

**MANUAL DE TROCA E DESBLOQUEIO DE SENHA PIN DO
TOKEN SAFENET ETOKEN 5110 FIPS (Linux)
Versão 1.0**

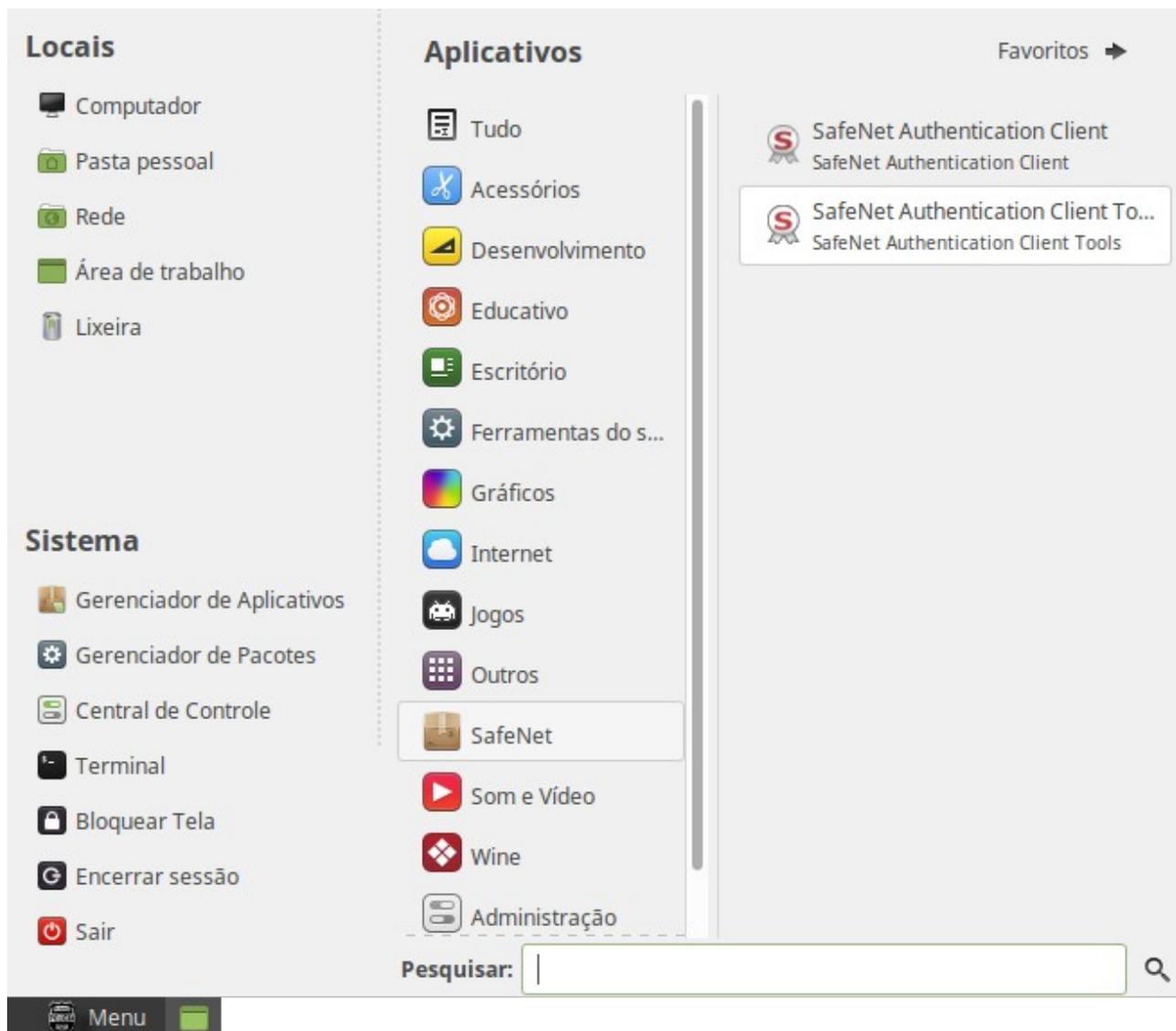
Sumário

Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools).....	3
Procedimento de alteração da senha de usuário (PIN) do token SafeNet.....	5
Procedimento para visualizar tentativas restantes dos códigos PIN e PUK.....	7
Procedimento para visualizar a data de emissão/validade do certificado.....	9
Desbloqueio da senha de usuário (PIN) utilizando a senha de administrador (PUK)	10
Revogação do certificado digital.....	13
Procedimento para revogação do certificado digital pelo site.....	14
Procedimento para revogação de certificado pessoalmente na AR celepar.....	16
Glossário.....	17

