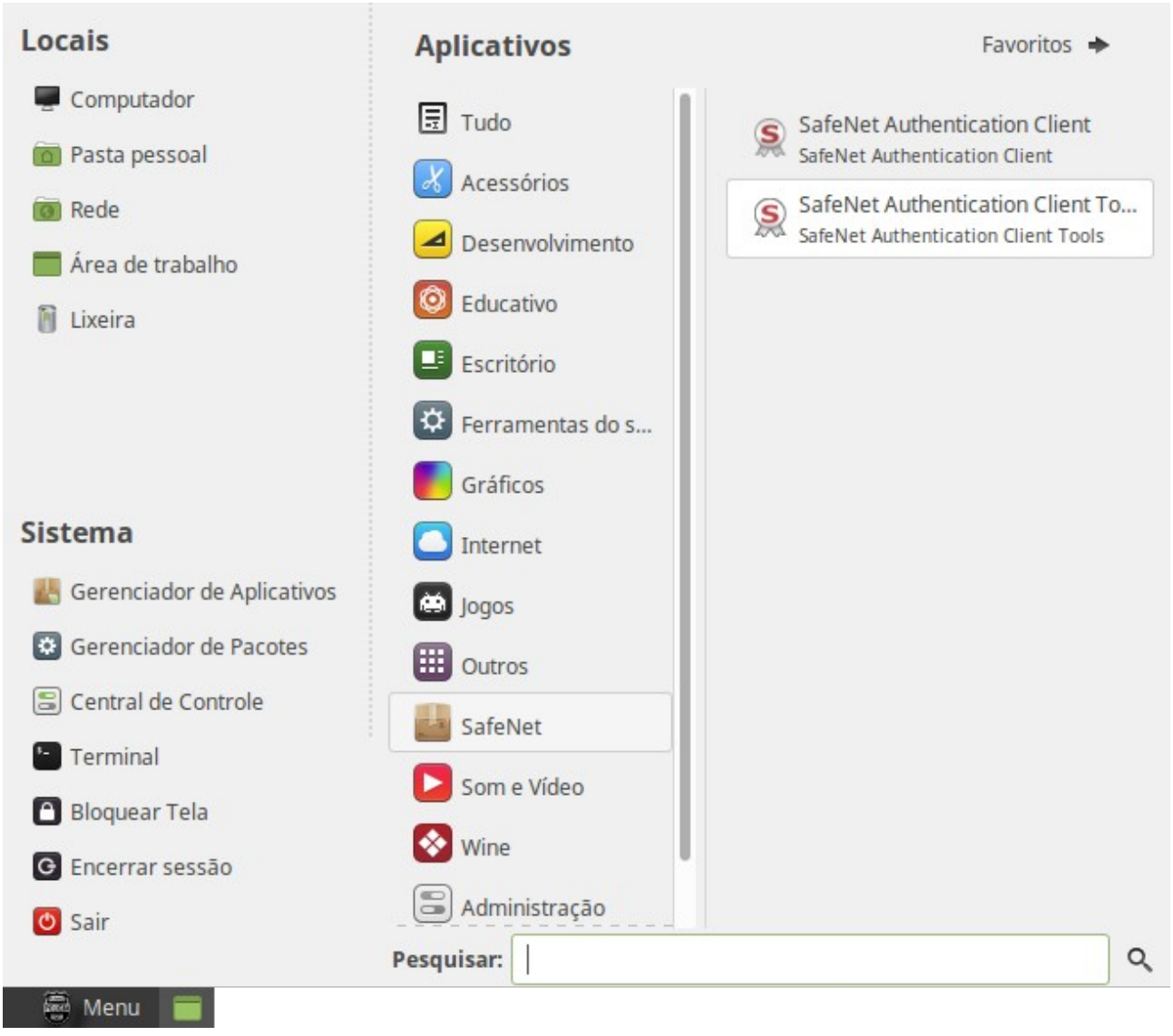
MANUAL DE TROCA E DESBLOQUEIO DE SENHA PIN DO TOKEN SAFENET ETOKEN 5110 FIPS (Linux)
Versão 1.0

