

MANUAL DE INSTALAÇÃO

E

ADMINISTRAÇÃO DE TOKEN

SAFESIGN

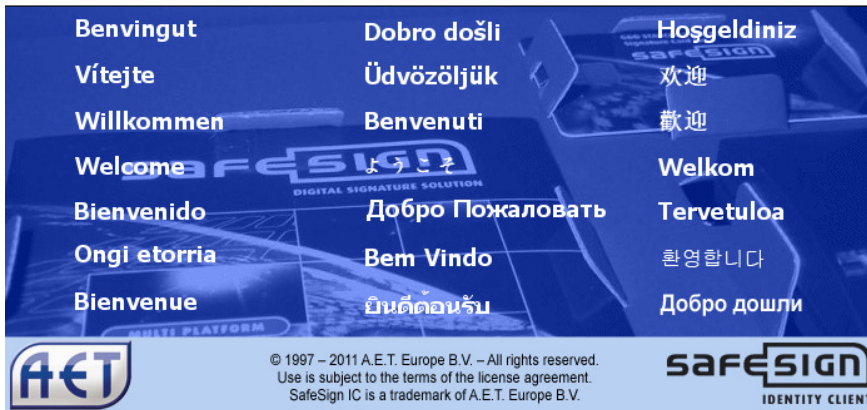
# Manual de utilização do software de gerenciamento SafeSign

## Índice

1.	Instalação .....	3
1.1.	Instalação no Windows.....	3
1.2.	Verificar versão do aplicativo.....	3
2.	Menu do aplicativo .....	4
2.1.	Opção de menu: IDs Digitais .....	4
2.1.1.	Mostrando as IDs Digitais registradas.....	4
2.1.1.1.	Transferir Identidade para token .....	6
2.1.1.2.	Importar cadeia confiável .....	9
2.1.1.3.	Apagando uma Identidade Digital .....	10
2.1.1.4.	Visualizando o Certificado .....	11
2.1.1.5.	Verificar Validade .....	13
2.1.1.6.	Fechar .....	13
2.1.2.	Importando uma Identidade Digital.....	13
2.1.3.	Importando Certificados .....	18
2.1.4.	Sair.....	19
2.2.	Opção de menu: Token.....	20
2.2.1.	Inicializar token .....	20
2.2.1.1.	Inicialização do token .....	20
2.2.1.2.	Importar certificados AC .....	23
2.2.2.	Alterar PIN e Alterar PUK .....	24
2.2.3.	Desbloquear PIN .....	26
2.2.4.	Mostrar informação do token .....	27
2.2.5.	Mostrar objetos do token .....	27
2.2.6.	Copiar o conteúdo do token para um arquivo .....	29
2.2.7.	Analisar qualidade do certificado .....	30
2.2.8.	Alterar tempo de expiração do PIN .....	31
2.2.9.	Apagar objetos do Token.....	33

## 1. Instalação

### SafeSign Identity Client 3.0



#### 1.1. Instalação no Windows

A instalação do aplicativo no Windows resume-se em executar o arquivo com extensão .EXE e seguir as instruções de instalação que aparecem na tela do *InstallShield Wizard*.

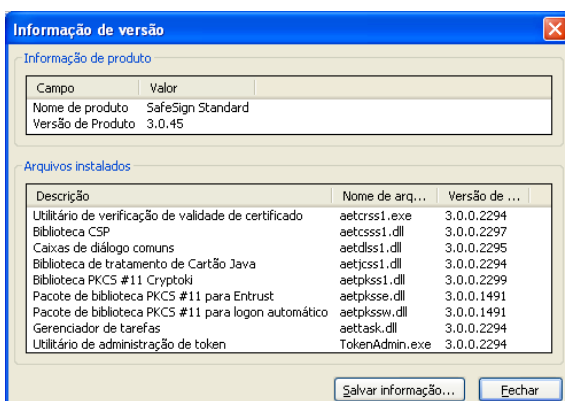
Ao término da instalação, clique em concluir.

Você encontrará no menu “*Iniciar / Programas / SafeSign Standard*” o ícone “*Administração de Token*” que, uma vez clicado, iniciará o aplicativo SafeSign.

#### 1.2. Verificar versão do aplicativo

Uma vez que as funcionalidades do aplicativo, presentes em seu menu, são as mesmas tanto na versão Windows quanto na versão Linux, os itens abaixo demonstrados e no decorrer deste manual servirão para utilização em ambas as versões de sistema operacional.

Para verificar o número da versão de seu aplicativo, entre no menu “Ajuda / Informação das versões...”:



## 2. Menu do aplicativo

A seguir demonstraremos as opções de utilização do SafeSign referentes ao uso deste aplicativo para a visualização e administração de certificados digitais em cartões.

