no item 3. Processo de Emissão é **necessária a instalação prévia de três softwares específicos**, a saber:

1. Driver do Token;
2. Ferramenta de Administração de Token e
3. SDK-Desktop (versão 1.0.35 ou superior).

Todos esses aplicativos podem ser encontrados na área de download do site da AC Defesa (https://www.acdefesa.mil.br/index.php/downloads) e os itens 1 e 2 são instalados

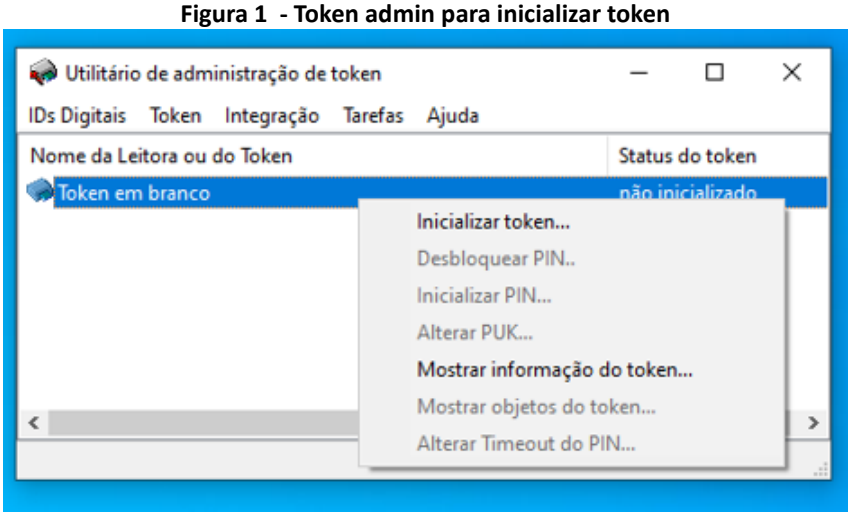
juntos baixando o **Software do token (Driver e Ferramenta de Administração - Token Admin)**, através de nosso site.

Atenção: Caso esteja utilizando o navegador **Firefox,** após baixar e instalar as aplicações é necessário o carregamento de uma biblioteca chamada libaetpkss1.dll. O passo a passo em PDF para esta ação pode ser encontrado em https://www.acdefesa.mil.br/images/manuais/orientacoes.pdf.

2.2 Preparação da Mídia

Caso seu token esteja em branco ele deverá ser inicializado. Para tanto, abra o aplicativo *Token Admin* e clique com o botão direito no token em branco e clique em **inicializar token.**

Figura 1 - Token admin para inicializar token



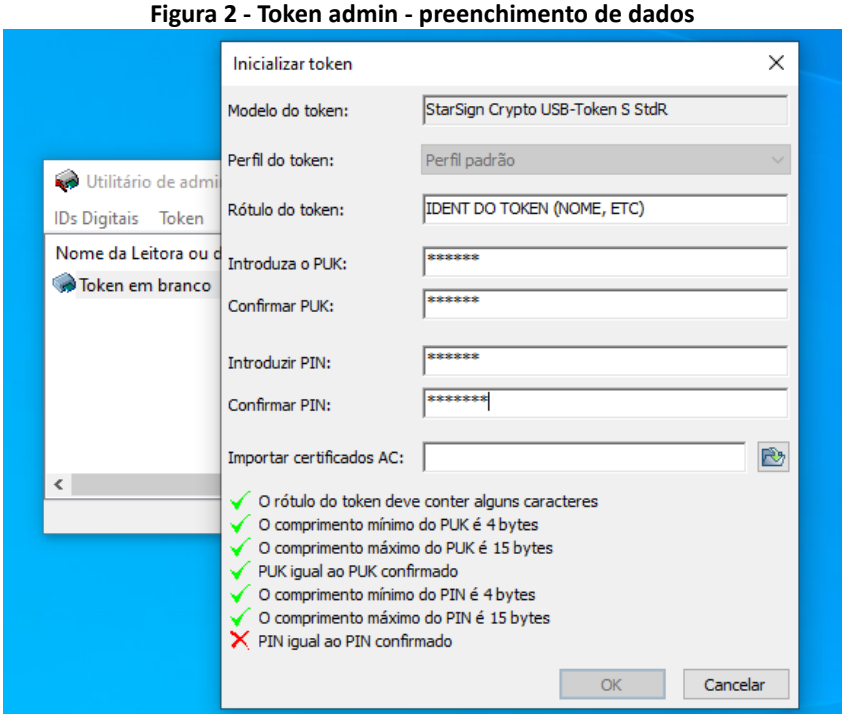
Atenção: Caso seu token já possua um certificado, previamente inserido ou já tenha sido inicializado, a opção pode se chamar "apagar token", dependendo de sua versão do Token Admin. **Inicializar ou apagar token** remove todos os certificados que possam existir na mídia, por isso deve ser executado com extrema cautela.

