



Manual de Utilização - Gerenciador do Token StarSign

# Introdução

Certificado Digital é a tecnologia que atribui segurança e validade às transações eletrônicas para troca de informação, transferência de arquivos, criação de documentos e identificação eletrônica de pessoas, empresas, computadores, aplicações e sites.

A **VALID** Certificadora Digital fornece certificados digitais do tipo A3 que são gerados e armazenados dentro de dispositivos criptográficos como cartões e tokens.

Este manual descreve as funcionalidades do Gerenciador do dispositivo para o token StarSign que utiliza como middleware o software Safesign que é instalado pelo Instalador VALID, quando selecionada a opção de instalação A3 em Token StarSign.

O token torna seguro o uso do certificado digital, pois é protegido por uma senha de utilização PIN e senha de desbloqueio PUK, essas senhas possuem uma política que bloqueia as senhas após 03 tentativas consecutivas de digitação incorreta. Para desbloquear a senha de utilização é necessário digitação a senha de desbloqueio, caso as duas senhas sejam bloqueadas os certificados armazenados no token também são bloqueados e caso o token queira ser reutilizado para armazenar novos certificados ele deve ser reinicializado.

## Sistemas Operacionais Compatíveis

A seguir a lista de sistemas operacionais compatíveis como o software de gerenciamento do cartão SafeSign:

- ✓ Windows XP Professional com Service Pack 2 ou superior<sup>1</sup>
- ✓ Windows Vista
- ✓ Windows 7<sup>1</sup>
- ✓ Windows 2003 Server
- ✓ Windows 2008 Server

---

<sup>1</sup> O Gerenciador SafeSign, não é compatível com a versão Start Edition

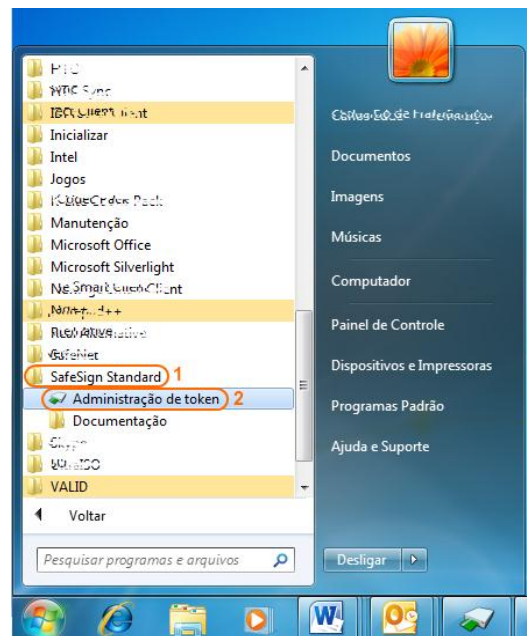
# Iniciando o Gerenciador do Token SafeSign

Para abrir o Gerenciador do token, o SafeSign, que é responsável por permitir que o computador se comunique com o token é necessário seguir os passos abaixo:

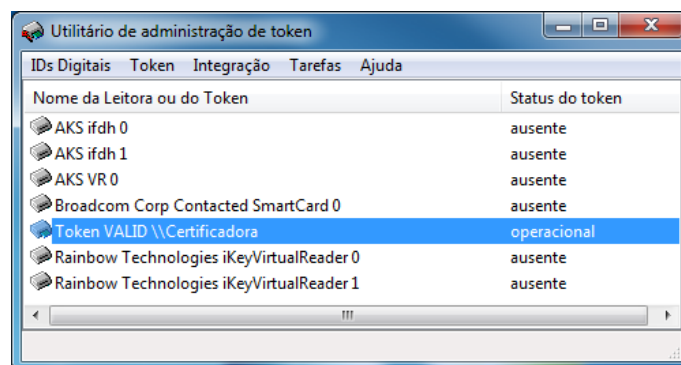
1. Clique sobre o botão Iniciar do Windows e depois clique sobre a opção Todos os Programas, conforme Figura 1;
2. Localize a pasta SafeSign Standard e clique sobre o ícone Administração do Token conforme Figura 2.