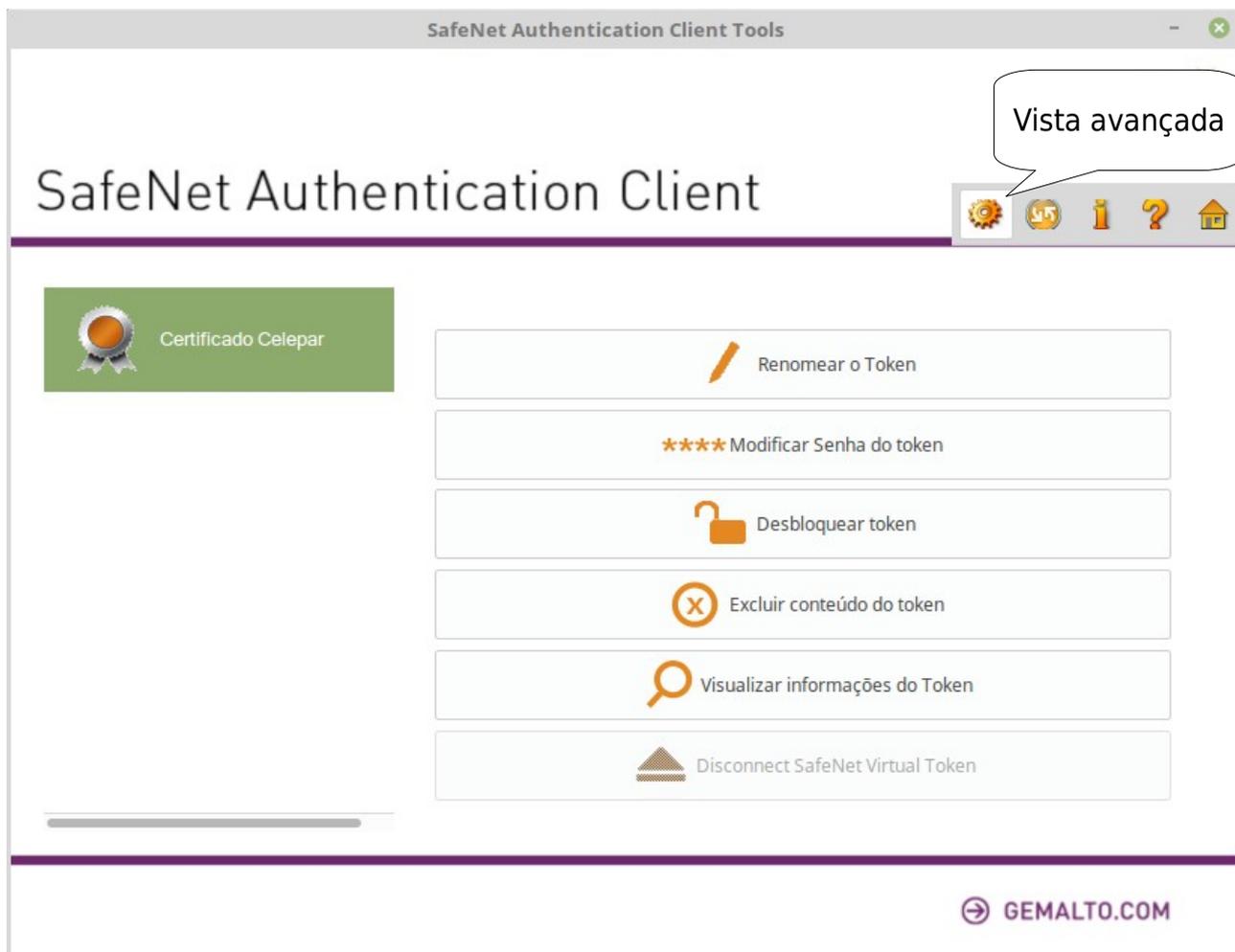
Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)

O aplicativo SafeNet Authentication Client Tools é utilizado para gerenciar tokens da SafeNet, com ele podemos visualizar informações do token e do certificado, alterar/desbloquear os códigos PIN e PUK, importar cadeias de certificados e até mesmo gerenciar opções do token como requisitos de complexidade e validade da senha.

1. Clique no botão Iniciar, localizar o gerenciador na lista de programas com o nome: **SafeNet Authentication Client Tools** - Caminho: Clique em "**Menu**" > "**SafeNet**" > "**SafeNet Authentication Client Tools**".