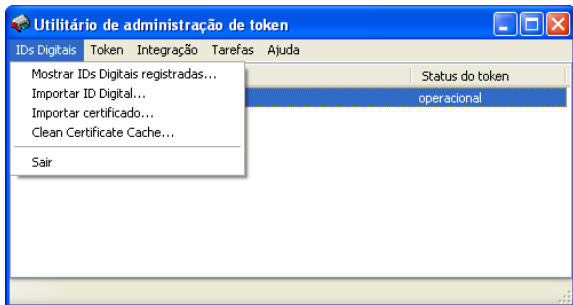
Basicamente temos 2 itens do menu que envolve a gestão de certificados digitais em um cartão/token:

### 2.1. Opção de menu: IDs Digitais

O Menu de IDs Digitais contém os seguintes itens:

- Mostrar IDs Digitais registradas
- Importar ID Digital
- Importar certificado
- Limpar memória cache de certificado
- Sair

O item Limpar memória cache de certificado apenas é utilizado para deixar vazio o repositório cache de certificados do software.



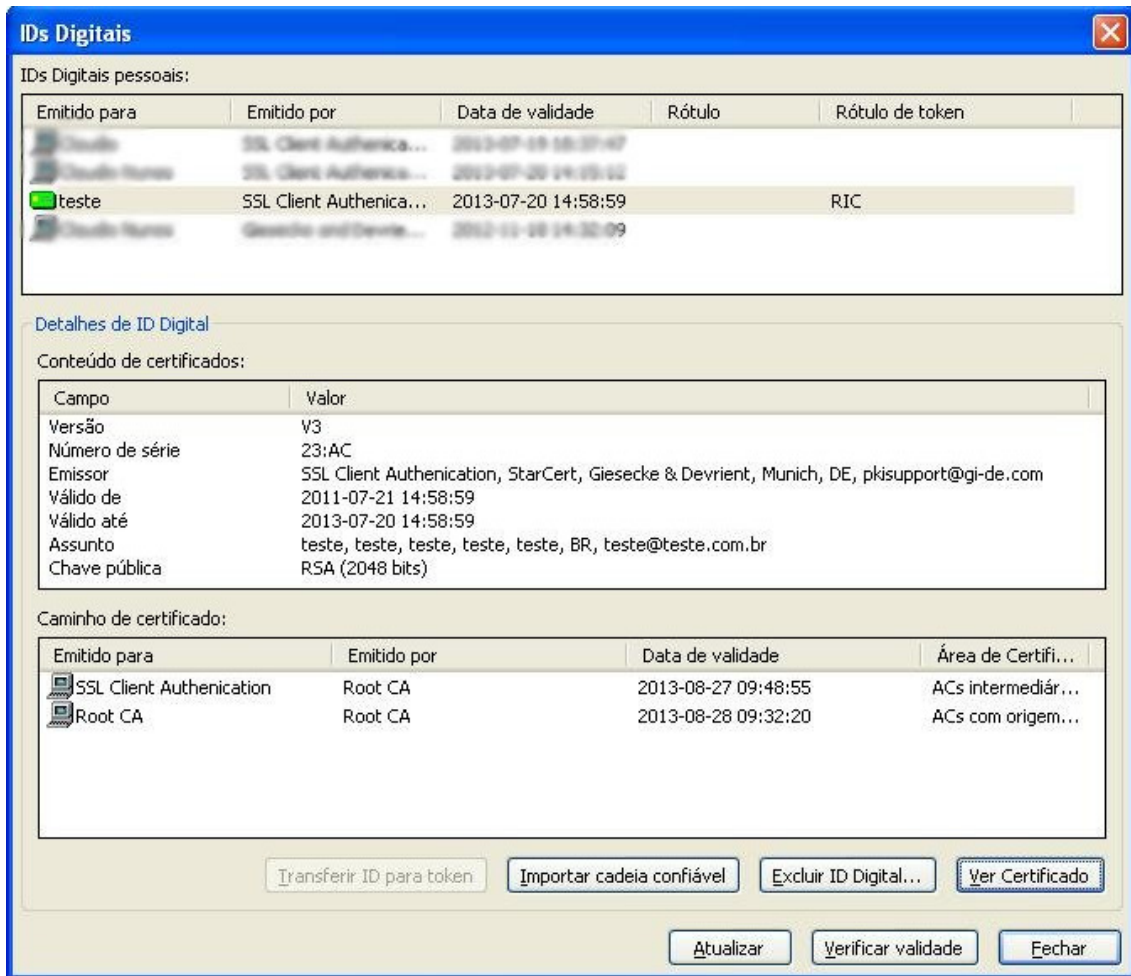
#### 2.1.1. Mostrando as IDs Digitais registradas

O utilitário de Gerenciamento SafeSign permite aos usuários identificar as identidades digitais registradas em um cartão/token. Uma identidade digital consiste em um par de chaves (pública e privada) e um certificado propriamente dito, os quais podem ser utilizados para diversas operações como assinar ou criptografar dados.