**Figura 1 – Menu Iniciar do Windows**



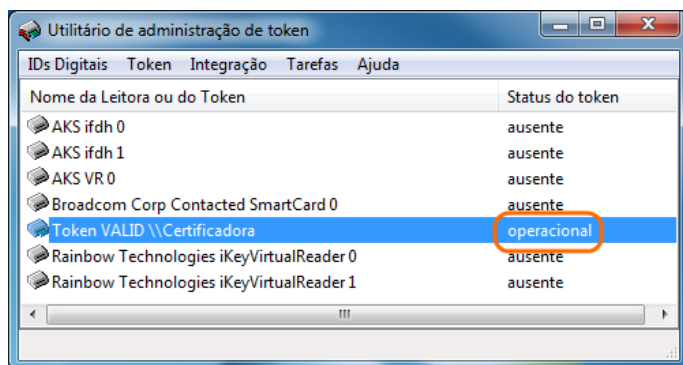
**Figura 2 – Menu Iniciar do Windows**



**Figura 3 – Tela de abertura SafeSign**

# Identificando o Token Ativo

Para identificar se o token foi identificado corretamente e está pronto para uso no computador, após conectar o token abra o SafeSign e verifique se existe algum Nome de Leitora ou Token com o Status do Token 'Operacional', como mostra a Figura 4.



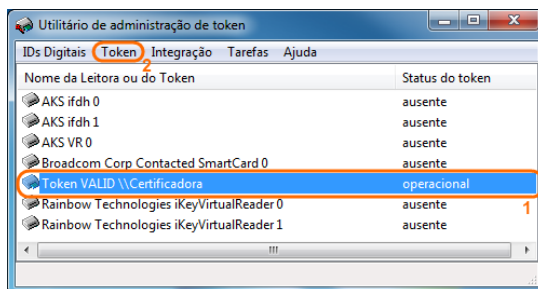
**Figura 4 – Status do Token Ativo**

Caso não seja localizado o token com o status de Operacional, é necessário verificar se o token está corretamente conectado a porta USB do computador ou se o Instalador VALID foi executado corretamente escolhendo a opção Instalar Token StarSign.

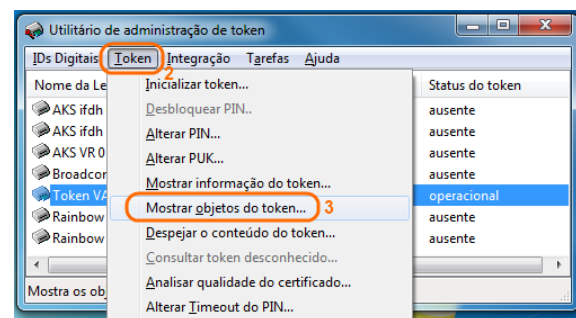
# Mostrar os certificados e chaves armazenados no token

Para visualizar os certificados digitais e o par de chaves presentes dentro do token, itens que compõem o certificado digital e necessários para o seu funcionamento, basta abrir o SafeSign e seguir os passos abaixo:

1. Clicar sobre o token com o Status 'Operacional';
2. Clicar sobre o menu Token;
3. Escolher a opção Mostrar objetos do token.

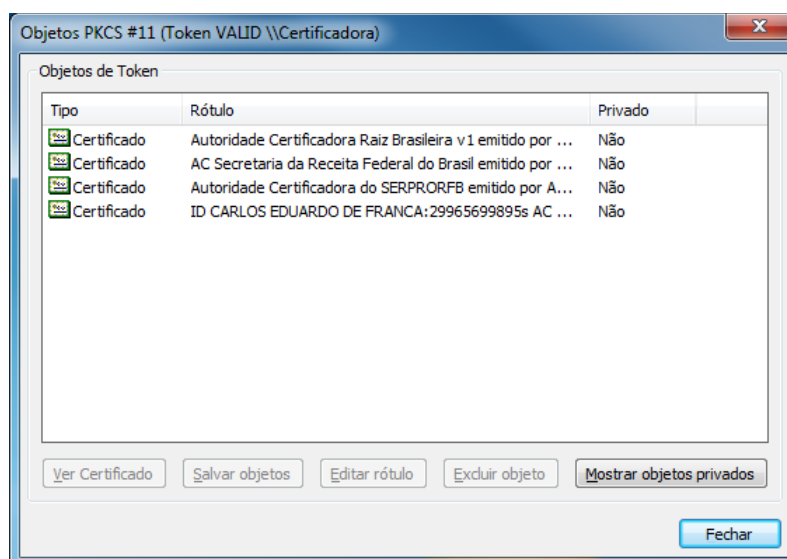


**Figura 5 – Escolha do Token Operacional**



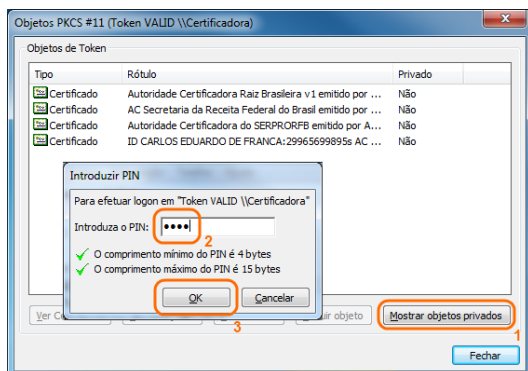
**Figura 6 – Mostrar objetos do token**

Será aberta a tela apresentando os Objetos Públicos (certificados e chave pública), que são publicados no sistema operacional toda vez que seu token é conectado ao computador e permitirá que o certificado seja reconhecido e utilizado.