Sumário

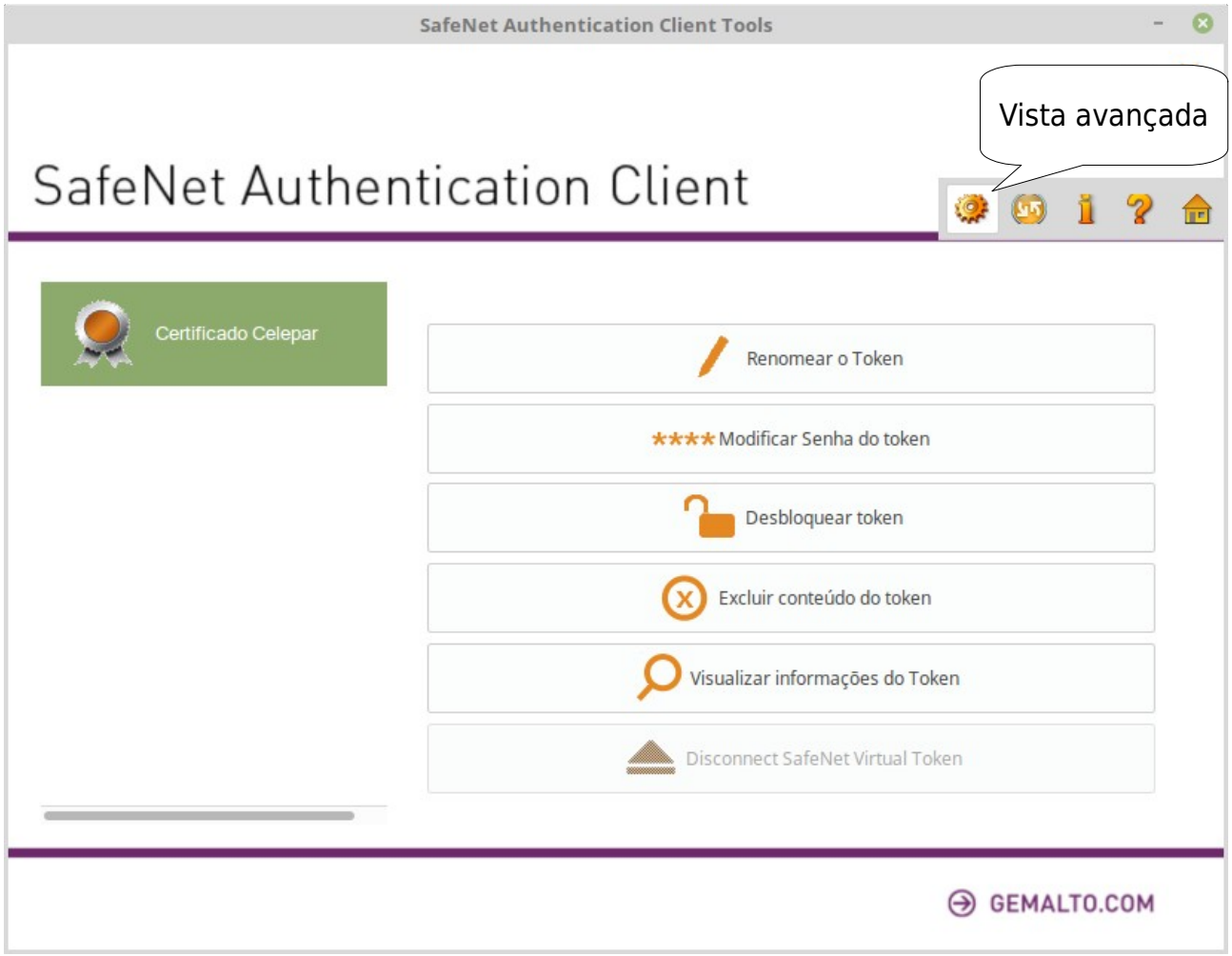
Acessando a interface de gerenciamento de tokens SafeNet (SafeNet Authentication Client Tools)

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*.