O item Mostrar IDs Digitais registradas mostra as identidades digitais que estão armazenadas no cartão/token e/ou tenham sido registradas no local onde o certificado está armazenado.

Nota: em alguns casos as IDs Digitais podem estar registradas e aparecer na caixa de diálogo dependendo da quantidade de objetos armazenados no cartão/token e a leitora que está sendo utilizada.

Quando não houver IDs Digitais, a caixa de diálogo IDs Digitais vai estar vazia. Todavia, quando uma Identidade Digital for gerada ou importada para o cartão/token, basta selecioná-la e a caixa de diálogo terá o visual conforme o exemplo abaixo:



Esta caixa de diálogo tem a finalidade de identificar os **IDs Digitais Pessoais** e os detalhes dos certificados, incluindo o **Conteúdo de Certificado** e o **Caminho do mesmo** pela hierarquia de certificação digital.

Quando a Certificado Digital (sendo **ID Digital Pessoal**) ou Certificado AC (**no Caminho de Certificado**) estiver no cartão/token, irá ser identificado pelo símbolo:

Quando o Código Digital (sendo **Código Digital Pessoal**) ou Certificado AC (**no Caminho de Certificado**) não estiver no Token, (mas alocado como um Certificado Microsoft) será identificado pelo símbolo:

Para transferir uma ID Digital para um cartão/token: consulte o item 2.1.1.1.

Para importar uma cadeia confiável para o cartão/token: consulte o item 2.1.1.2.

A caixa de diálogo ID Digital também é usada como uma ferramenta de performance de um número de operações com relação de IDs Digitais armazenadas no cartão/token e permite ainda as seguintes ações:

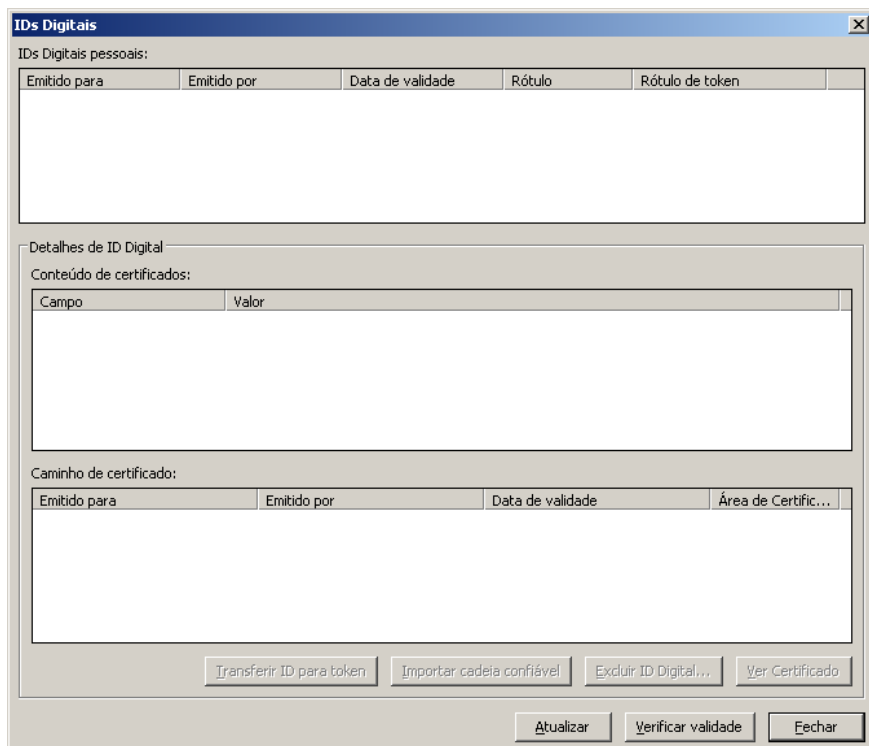
- Transferir identidade para token
- Importar cadeia confiável
- Apagando uma Identidade Digital

- Visualizar o Certificado
- Atualizar
- Verificar validade
- Fechar

Estas funções estão descritas nos próximos itens.

## Perda do Token

Quando o Token que contém as Identidades Digitais não estiver na leitora de cartões, enquanto o certificado é registrado, a caixa de diálogo de IDs Digitais terá o seguinte visual:



O ícone do cartão/token ficará em branco.