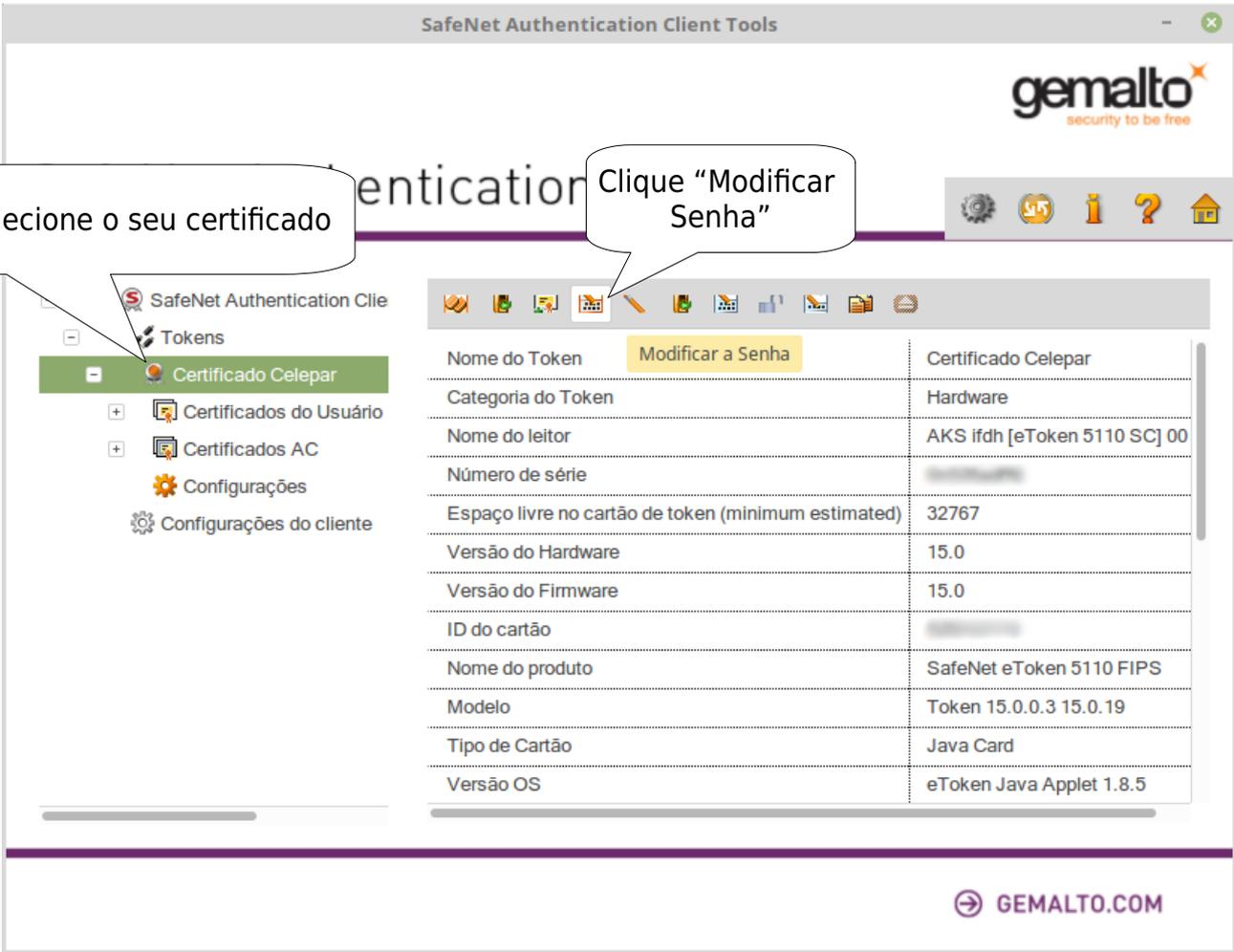
2. Clique no ícone da engrenagem para acessar a *Vista avançada*.



Procedimento de alteração da senha de usuário (PIN) do token SafeNet

A execução deste procedimento é fortemente recomendada logo após a aquisição do token, pois seu certificado digital é um documento com validade jurídica e a maioria dos sistemas do Estado e permite acesso a informações pessoais e sensíveis.

1. Abra o gerenciador do SafeNet eToken no modo avançado conforme descrito em **Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)**.
2. Selecione o seu certificado - na maioria dos casos estará nomeado como *Certificado Celepar* por padrão - e clique em *Modificar a Senha*.