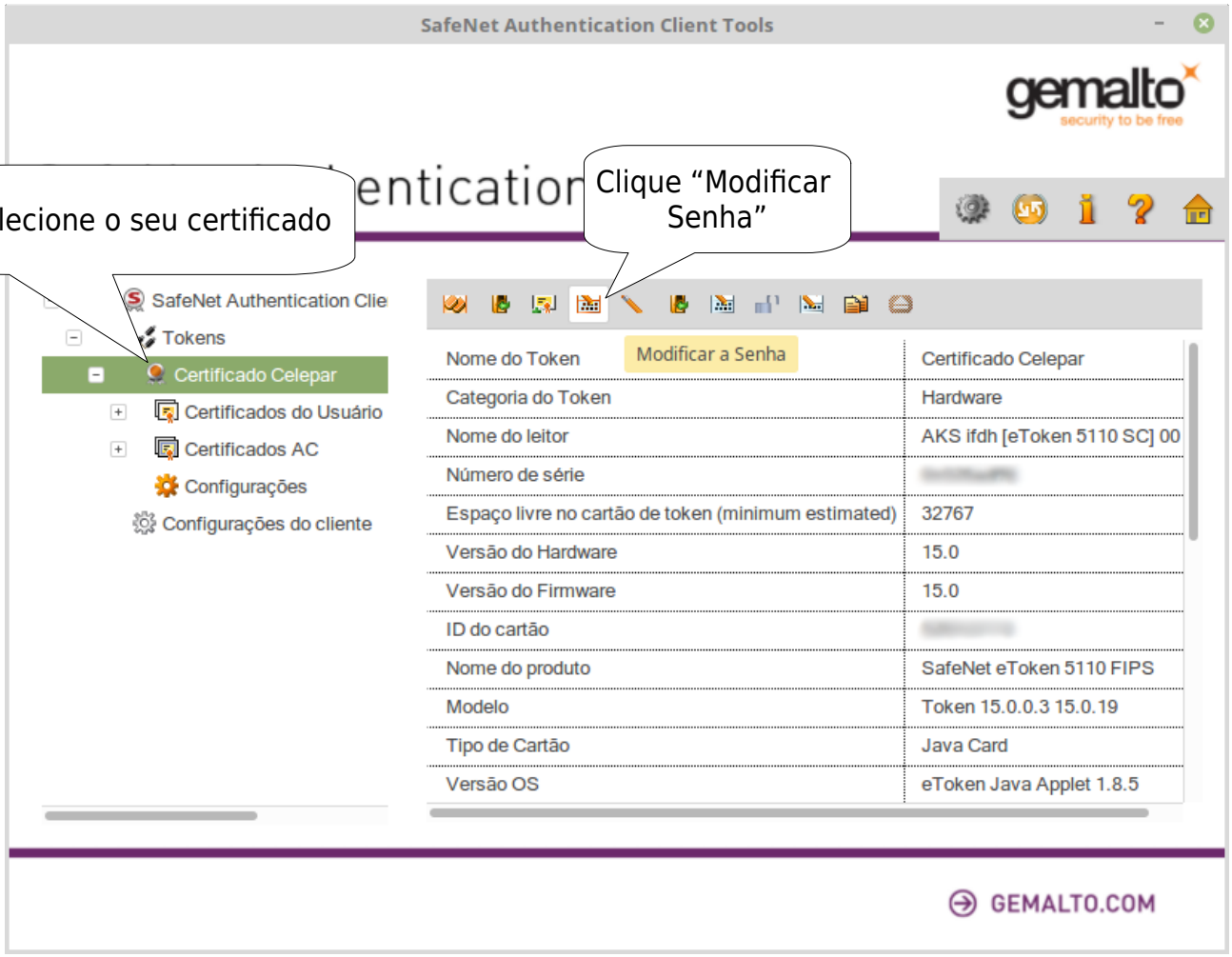


Procedimento de alteração da senha de usuário (PIN) do token SafeNet

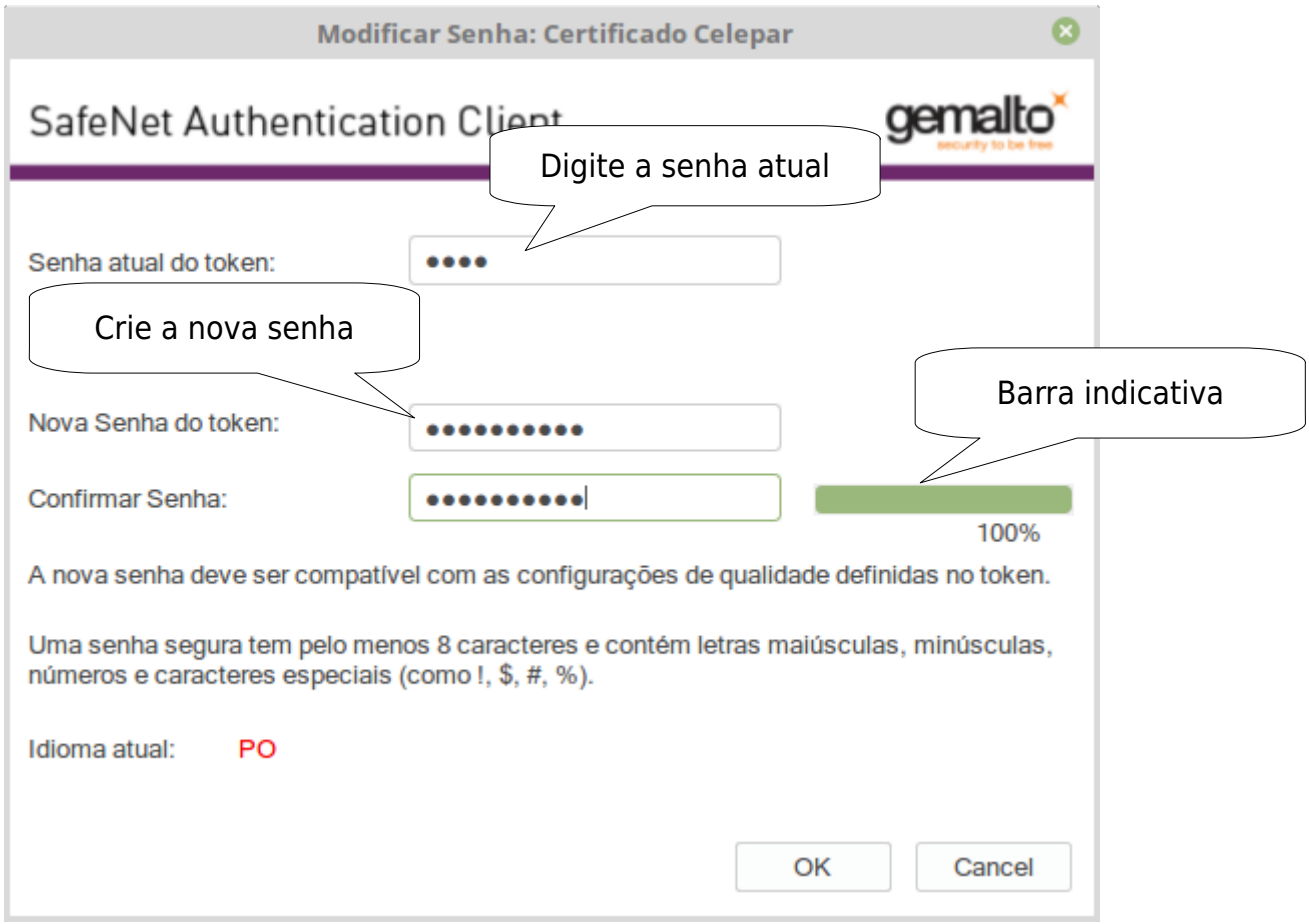
A execução deste procedimento é fortemente recomendada logo após a aquisição do token, pois seu certificado digital é um documento com validade jurídica e a maioria dos sistemas do Estado e permite acesso a informações pessoais e sensíveis.

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)**.

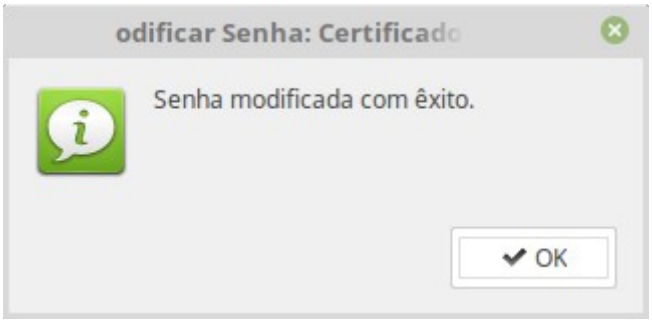
2. Selecione o seu certificado – na maioria dos casos estará nomeado como *Certificado Celepar* por padrão – e clique em *Modificar a Senha*.