Esta situação talvez poderá ocorrer se o usuário estiver sem o seu cartão/token inserido na leitora de cartões.

### 2.1.1.1. Transferir Identidade para token

É possível transferir (mover) uma Identidade Digital (certificado) para o cartão/token, por exemplo, quando você tiver uma identidade pessoal (com a sua chave privada correspondente a esse certificado) no compartimento de Certificados Microsoft de origem que você desejar transferir para o seu cartão/token.

A segurança de seu Certificado estará protegida por dois fatores de autenticação: por acesso, você deverá ter a necessidade de possuir um cartão/token e o conhecimento do PIN deste respectivo cartão/token.

Note que quando você efetuar a transferência de uma Identidade Digital para o cartão/token, a chave privada será movida juntamente para o cartão/token e não estará mais no seu disco rígido (Hard disk).

Quando uma Identidade Digital (alocada na parte pessoal de IDs Digitais) não estiver no cartão/token (mas no compartimento de Certificados Microsoft) irá ser identificado por este símbolo: 

Selecione a Identidade Digital (com seu certificado) que você deseja transferir para o cartão/token:

**1º** – Clique em **Transferir ID para token** para mover a Identidade digital do local de origem para o cartão/token.

**2º** – Você será consultado sobre a confirmação da transferência da ID Digital com os dados específicos

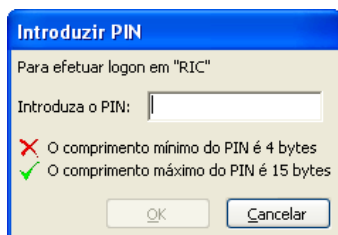
Clique em **Sim** para transferir a ID Digital especificada para o cartão/token. Se você clicar em **Não**, o processo de transferência será abortado e a ID Digital não será transferida.

**3º** – Você será consultado se o Certificado de AC que pertence ao Código Digital (“cadeia confiável”) deverá ser importado.

Clique em **Sim** se você quiser importar o Certificado de AC que pertence à respectiva Identidade Digital.

Se você clicar **Não**, o Certificado de AC que pertence à Identidade Digital (Certificado em questão) não será importado para o cartão/token (mas o processo de transferência da Identidade Digital continua).

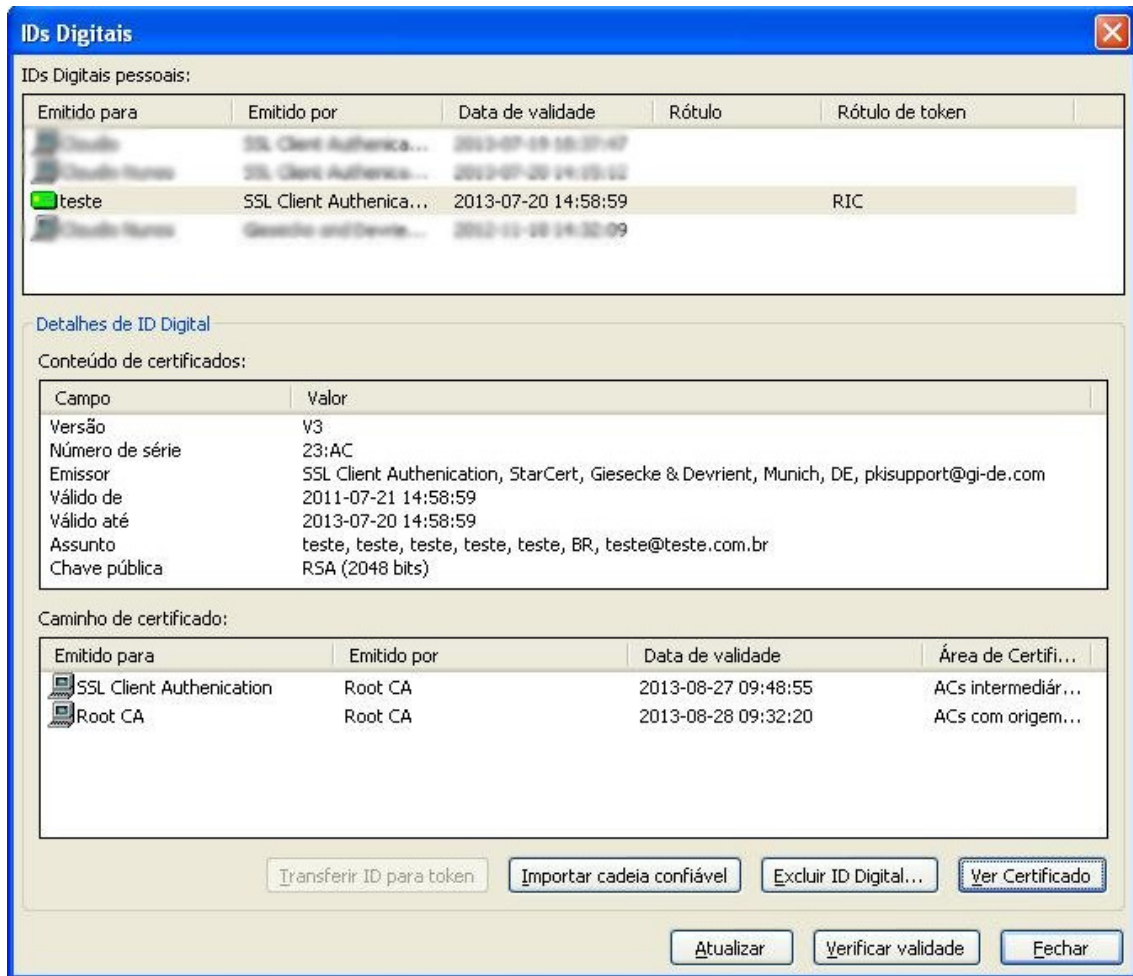
**4º** – Você será solicitado a inserir o PIN para o cartão/token.