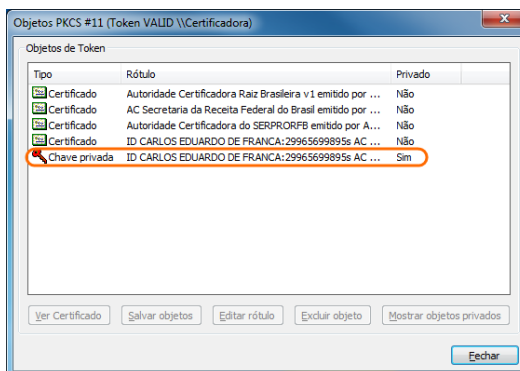


**Figura 7 – Objetos Públicos do Token**

Dentro do token as informações do certificado são separadas em duas áreas uma pública e outra privada, na memória privada é armazenada a chave privada do certificado digital e apenas pode ser utilizada pelo próprio token, para visualizar as chaves privadas clique sobre o botão Mostrar objetos privados digite corretamente o PIN e clique sobre o botão OK.



**Figura 8 – Mostrar Objetos Privados**



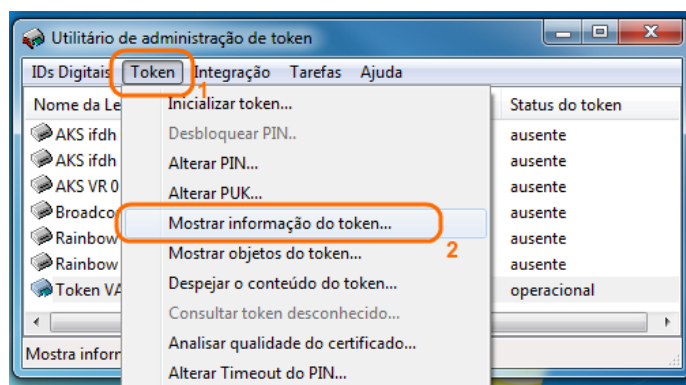
**Figura 9 – Apresentação objetos privados**

# Mostrar as informações do token

É possível visualizar as informações do token como Modelo, Fabricante, Status do PIN, Status do PUK, entre outras informações é que podem ajuda-lo a entender possíveis problemas no uso do certificado digital.

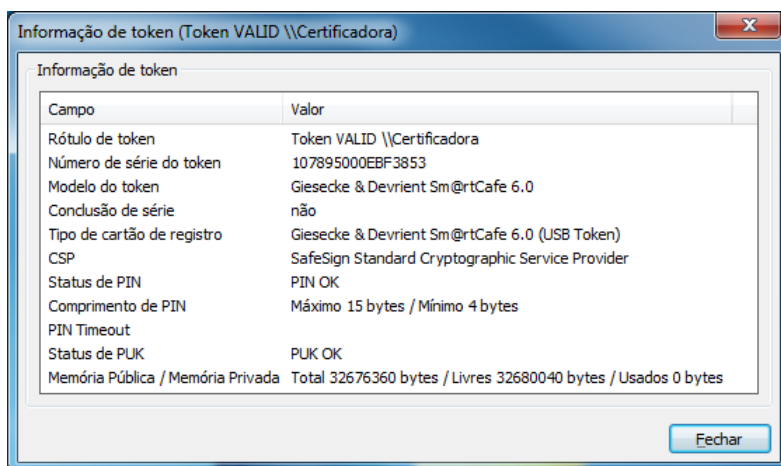
Para visualizar as informações do token, siga os passos abaixo:

1. Após clicar sobre o token com status operacional clique sobre o menu Token;
2. Clique sobre a opção de menu Mostrar informações do token.



**Figura 10 – Menu Token**

Na tela aberta constam informações como Rótulo do token, Status das senhas PIN e PUK, memória utilizada, nome do Modelo do token e o tipo de CSP utilizada.