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 (!@#$?%°).



4. Pronto. Sua senha foi alterada com sucesso.

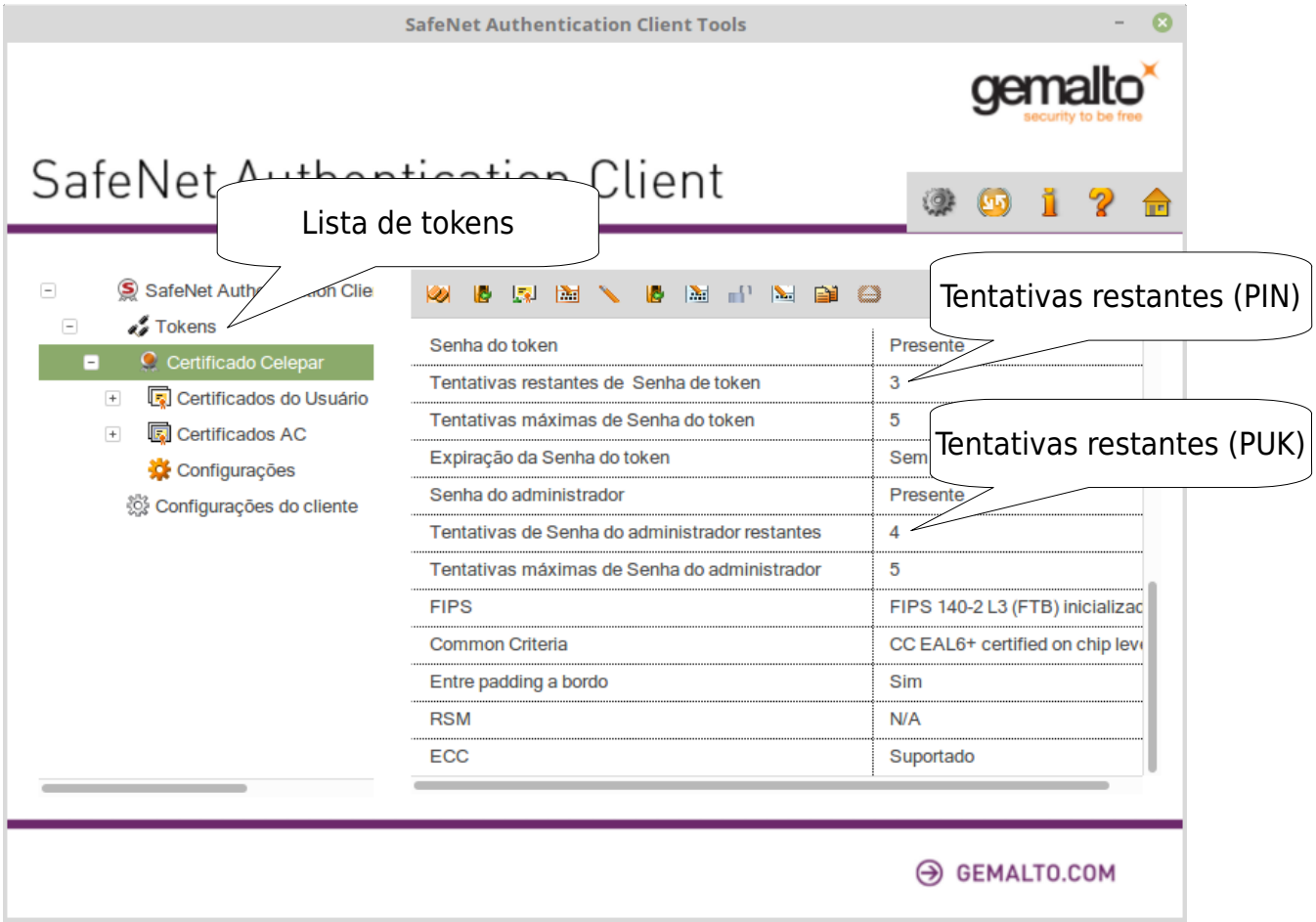


Procedimento para visualizar tentativas restantes dos códigos PIN e PUK

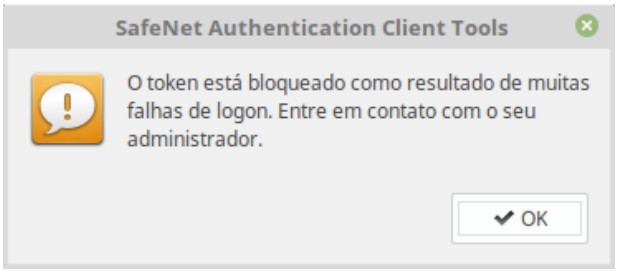
É possível verificar tentativas de acesso às informações do token restantes por meio da interface de gerenciamento. *Senha do token* se refere ao código PIN e *Senha do administrador* ao PUK.