Após isso, você deverá preencher os seguintes dados, obrigatoriamente:

- **Rótulo do token:** o nome a ser mostrado para acessar o token. Geralmente se utiliza o nome completo do titular;

- **PUK:** (senha utilizada para recuperação da mídia, caso você esqueça o PIN ou, durante o uso, erre o PIN mais de 3 vezes em uso) e
- **PIN**: senha de uso do token (para assinatura, login etc.).

Figura 2 - Token admin - preenchimento de dados



3. Processo de Emissão

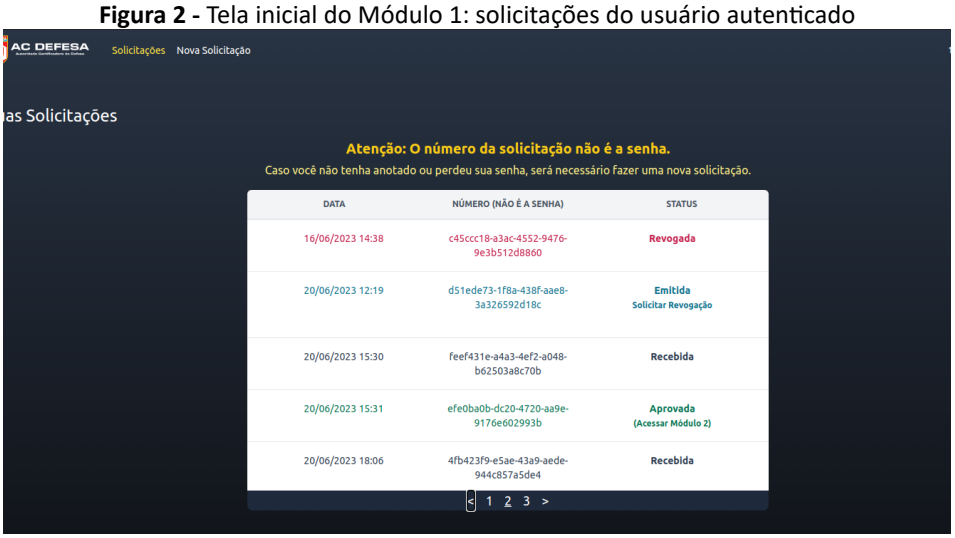
A emissão de um certificado digital AC Defesa através da Emissão Simplificada ocorre em 3 passos básicos:

1. **Busca** dos dados e **Solicitação**;
2. **Verificação** e **Aprovação** e
3. **Emissão** e **Instalação.**

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 (chamado de Módulo 1) 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**.

Figura 2 - Tela inicial do Módulo 1: solicitações do usuário autenticado



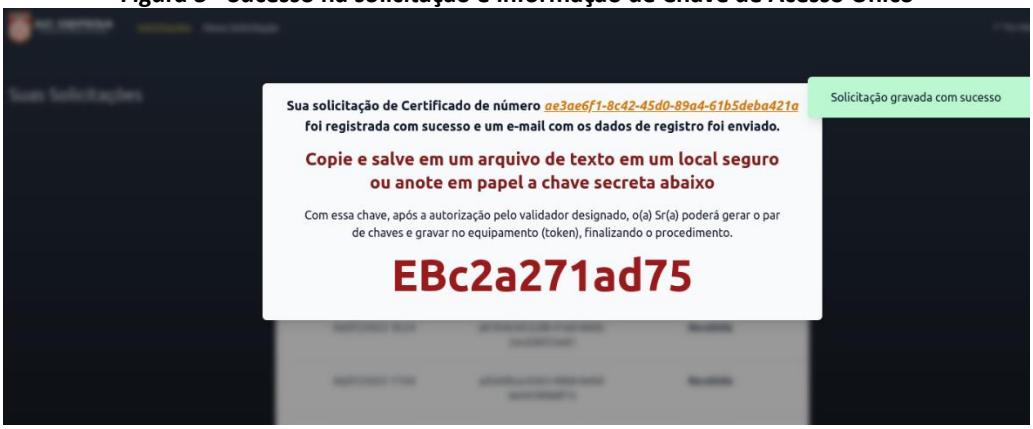
Fonte: captura de tela do Módulo 1 extraída pelo autor no navegador Google Chrome

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.