**Figura 11 – Informações do Token**

# Alterar senha PIN (senha de uso)

O token possui uma senha de utilização chamada PIN, essa senha possui um valor padrão configurado de fábrica (1234), que foi alterado pelo titular do certificado digital ICP-Brasil no momento da validação presencial.

Mesmo que a senha PIN tenha sido alterada durante a validação presencial, ela pode ser alterada novamente sempre que o proprietário do token achar necessário, para isso basta conhecer a senha PIN atual e seguir os passos a seguir:

1. Após clicar sobre o token com status operacional clique sobre o menu Token;
2. Clique sobre a opção de menu Alterar PIN.
3. Informe o PIN atual;
4. Informe o novo PIN;
5. Confirme o novo PIN e clique no botão OK.

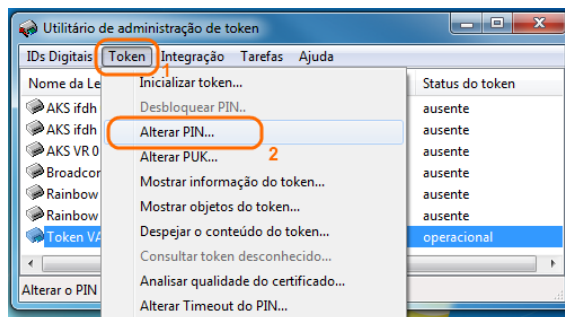


Figura 12 - Menu Token

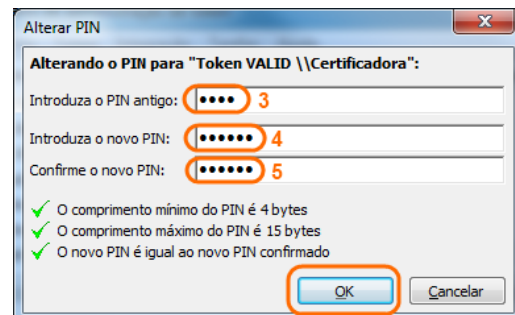


Figura 13 – Alterando o PIN

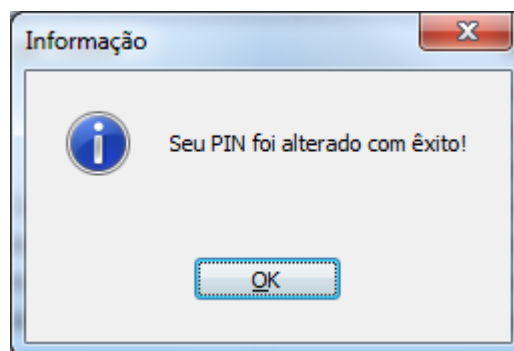


Figura 14 – PIN alterado

# Alterar PUK (senha de administração)

O token possui uma senha de desbloqueio chamada PUK, essa senha possui um valor padrão configurado de fábrica (1234), que foi alterado pelo titular do certificado digital ICP-Brasil no momento da validação presencial.

Mesmo que a senha PUK tenha sido alterada durante a validação presencial, ela pode ser alterada novamente sempre que o proprietário do token achar necessário, para isso basta conhecer a senha PUK atual e seguir os passos a seguir:

6. Após clicar sobre o token com status operacional clique sobre o menu Token;
7. Clique sobre a opção de menu Alterar PUK.
8. Informe o PUK atual;
9. Informe o novo PUK;
10. Confirme o novo PUK e clique no botão OK.