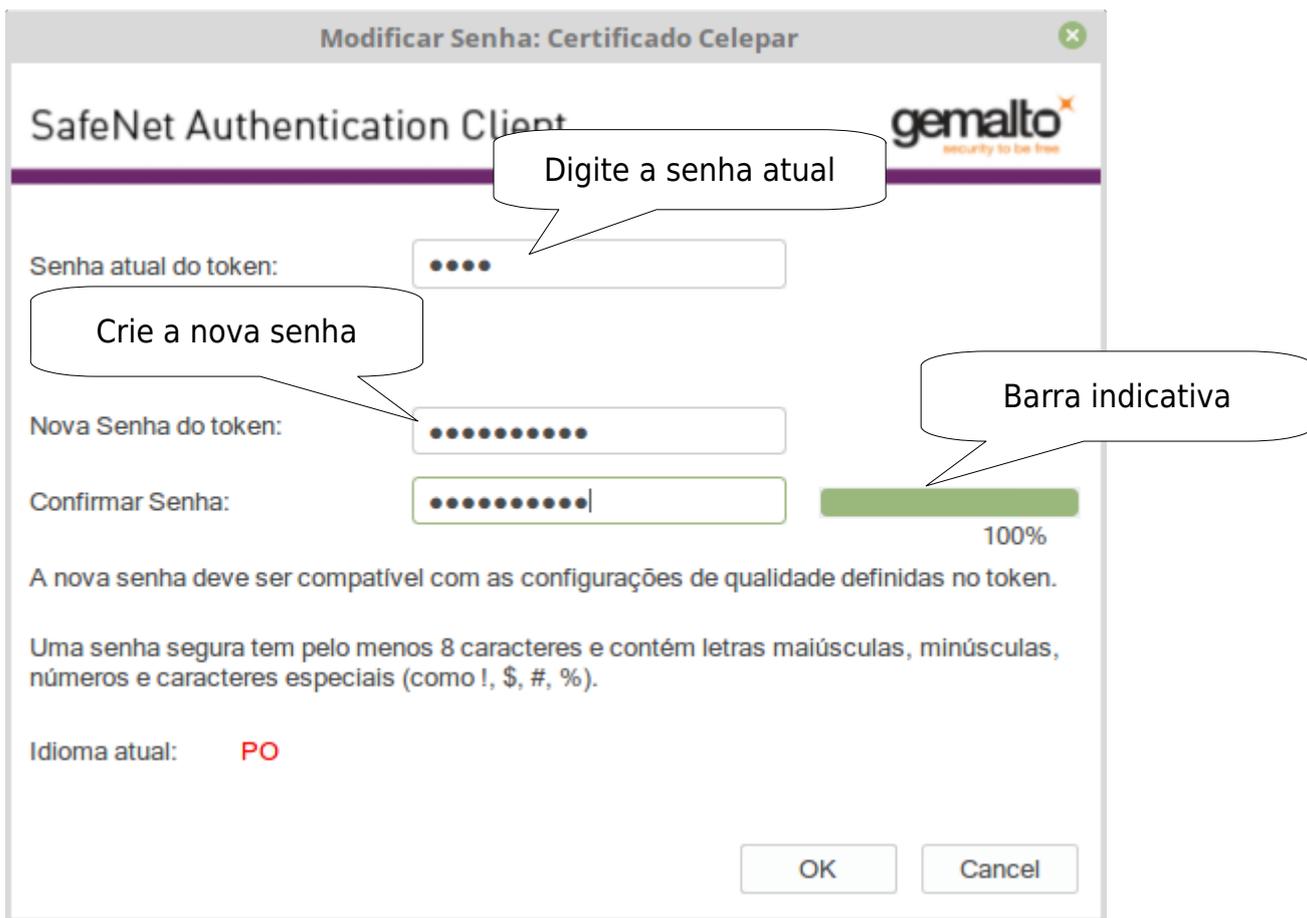


The screenshot shows the 'SafeNet Authentication Client Tools' window. On the left, a tree view under 'Tokens' has 'Certificado Celepar' selected. A callout bubble points to this selection with the text 'Selecione o seu certificado'. In the main area, a table displays token details. A yellow button labeled 'Modificar a Senha' is positioned above the table. A callout bubble points to this button with the text 'Clique "Modificar Senha"'. The table contains the following data:

Nome do Token	Certificado Celepar
Categoria do Token	Hardware
Nome do leitor	AKS ifdh [eToken 5110 SC] 00
Número de série	
Espaço livre no cartão de token (minimum estimated)	32767
Versão do Hardware	15.0
Versão do Firmware	15.0
ID do cartão	
Nome do produto	SafeNet eToken 5110 FIPS
Modelo	Token 15.0.0.3 15.0.19
Tipo de Cartão	Java Card
Versão OS	eToken Java Applet 1.8.5

The Gemalto logo and 'GEMALTO.COM' are visible at the bottom of the interface.

3. Digite a senha atual, a nova senha, confirme a nova senha e em seguida clique em OK. A senha será aceita desde que a barra indicativa complete 100%, mas é recomendável o uso de uma senha com no mínimo 8 caracteres, dentre eles pelo menos duas letras, dois números, e um caractere especial (!@#\$?%°).



Modificar Senha: Certificado Celepar

SafeNet Authentication Client

gemalto
security to be free

Senha atual do token:

Digite a senha atual

Crie a nova senha

Nova Senha do token:

Confirmar Senha:

Barra indicativa

100%

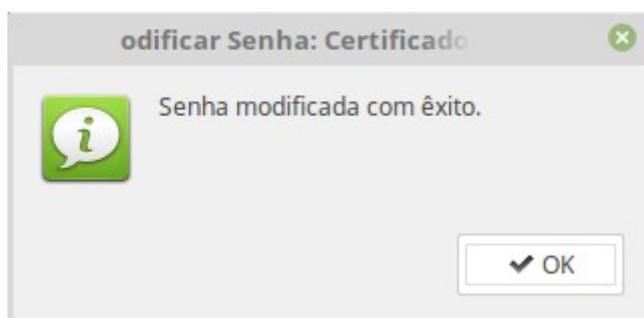
A nova senha deve ser compatível com as configurações de qualidade definidas no token.

Uma senha segura tem pelo menos 8 caracteres e contém letras maiúsculas, minúsculas, números e caracteres especiais (como !, \$, #, %).

Idioma atual: PO

OK Cancel

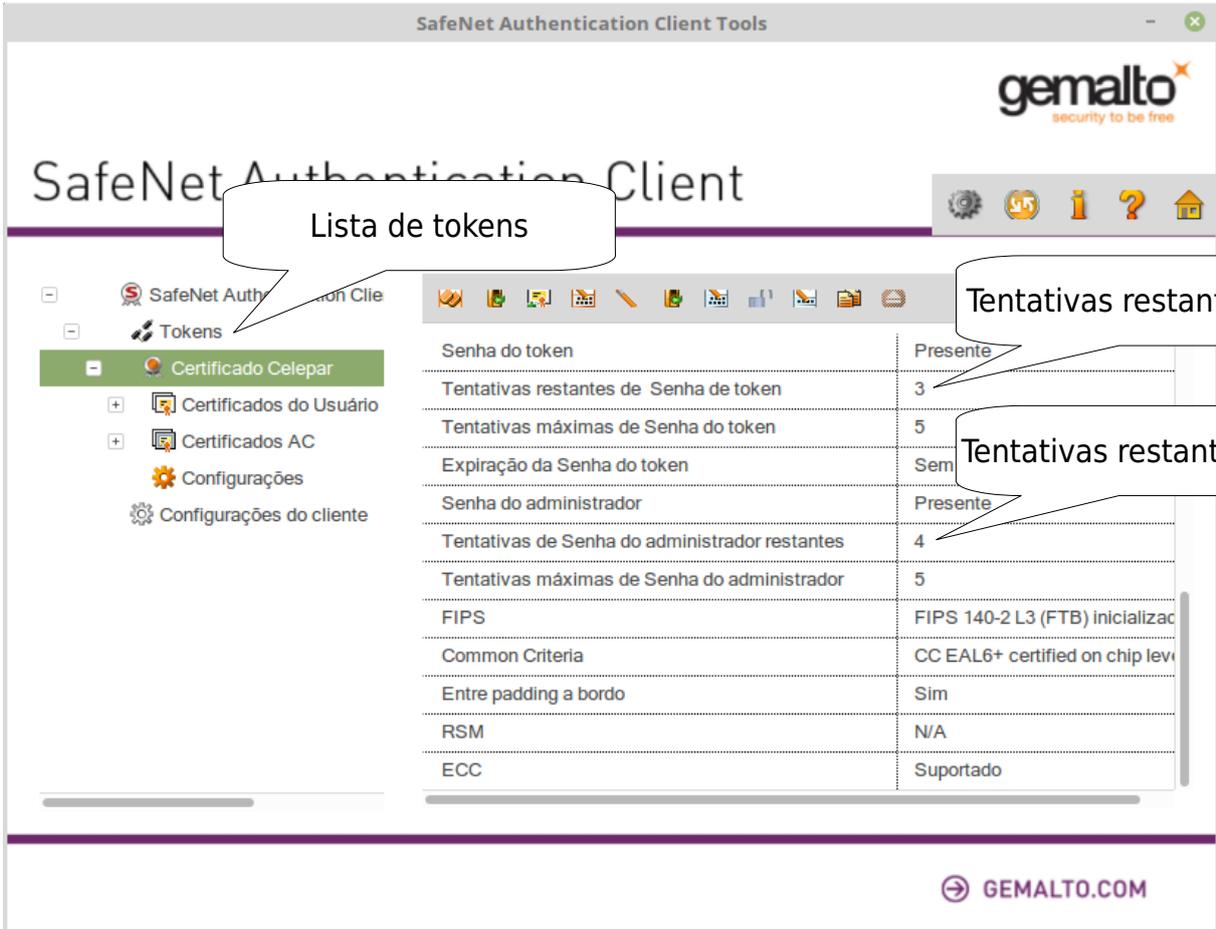
4. Pronto. Sua senha foi alterada com sucesso.