Insira o PIN referente a este cartão/token e clique em **OK**.

**5º** – O seu certificado será importado.

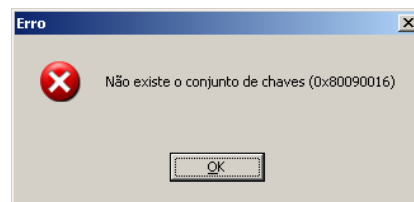
**6º** – Quando a Identidade Digital for totalmente transferida para o cartão/token você será notificado e poderá visualizá-lo devidamente na tela abaixo:



Quando você tiver clicado em **Sim** para importar do prompt o Certificado de AC que pertence à Identidade Digital, o certificado também estará no cartão/token (conforme o Caminho de certificado na imagem acima).

### Chave privada não-exportável

Quando a chave privada pertencente à Identidade Digital não é exportada, a transferência é interrompida e a seguinte mensagem de erro será mostrada:



Clique em **OK** para fechar esta caixa de dialogo.

### Caminho de certificado

Quando o certificado de AC não estiver disponível (nenhum no cartão/token ou em um compartimento com o certificado apropriado Microsoft), não haverá certificados a serem visualizados no **Caminho de certificado**.



Quando o Certificado de AC não estiver no cartão/token (por exemplo, quando você escolhe não importar o certificado da cadeia durante a transferência), mas este é um certificado apropriado da Microsoft (Trust Root Certification Authorities), você poderá importar a cadeia confiável para o cartão/token e para isso, basta realizar o procedimento descrito no item 2.1.1.2.

### 2.1.1.2. Importar cadeia confiável

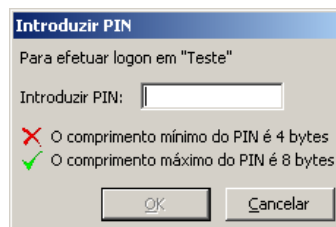
A operação de **importar uma cadeia confiável** reservada para ser importada para a Identidade Digital em um cartão/token, serve para garantir uma máxima flexibilidade e interoperabilidade. Quando você verificar seu cartão/token em outro computador (onde a cadeia confiável apropriada não estiver instalada), você sempre terá os certificados com você e sempre poderá registrá-los.

Você pode usar esta funcionalidade quando for transferir a Identidade Digital para um compartimento de código pessoal do cartão/token e escolher não importar o certificado de AC nessa hora (conforme descrito no item 2.1.1.1) ou se você recuperar o certificado de AC posteriormente (com seu certificado já dentro do cartão/token).

1º – Selecione a Identidade Digital da cadeia confiável de onde você deseja importar para o seu cartão/token:

Clique em **Importar cadeia confiável** para importar uma cadeia confiável para o cartão/token.

2º – Você será solicitado a incluir o PIN do seu Token:



Insira o PIN e clique em **OK**.