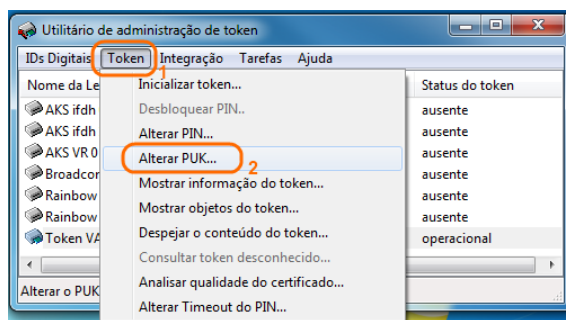


Figura 15 – Menu Token

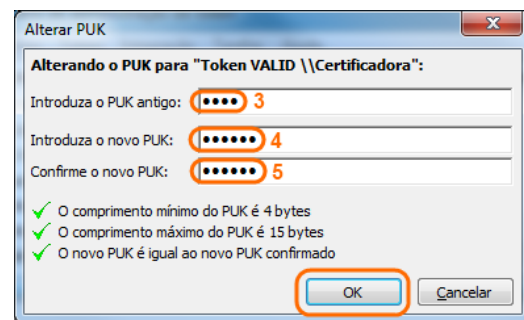


Figura 16 – Alterando o PUK

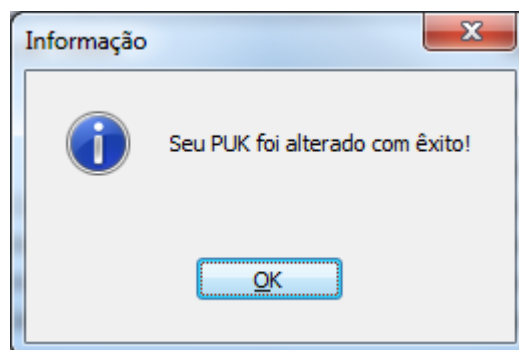
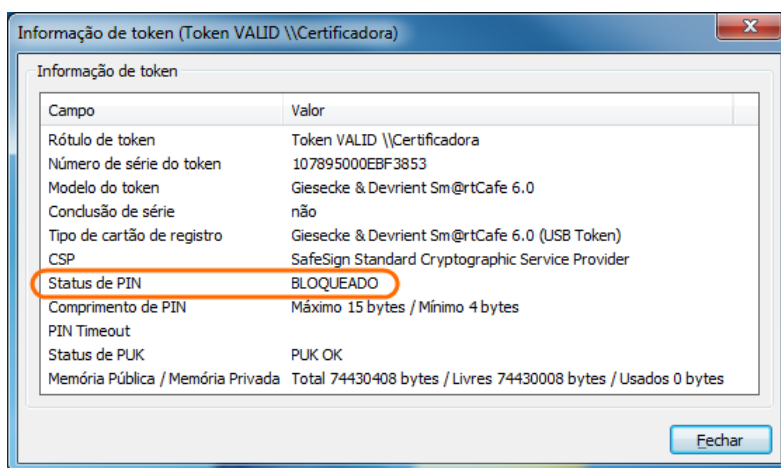


Figura 17 – PUK Alterado

# Desbloquear senha PIN

O token StarSign é protegido por uma senha PIN que libera o seu uso, para aumentar a segurança essa senha possui uma política de bloqueio onde após 3 tentativas de digitação incorreta consecutivas causa o bloqueio da senha PIN e do cartão.

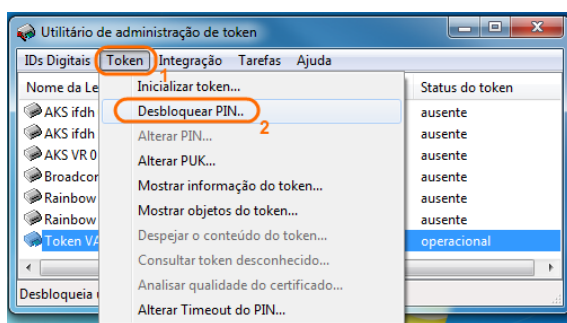
Para identificar se o token está bloqueado, basta tentar usar o certificado e quando for solicitada a senha PIN será apresentada mensagem informando que o PIN está bloqueado, outra forma de identificar esse bloqueio é abrir o painel de informações do token através do menu token, opção Mostrar informações do token.



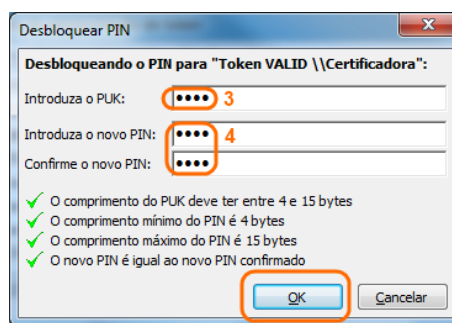
**Figura 18 – Informações do Token**

Para desbloquear o cartão e a senha PIN é necessária utilizar a senha PUK e os passos a seguir, para cadastrar uma nova senha PIN:

1. Após clicar sobre o token com status operacional clique sobre o menu Token;
2. Clique sobre a opção de menu Desbloquear PIN.
3. Informe o PUK atual;
4. Informe e Confirme a nova senha PIN e depois clique no botão OK.