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.



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:



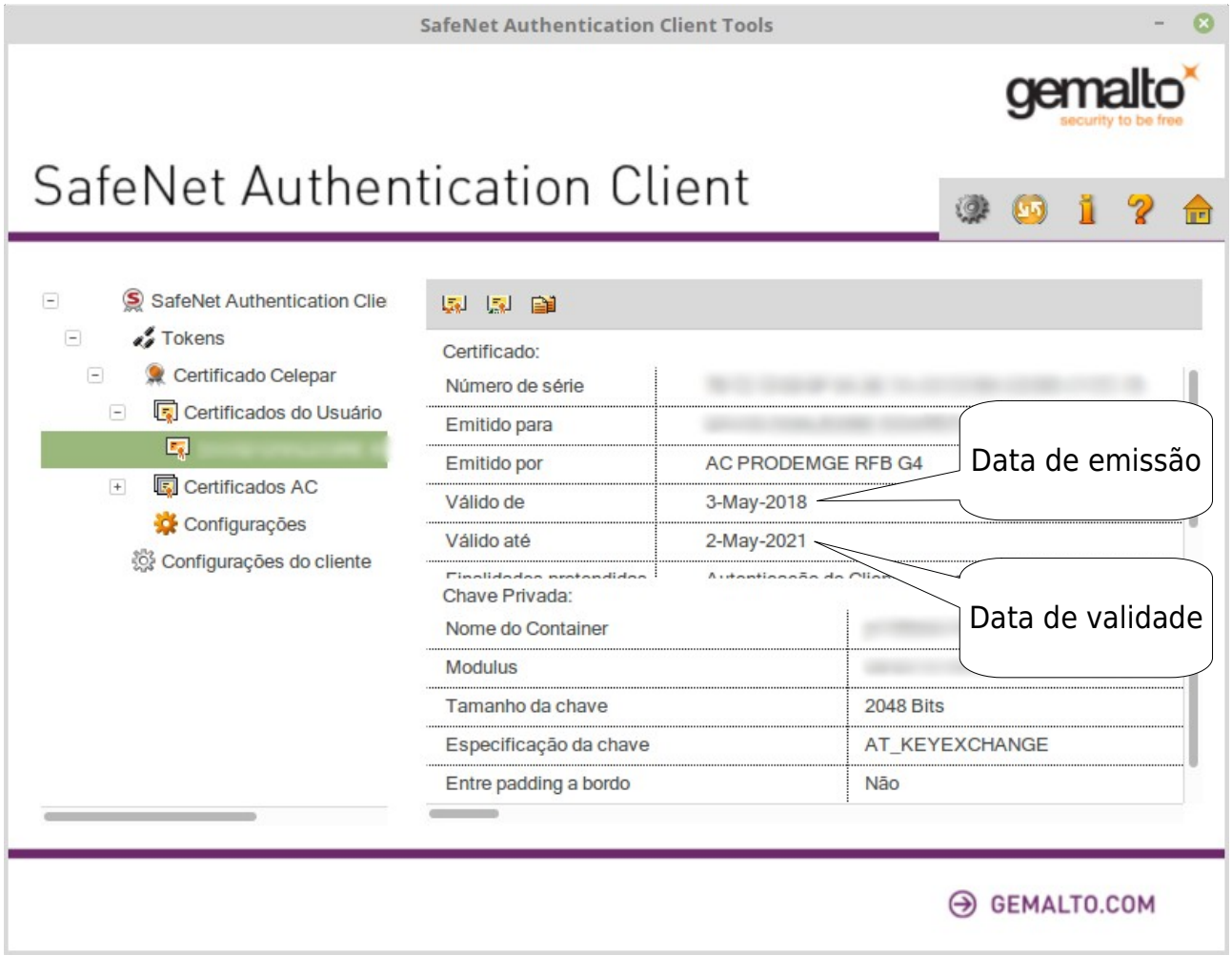
Se este comportamento for aplicável, siga as instruções para **Procedimento para desbloqueio da senha de usuário (PIN) utilizando a senha de administrador (PUK)** descritas a partir da página seguinte.