Procedimento para visualizar tentativas restantes dos códigos PIN e PUK

É possível verificar tentativas de acesso às informações do token restantes por meio da interface de gerenciamento. *Senha do token* se refere ao código PIN e *Senha do administrador* ao PUK.

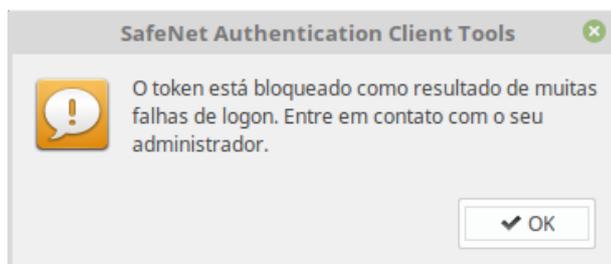
1. Abra o gerenciador do SafeNet eToken no modo avançado conforme descrito em **Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)**.
2. Expanda a lista de *Tokens* e selecione o seu token, por padrão, tokens fornecidos pela celepar são nomeados como "*Certificado Celepar*". Em seguida abaixe a barra de rolagem até o fim da página.



The screenshot shows the 'SafeNet Authentication Client Tools' window. The left sidebar has a 'Tokens' section expanded, with 'Certificado Celepar' selected. The main area displays a table of token details. Callouts point to specific values in the table: 'Lista de tokens' points to the sidebar, 'Tentativas restantes (PIN)' points to the value '3', and 'Tentativas restantes (PUK)' points to the value '4'.

Senha do token	Presente
Tentativas restantes de Senha de token	3
Tentativas máximas de Senha do token	5
Expiração da Senha do token	Sem
Senha do administrador	Presente
Tentativas de Senha do administrador restantes	4
Tentativas máximas de Senha do administrador	5
FIPS	FIPS 140-2 L3 (FTB) inicializac
Common Criteria	CC EAL6+ certified on chip lev
Entre padding a bordo	Sim
RSM	N/A
ECC	Suportado

Caso ocorram muitas falhas na digitação do PIN (padrão: 5), o campo *Tentativas restantes de Senha do Token* vai apresentar o valor '0'. O token ficará inutilizável e ao tentar logar ou alterar a senha, a mensagem abaixo será exibida:

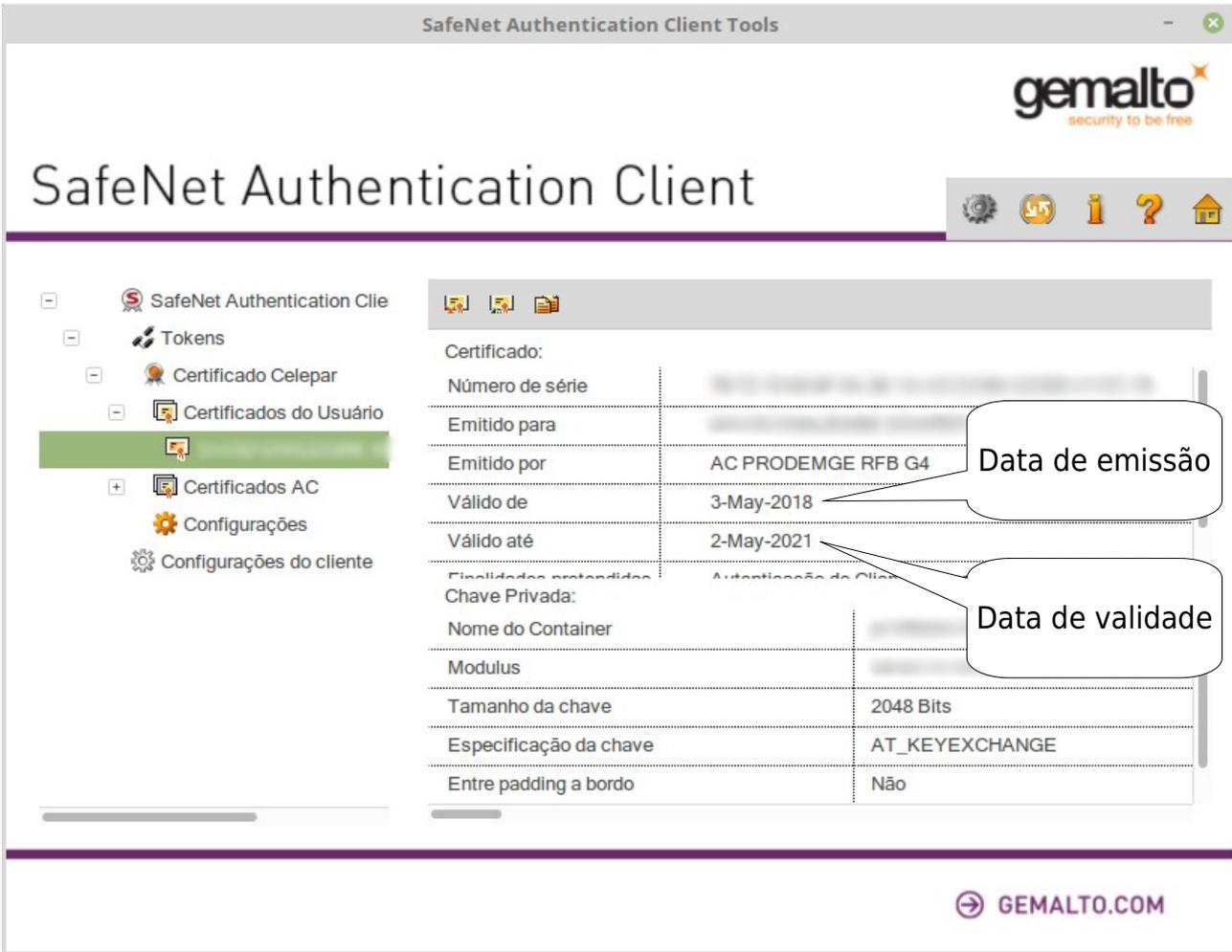


Se este comportamento for aplicável, siga as instruções para **Procedimento para desbloqueio da senha de usuário (PIN) utilizando a senha de administrador (PUK)** descritas a partir da página seguinte.

Caso ambos os campos *Tentativas restantes de Senha do Token* e *Tentativas de Senha do administrador restantes* estejam com o valor '0', o token ficará inutilizável permanentemente, nesse caso é importante realizar o **Procedimento de revogação do certificado**, e para a aquisição de um novo certificado digital siga o **Procedimento de aquisição do certificado digital**.

Procedimento para visualizar a data de emissão/validade do certificado

1. Abra o gerenciador do SafeNet eToken no modo avançado conforme descrito em **Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)**.
2. Expanda a lista de *Tokens* e selecione o seu dispositivo, por padrão tokens fornecidos pela celepar são nomeados como “*Certificado Celepar*”. Em seguida expanda os *Certificados do Usuário* e selecione seu certificado. Nesse momento as informações de data de emissão e validade estarão visíveis.