**Figura 19 – Menu Token**



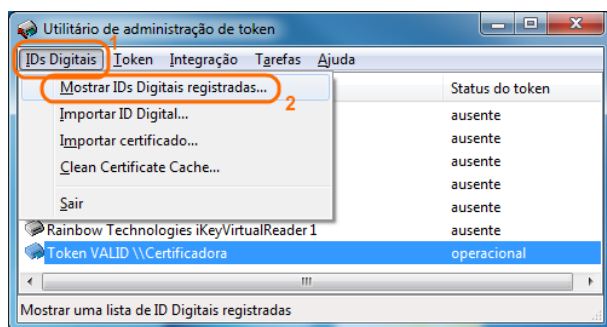
**Figura 20 – Desbloqueando PIN**

# Mostrar certificados digitais registrados

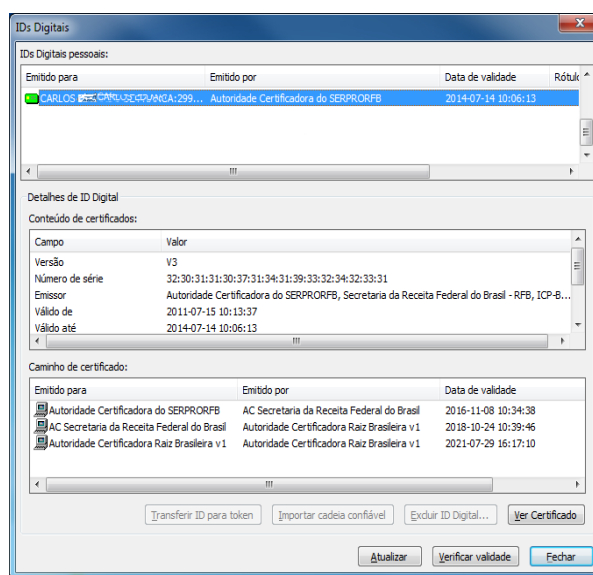
O Gerenciador do token o software SafeSign possui uma funcionalidade que permite verificar se os certificados armazenados no token estão sendo publicados no sistema operacional, sem essa publicação o certificado não ira funcionar no computador.

Para verificar essa publicação basta seguir os passos abaixo:

1. Após clicar sobre o token com status operacional clique sobre o menu IDs Digitais;
2. Clique sobre a opção de menu Mostrar IDs Digitais registradas.
3. Localize seu certificado e verifique se ele está publicado e possui todos os elementos necessários ao seu funcionamento.



**Figura 21 – Menu IDs Digitais**



**Figura 22 – Painel de Certificados Registrados**

No painel são apresentadas informações como a identificação do certificado, número de série, período de validade do certificado e a cadeia de confiança a qual o certificado digital pertence.

Caso um desses elementos esteja em desconformidade como o certificado esteja fora do período de validade ou a cadeia de confiança não esteja sendo apresentada, o certificado pode não ser aceito pelas aplicações.

# Importar certificado digital de Entidade Final

Com o Gerenciador SafeSign é possível realizar a importação de certificados digitais emitidos em software e codificados no formato PKCS#12. Esses certificados normalmente apresentam a extensão PFX e além do certificado e o par de chaves da entidade final (na ICP-Brasil pessoa ou empresa) ele também possui os certificados digitais das Autoridades Certificadoras que compõem a cadeia de confiança do certificado digital.

Para importar o certificado digital basta seguir os passos a seguir:

1. Após clicar sobre o token com status operacional clique sobre o menu IDs Digitais;
2. Clique sobre a opção de menu Importar ID Digital.
3. Selecione o arquivo PFX que será importado;
4. Indique a senha de proteção do certificado digital;
5. Clique sobre o botão OK para confirmar as informações;
6. Digite o PIN para completar a informação