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)**.

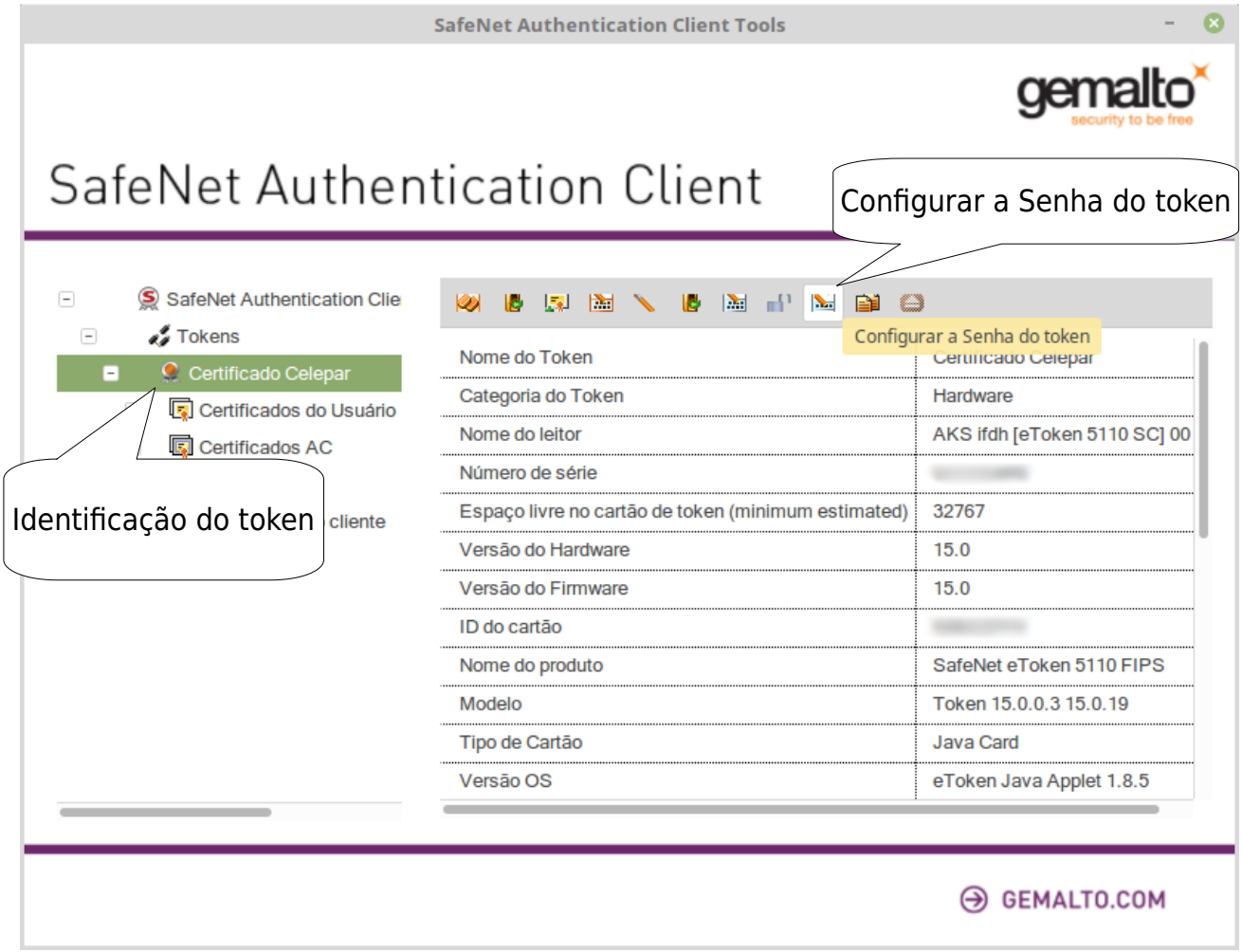
2. Expanda a lista de *Tokens* e selecione o seu dispositivo, por padrão tokens fornecidos pela celepar são nomeados como *"Certificado Celepar"*. Em seguida expanda os *Certificados do Usuário* e selecione seu certificado. Nesse momento as informações de data de emissão e validade estarão visíveis.