Figura 3 - Sucesso na solicitação e informação de Chave de Acesso Único



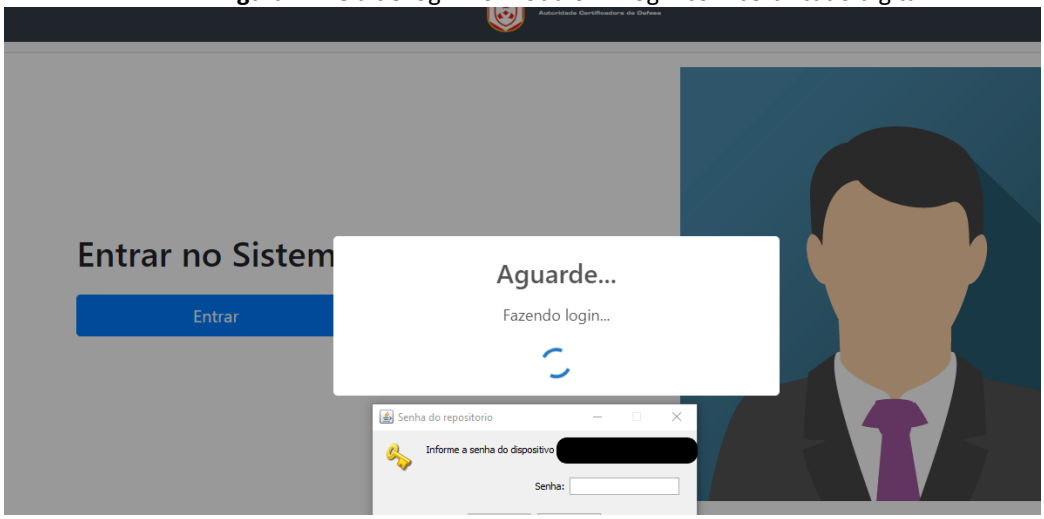
Fonte: captura de tela do Módulo 1 extraída pelo autor no navegador Google Chrome

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, a máquina do Autorizador deve possuir os softwares **Token Administrator e SDK-Desktop** versão 1.0.35 ou superior instalados

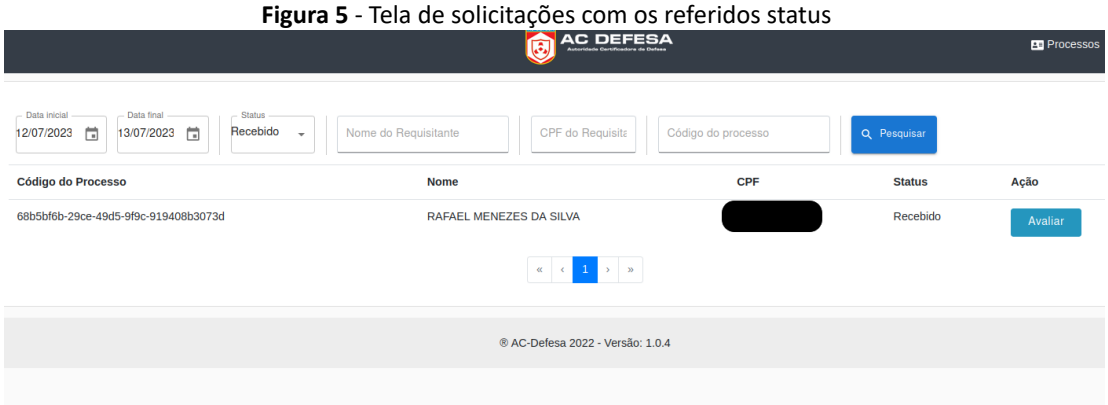
Figura 4 - Tela de login no Módulo 2 - login com certificado digital



Fonte: captura de tela do Módulo 2 extraída pelo autor no navegador Google Chrome

Ao acessar o Módulo 2, utilizando como forma de login seu próprio certificado digital, o Autorizador Designado irá encontrar uma lista de solicitações a serem tratadas por ele.

Figura 5 - Tela de solicitações com os referidos status

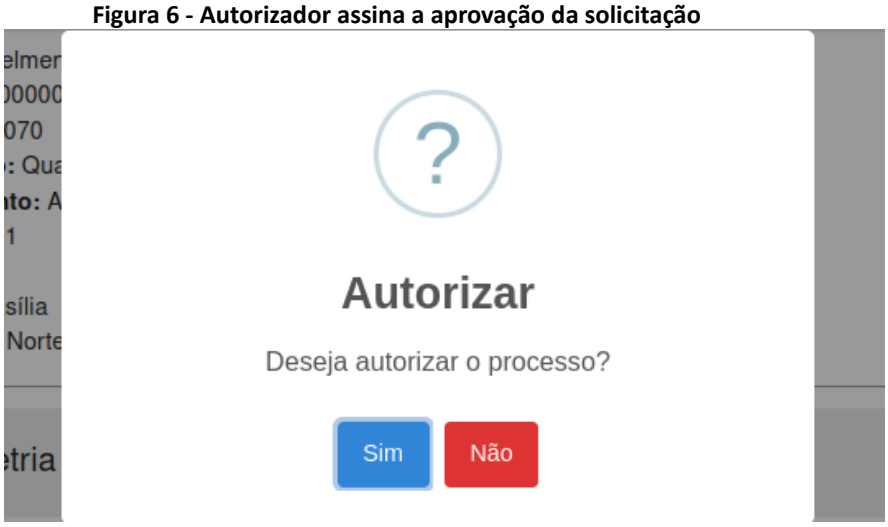


Fonte: captura de tela do Módulo 2 extraída pelo autor no navegador Google Chrome

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.