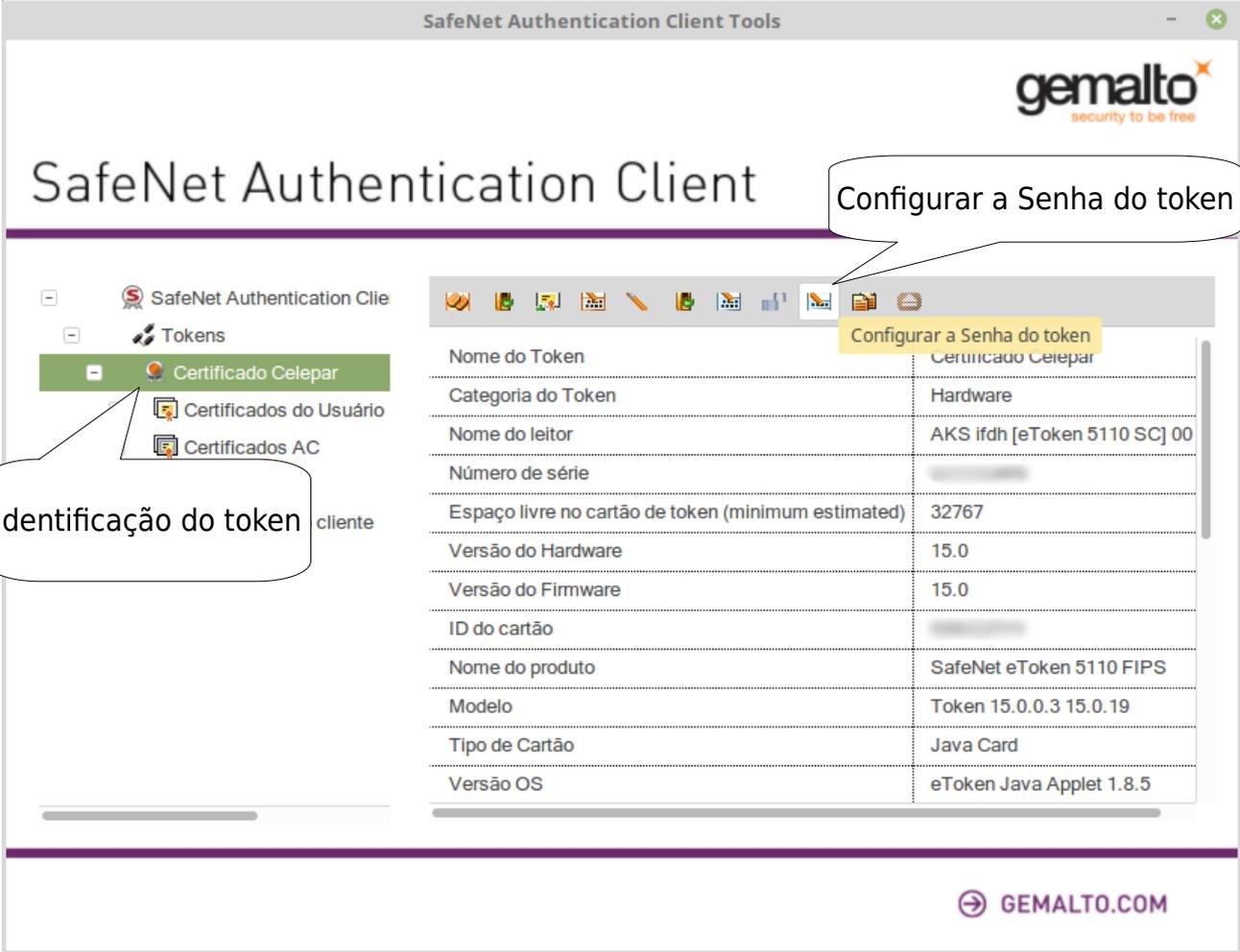
The screenshot displays the 'SafeNet Authentication Client Tools' window. The main title is 'SafeNet Authentication Client'. On the left, a navigation tree shows 'Tokens' expanded to 'Certificados do Usuário'. The main area shows a table of certificate details:

Certificado:	
Número de série	
Emitido para	
Emitido por	AC PRODEMG E RFB G4
Válido de	3-May-2018
Válido até	2-May-2021
Finalidades pretendidas	Autenticação de Cliente
Chave Privada:	
Nome do Container	
Modulus	
Tamanho da chave	2048 Bits
Especificação da chave	AT_KEYEXCHANGE
Entre padding a bordo	Não

Two callout boxes highlight the 'Válido de' (3-May-2018) and 'Válido até' (2-May-2021) fields, labeled 'Data de emissão' and 'Data de validade' respectively. The Gemalto logo and 'GEMALTO.COM' are also visible.

Procedimento para desbloqueio da senha de usuário (PIN) utilizando a senha de administrador (PUK)

1. Abra o gerenciador do SafeNet eToken no modo avançado conforme descrito em **Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)**.
2. Selecione seu token - por padrão, tokens fornecidos pela celepar são nomeados como "Certificado Celepar" - e clique em *Configurar a Senha do token*.



The screenshot displays the 'SafeNet Authentication Client Tools' window. The title bar reads 'SafeNet Authentication Client Tools'. The main header area features the 'gemalto' logo with the tagline 'security to be free' and the text 'SafeNet Authentication Client'. On the left, a tree view shows 'SafeNet Authentication Client' expanded to 'Tokens', with 'Certificado Celepar' selected. A callout bubble labeled 'Identificação do token' points to this selection. The main panel shows a table of token details for 'Certificado Celepar'. A callout bubble labeled 'Configurar a Senha do token' points to a button in the toolbar above the table.

Nome do Token	Certificado Celepar
Categoria do Token	Hardware
Nome do leitor	AKS ifdh [eToken 5110 SC] 00
Número de série	
Espaço livre no cartão de token (minimum estimated)	32767
Versão do Hardware	15.0
Versão do Firmware	15.0
ID do cartão	
Nome do produto	SafeNet eToken 5110 FIPS
Modelo	Token 15.0.0.3 15.0.19
Tipo de Cartão	Java Card
Versão OS	eToken Java Applet 1.8.5

3. Digite a senha de administrador (PUK) do SafeNet eToken e clique em **OK**.



Log on do Administrador

SafeNet Authentication Client 

Introduza a Senha do Administrador (PUK) do token

Nome do Token:

Senha Administrator (PUK):

Idioma atual: **PO**

4. Configure o novo PIN e clique em **OK**. A senha será aceita desde que a barra indicativa complete 100%.



Configurar senha: Certificado Celepar

SafeNet Authentication Client 

Senha do token:

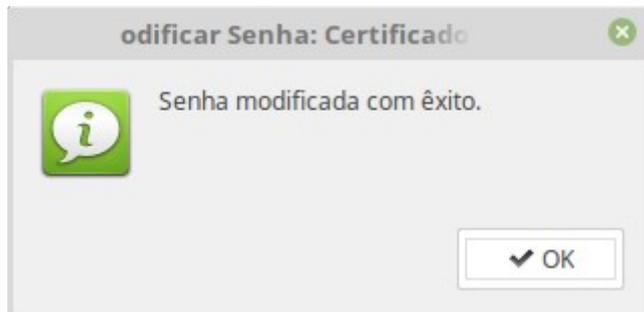
Confirmar Senha:  100%

A nova senha deve ser compatível com as configurações de qualidade definidas no token.