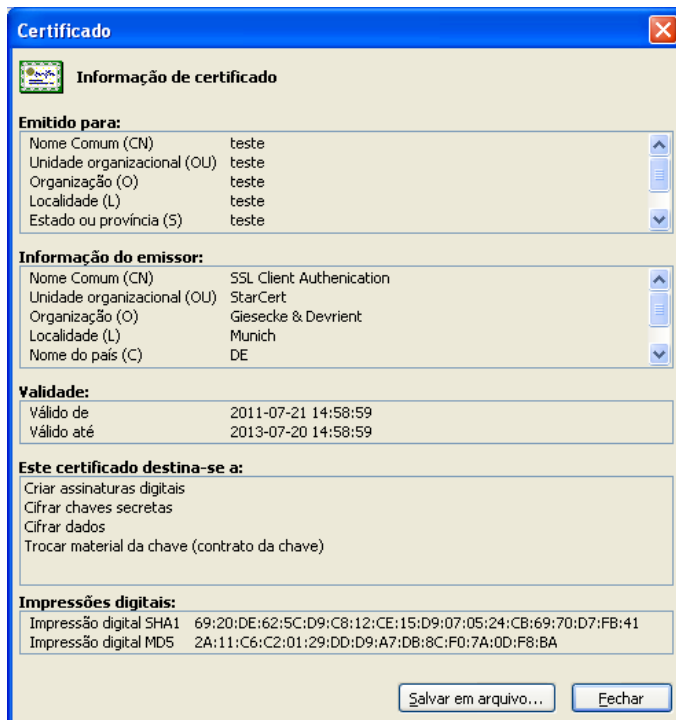
3º – O certificado será importado.

4º – Quando a cadeia do certificado for importada com sucesso, você será informado:




Clique em **OK** para fechar esta caixa de diálogo.

O certificado com sua cadeia aparecerá conforme abaixo:



### 2.1.1.3. Apagando uma Identidade Digital

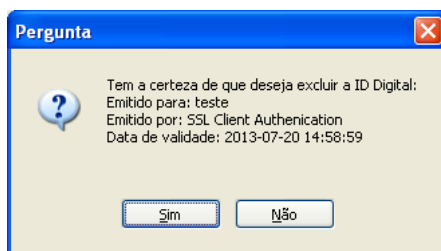
É possível apagar uma Identidade Digital (certificado e chaves) alocada no cartão/token pelo botão **Excluir ID Digital**. Note que você somente pode apagar a Identidade Digital que estiver contida no cartão/token.

Você não conseguirá apagar as IDs Digitais que aparecem na caixa de diálogo e que não estão contidos no cartão (o botão **Excluir ID Digital** ficará cinza – ).

#### Nota

Sobre as informações de Excluir ID Digital acima, todos os objetos da Identidade Digital (chave pública, chave privada e certificado) serão apagados.

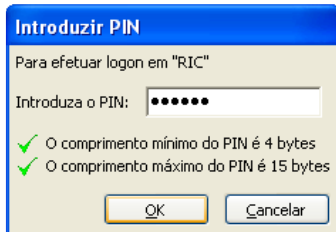
1º – Quando você clicar no botão **Excluir ID Digital**, você será consultado sobre apagar ou não o Código Digital com os dados especificados:



Clique em **Sim** para apagar a Identidade Digital.

Se você clicar em **Não**, o processo de limpeza (excluir) a Identidade Digital será abortado e o certificado com suas respectivas chaves pública e privada não serão apagados.

2º – Após ter clicado em **SIM** conforme acima, você será solicitado para inserir o PIN do seu cartão/token:



3º – Informe corretamente o seu PIN.

### Quantidade de caracteres do PIN / PUK

O SafeSign reforça o mínimo e o máximo de parâmetros do PIN/PUK. Se você inserir o PIN / PUK com menos ou mais caracteres do que o informado, você não estará habilitado para clicar no botão **OK**. Somente quando você clicar no PIN / PUK com o mínimo e o máximo número que caracteres o botão de OK será habilitado e a operação aceita. A quantidade máxima e mínima de caracteres de PIN / PUK podem ser diferentes de acordo com o perfil de configuração de seu cartão/token.

4º – Após ser inserido o PIN, a Identidade Digital será apagada.

5º – Quando a Identidade Digital for apagada com sucesso, você será informado.

A Identidade Digital, seu par de chaves e certificado correspondentes, são apagados do cartão/token.

#### 2.1.1.4. Visualizando o Certificado

O botão **Ver Certificado** possibilita que você veja o conteúdo dos Certificados Digitais, tais como os dados do certificado que foi selecionado.

Note que você pode também ver o conteúdo do certificado com um duplo clique em outros certificados que estiverem na lista de IDs Digitais pessoais ou em qualquer outro certificado da cadeia.