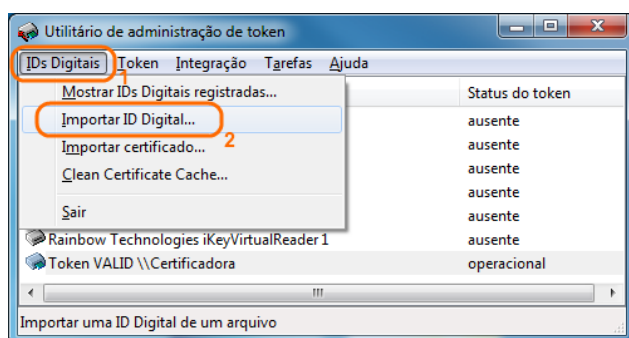


Figura 23 – Menu IDs Digitais

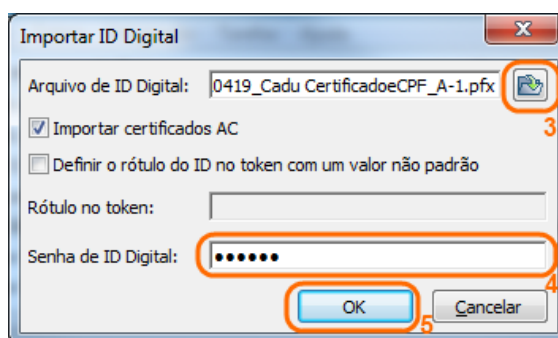


Figura 24 – Importar ID Digital

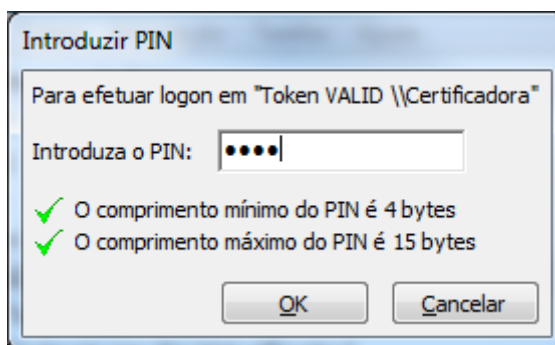


Figura 25 – Digitar PIN

# Importar certificado digital de Autoridade Certificadora

Com o Gerenciador SafeSign é possível realizar a importação de certificados digitais das Autoridades Certificadoras que compõem a cadeia de confiança do certificado digital.

Os certificados digitais de Autoridade certificadora devem estar codificados no formato binário (DER), normalmente identificado pela extensão CER.

Para importar o certificado digital basta seguir os passos a seguir:

1. Após clicar sobre o token com status operacional clique sobre o menu IDs Digitais;
2. Clique sobre a opção de menu Importar Certificados.
3. Navegue e selecione o arquivo com a extensão CER que será importado.
4. Clique sobre o botão Abrir;
5. Digite o PIN para confirmar a gravação do certificado.