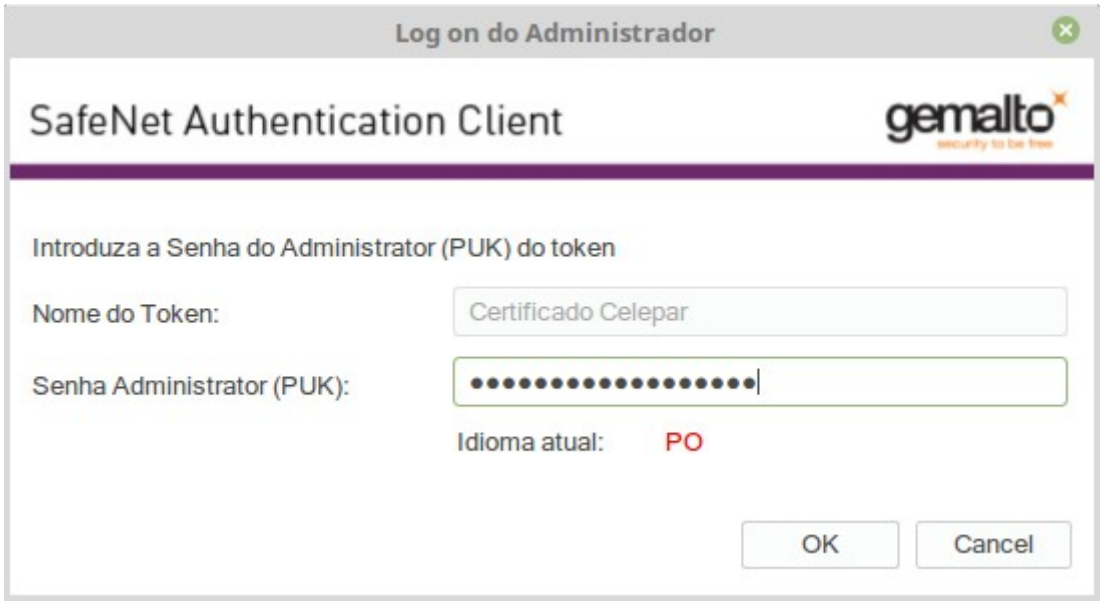
Procedimento para desbloqueio da senha de usuário (PIN) utilizando a senha de administrador (PUK)

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*.

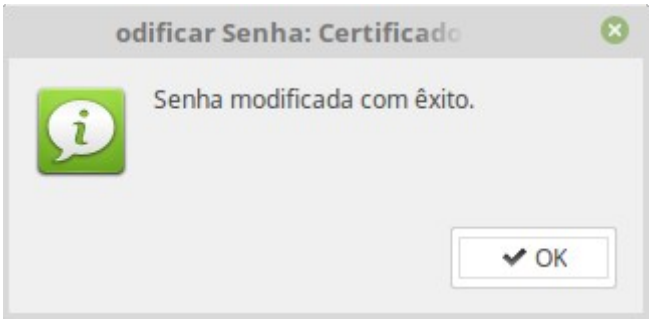


3. Digite a senha de administrador (PUK) do SafeNet eToken e clique em *OK*.



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

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:

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

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.