Clicando em **Ver Certificado** quando a ID Digital estiver selecionada, a caixa de diálogo aparecerá como segue:



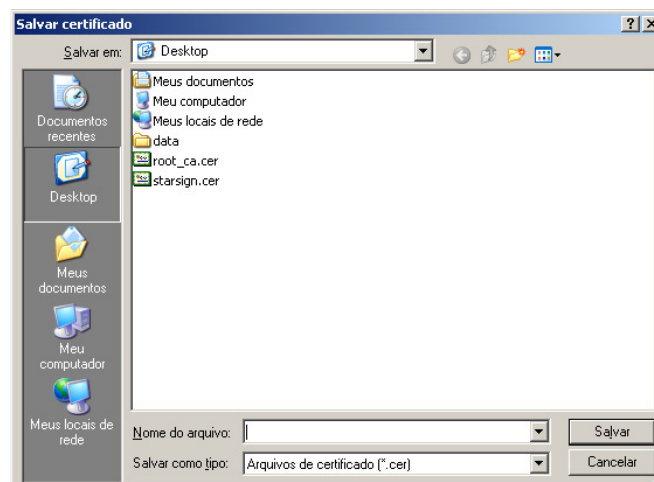
As informações do certificado estarão disponíveis para verificação.

Clique em **Fechar** para fechar a caixa de diálogo.

### Salvando o arquivo

Para salvar as informações do certificado em um arquivo, clique em **Salvar em arquivo**.

Depois de clicar em **Salvar em arquivo**, você pode reservar seu certificado salvando-o com a extensão (\*.cer):



Esta é uma imagem ilustrativa no ambiente Windows. Em outro sistema operacional a tela pode apresentar pequenas diferenças visuais, porém a funcionalidade será a mesma

Selecione uma localidade para salvar o arquivo em seu computador e crie um nome para o mesmo, logo em seguida clique em **Salvar**.

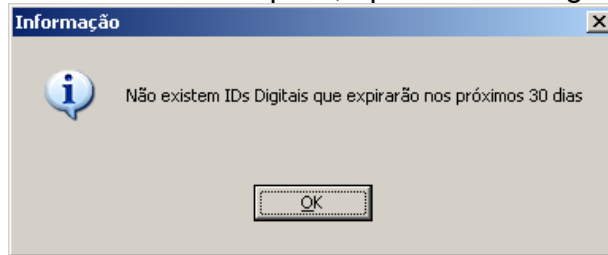
## Atualizar

O botão **Atualizar** é utilizado para atualizar as informações da Identidade Digital na caixa de diálogo.

### 2.1.1.5. Verificar Validade

Você pode checar o status de expiração da Identidade Digital no cartão/token com um clique em **Verificar Validade**.

Quando não houver certificados a expirar, aparecerá a seguinte mensagem:



Clique em **OK** para fechar a caixa de diálogo.

Quando a identidade digital for expirar ou já tiver expirado, o aviso de expiração de identidades digitais aparecerá informando a quantidade de dias que restam para a data de expiração ou que passaram da data de expiração.

### Aviso de Expiração do Certificado

A caixa de diálogo do Aviso de Expiração do Certificado também irá aparecer toda vez que o cartão/token for inserido, a qual conterà os certificados que expirarão no período consultado.

Se você selecionar um certificado para saber sobre sua expiração, você pode visualizar o conteúdo do certificado que está registrado no compartimento onde ele estiver alocado, e este aviso não aparecerá novamente e não será mostrado novamente no futuro.

### 2.1.1.6. Fechar

Clicando no botão **Fechar** a caixa de IDs Digitais será fechada.

## 2.1.2. Importando uma Identidade Digital

O utilitário de gerenciamento proporciona um armazenamento seguro de sua Identidade Digital em uma área protegida de seu cartão/token. Devido à importância destes arquivos, suas chaves e certificados estarão seguramente alocados no seu cartão/token, podendo ser utilizados de forma segura na comunicação.

A segurança de sua Identidade Digital é protegida por dois fatores de autenticação: para efetuar o acesso, você precisará estar com o seu cartão/token e fornecer o PIN (senha de acesso ao conteúdo protegido).

Note que este procedimento pode ser usado para importar a sua Identidade Digital com seus arquivos alocados em PKCS#12 ou no formato PFX do seu disco rígido (ou mídia removível, como disquete, etc.), visto que a função **Importar ID Digital** para o cartão/token podem ser utilizado para certificados digitais presentes na pasta em que estiver alocada a Identidade Digital pessoal Microsoft.

### **Nota**

O termo arquivo ID Digital é usado para se referir à combinação do certificado, incluindo a chave pública e a chave privada (em formato PKCS #12), usualmente protegido por senha.

Esta ID Digital deve ser alocada como um arquivo PKCS #12 (.p12) / (Netscape) ou arquivo Personal Information Exchange (.pfx) – (Microsoft). Ambos os formatos possuem a chave privada, no disquete ou no disco rígido.