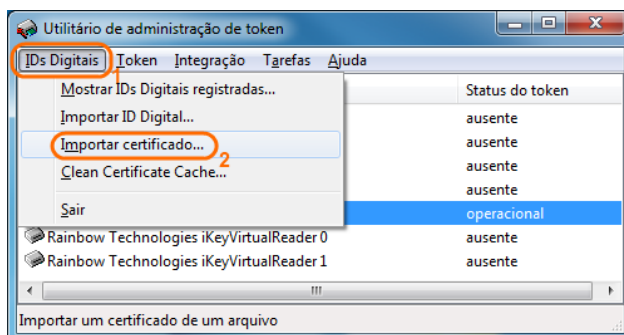


Figura 26 – Menu IDs Digitais

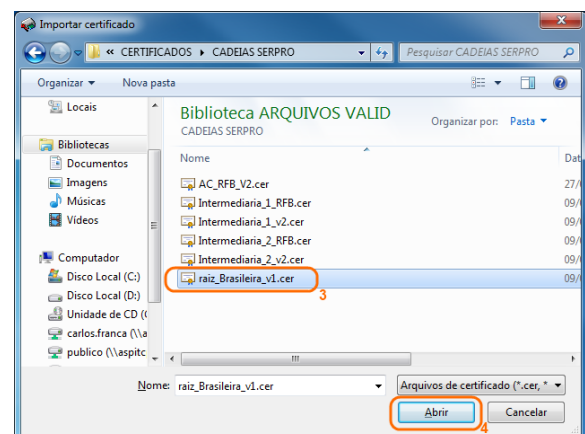


Figura 27 – Seleção certificado .CER

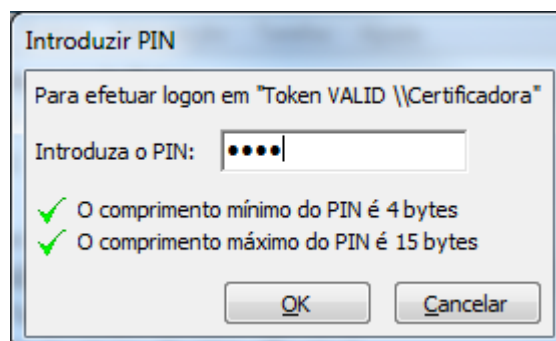


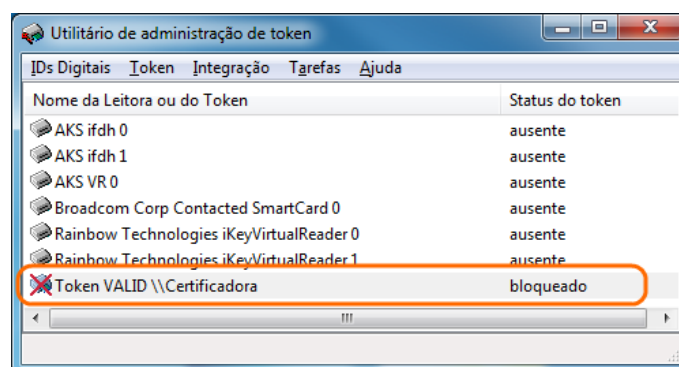
Figura 25 – Digitar PIN

# Reinicializar token bloqueado

Com a utilização da política de bloqueio de senha existente para as senhas PIN e PUK, existe a possibilidade de bloqueio das duas senhas e a inutilização do certificado uma vez que sem a senha PUK não é possível desbloquear a senha PIN.

Quando ocorrer esse tipo de bloqueio é possível realizar a reinicialização do token apagando e inutilizando todos os dados existentes ali dentro, sendo necessárias novas emissões dos certificados digitais armazenados dentro do token.

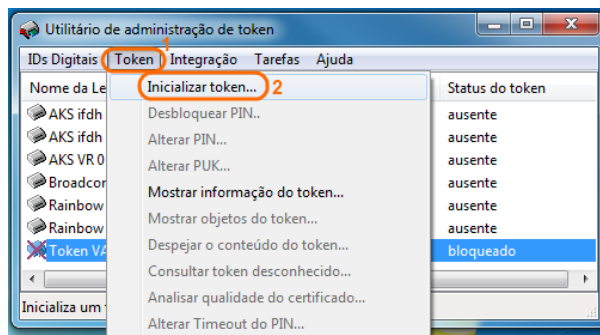
Para identificar se o token está bloqueado, basta abrir o SafeSign e observar o Status do token, caso ele apareça como BLOQUEADO, para poder utilizar novamente o token será necessário fazer sua reinicialização e como consequência será apagado todos os certificados digitais armazenados em sua memória.



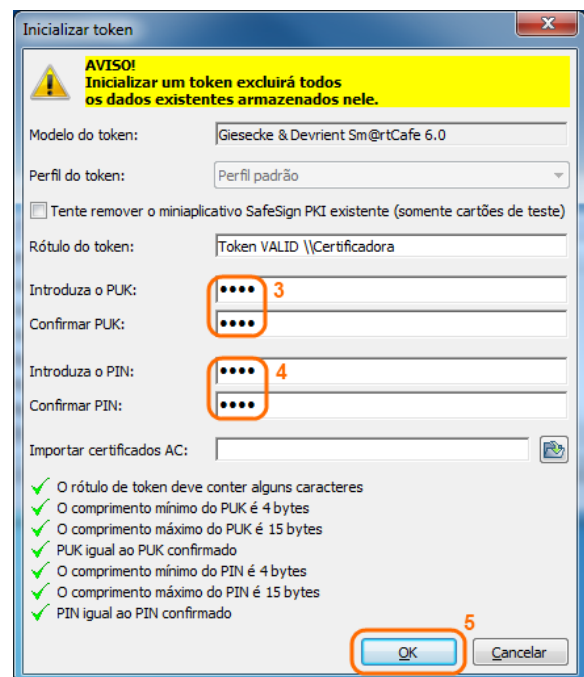
**Figura 26 - Tela de abertura do SafeSign**

Para reinicializar o token basta seguir os passos abaixo:

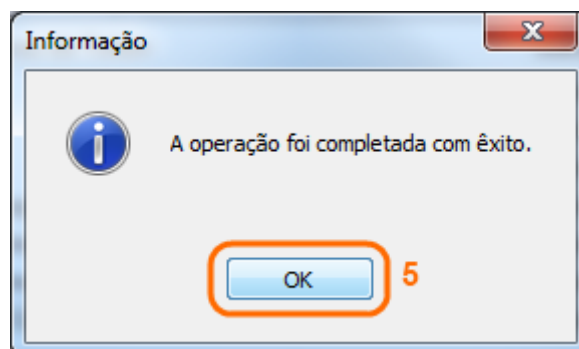
1. Após clicar sobre o token com status bloqueado clique sobre o menu Token;
2. Clique sobre a opção de menu Inicializar token...
3. Informar e confirmar uma nova senha PUK
4. Informar e confirmar uma nova senha PIN
5. Clicar sobre o botão OK.



**Figura 27 – Menu Token**



**Figura 28 – Painel de inicialização**



**Figura 29 – Sucesso Inicialização**

**VALID Certificadora Digital**

Para maiores informações acesse  
[www.validcertificadora.com.br](http://www.validcertificadora.com.br)

setembro de 2011