Figura 6 - Autorizador assina a aprovação da solicitação



Fonte: captura de tela do Módulo 2 extraída pelo autor no navegador Google Chrome

Atenção: O autorizador é responsável pela exatidão dos dados, por isso deve realizar a conferência e o confrontamento dos dados do solicitante com o constante no SICAPEx, assinando digitalmente Termo que confirma essa conferência, ao aprovar.

Passo 3 – Emissão e Instalação

Neste passo, o militar solicitante, após ter sua solicitação aprovada irá preparar a mídia para receber o certificado e realizar a geração do par de chaves (emissão) e instalação do certificado no token. Para realizar o login e a aprovação ou rejeição, a máquina do usuário deve possuir os softwares **Token Administrator** e **SDK-Desktop** versão 1.0.35 ou superior instalados.

A mídia a ser utilizada deve ter sido previamente inicializada (zerada) através do Token Administrator.

Figura 7 - Captura de tela: e-mail informando aprovação

Fonte: captura de tela e-mail extraída pelo autor no navegador Google Chrome

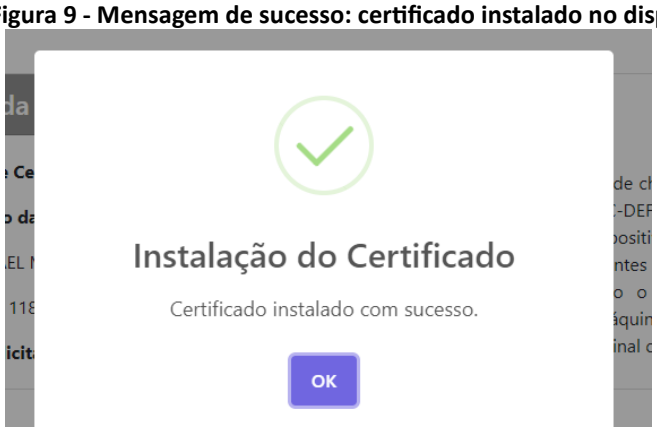
Utilizando o link (presente no e-mail recebido após a aprovação ou em link mostrado na lista de solicitações do Módulo 1) e a senha de acesso único gerada no momento da solicitação, o usuário acessa o Módulo 2 e é direcionado para a geração do par de chaves e instalação do certificado.

Figura 8 - Tela de autenticação por parte do solicitante

Fonte: captura de tela do Módulo 2 extraída pelo autor no navegador Google Chrome

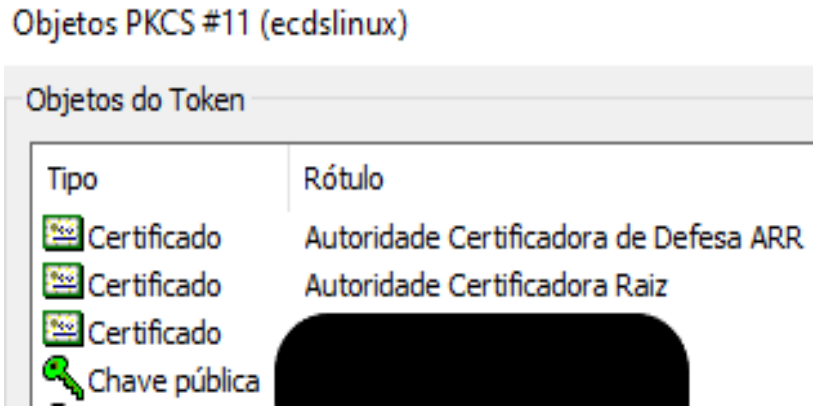
Ao final do processo o usuário recebe uma mensagem de sucesso e pode utilizar o Token Administrator para verificar o certificado e as chaves geradas.

Figura 9 - Mensagem de sucesso: certificado instalado no dispositivo



Fonte: captura de tela do Módulo 2 extraída pelo autor no navegador Google Chrome

Figura 10 - Objetos do token



Fonte: captura de tela do Token admin extraída pelo autor

Os passos descritos *para a emissão constantes neste* guia também são cobertos por vídeos tutoriais em https://certificadodigital.eb.mil.br/tutoriais


AC DEFESA