Uma senha segura tem pelo menos 8 caracteres e contém letras maiúsculas, minúsculas, números e caracteres especiais (como !, \$, #, %).

Idioma atual: **PO**

5. E o processo de desbloqueio está concluído.



Revogação do certificado digital

No caso de perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente ou da mídia armazenadora (token/smartcard), é importante revogar o certificado para evitar o uso indevido da sua identidade. O certificado digital é um documento com validade jurídica e permite acesso a informações pessoais, além de poder ser utilizado como forma de identificação em boa parte dos sistemas do Estado.

Você pode fazer revogar seu certificado utilizando o Procedimento para revogação do certificado digital pelo site ou o Procedimento para revogação de certificado pessoalmente na AR celepar.

Procedimento para revogação do certificado digital pelo site

Para executar esse procedimento, você deve estar munido de seu CPF e da senha de revogação do seu certificado. A senha de revogação padrão é enviada para o e-mail que você cadastrou no momento da entrega do certificado.

1. Caso não tenha alterado a senha de revogação do seu certificado, procure em sua caixa pelo e-mail da AC com a senha de revogação padrão:



Caixa de Entrada [0 / 10430] **Senha de Revogação**

prodemgecertifi..., 03/05/2018 📎 Marcar como: Não lida Importante

De:  "prodemgecertificadora@prodemge.gov.br" <prodemgecertificadora@prodemge.gov.br>
Para: 
Data: 
Assunto: **Senha de Revogação**
Anexos: cab.gif (30 KB)

 **CERTIFICADO DIGITAL PRODEMGE** 

Prezado(a) ,

Parabéns! O seu certificado e-CPF A3 com token - validade 3 anos - AC Prodemge RFB foi emitido com sucesso e está pronto para ser utilizado.

Em caso de perda, comprometimento do certificado ou outros motivos, é possível invalidar o certificado.
Para tanto é necessária a utilização de uma senha de revogação.

O seu certificado foi configurado com a seguinte senha de revogação (gerada automaticamente):



Recomendamos que a senha gerada pelo sistema seja ALTERADA.
Para modificá-la acesse a URL abaixo:

gestaoar.certisign.com.br/GestaoAR/cliente/revogacao/trocaSenha?pedido=&skinDir=PRODEMGE

Senha de revogação

2. Para saber qual portal utilizar, precisamos saber se a data de emissão do seu certificado é anterior ou posterior a 21/01/2019. Para verificar a data de emissão do seu certificado siga os passos descritos no Procedimento para visualizar a data de emissão/validade do certificado.
3. Agora munido de sua senha de revogação do certificado e CPF acesse o sistema de busca de certificados emitidos, acesse o portal conforme a data de emissão de seu certificado, preencha os campos conforme indicado, confira os dados e clique no botão *Revogar*.
 - i. Certificados com data de emissão anterior a 21/01/2019: [LINK](#)
 - ii. Certificados com data de emissão igual ou posterior a 21/01/2019: [LINK](#)



CERTIFICADO DIGITAL PRODEMGE

Busca de certificados emitidos

Preencha os campos ao lado e clique em buscar.

CPF do titular (apenas números):

Senha de revogação:

Não sou um robô  **Buscar**

Pedido: **Validade:** de 03/05/2018 a 02/05/2021 **Serial:**
CNPJ: - **E-mail:** **Status:** **Válido**
CPF:
Nome:
Produto: e-CPF A3 com token - validade 3 anos - AC Prodemge RFB
Certificado: Prodemge eCPF A3 - AC Prodemge RFB V5

Botão Revogar

ICP Brasil   **Autoridade Certificadora prodemge**

© PRODEMGE
Rua da Bahia, 2277 - Lourdes - BH/MG - CEP 30160 012
Tel: (31)3339-1251
Todos os direitos reservados. Aspectos legais e responsabilidades

Procedimento para revogação de certificado pessoalmente na AR celepar

Caso tenha perdido a senha de revogação ou esteja tendo dificuldades pelo site, o processo de revogação também pode ser feito pessoalmente no local de atendimento em que o certificado foi registrado. Para fazê-lo o titular do certificado deve comparecer ao local de atendimento com seu CPF ou CNPJ e RG. Também é necessário explicar ao agente de registro o motivo do requerimento de revogação.

Ao final do processo, será fornecido um documento contendo a solicitação de revogação e será encaminhado para o e-mail cadastrado no certificado digital a confirmação de revogação.

Glossário

Certificado digital: É a tecnologia que garante autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas. Trata-se de um documento digital utilizado para identificar pessoas e empresas no mundo virtual.

Token: É uma das mídias que podem ser utilizadas para armazenar um certificado digital (geralmente do tipo A3), um hardware capaz de gerar/armazenar chaves criptográficas que compõem os certificados digitais.

PIN: Senha de uso do token, utilizada para se autenticar em sistemas ou assinar digitalmente documentos/arquivos.

PUK: Senha administrativa, utilizada para gerenciar credenciais, desbloqueio do PIN e demais funções do token por meio.

AC: *Autoridades Certificadoras* são as entidades responsáveis pela emissão dos certificados digitais. Cada certificado é assinado digitalmente pela AC emitente, que garante que os dados constantes do certificado são verdadeiros.

AR: *Autoridades de Registro* são responsáveis pela identificação presencial do solicitante de um certificado e por autorizar a emissão do mesmo.

Agente de registro: Funcionário da Autoridade de Registro responsável por confirmar a autenticidade dos documentos pessoais e/ou da empresa.