O arquivo neste formato pode ser obtido em qualquer modo de exportação de chaves e certificados do seu Netscape Communicator Database (.p12) ou pela exportação das chaves e certificados do seu compartimento de Certificações Microsoft. (.pfx). Note que durante este processo, você será solicitado a inserir a senha que protege este arquivo. Esta senha é solicitada quando ocorre a importação de uma Identidade Digital para o seu Token.cartão/token.

### **Nota**

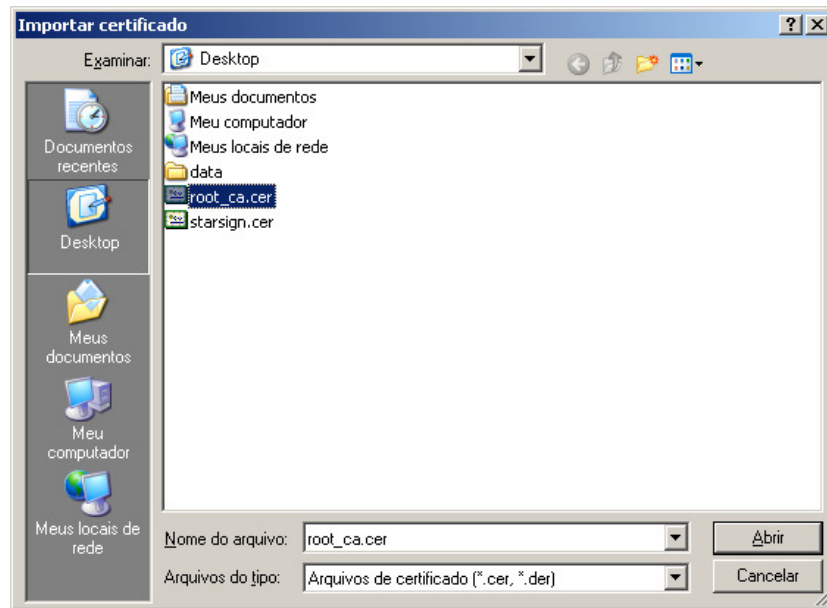
Note que a aplicação (podendo variar alguns detalhes entre uma e outra versão do SafeSign) usam determinados formatos visuais de ID Digital. Por exemplo, quando um par de chaves é gerado e transferido um certificado para o cartão/token através do Internet Explorer, você pode ir até o item do menu mostrar objetos do cartão/token e mostrar-se-á a chave pública + chave privada + certificado.

Quando o par de chaves é gerado e transferido através do Netscape, você pode ir até o item do menu mostrar objetos do cartão/token, e aparecerá somente a chave privada + certificado.

Quando o SafeSign importa uma ID Digital, a chave pública não é alocada no cartão/token. O motivo é economizar espaço de memória pública no cartão/token.

O usuário poderá visualizar as IDs Digitais disponíveis na caixa de diálogo de ID Digital (IDs Digitais – Mostrar IDs Digitais registradas) que aparecerá corretamente no item de IDs Digitais pessoais e poderá ser usada para operações de criptografia.

**1º** – Para importar um Certificado, clique **IDs Digitais > Importar Certificado**:



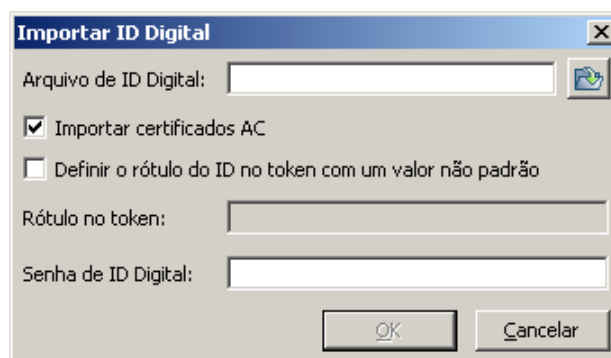
**2º** – Primeiramente você deverá especificar a localidade onde o Certificado está alocado. O arquivo do Certificado pode estar alocado em disco rígido ou uma mídia removível. Clique para selecionar a localidade. No exemplo acima, o arquivo escolhido com “root\_ca.cer”  
 Selecione o arquivo do Certificado e clique para **Abrir**.  
 A caixa de diálogo da importação do Certificado irá mostrar o arquivo que você selecionou.

### Importando Certificados AC

Quando você importa uma ID Digital, você pode escolher se você quer importar um certificado AC (Autoridade Certificadora ou Certification Authority). Fazendo isso, você garante mais flexibilidade e interoperabilidade.

Quando você inserir seu cartão/token em outro computador (onde houver uma cadeia confiável instalada) você sempre terá os seus certificados e seus registros.

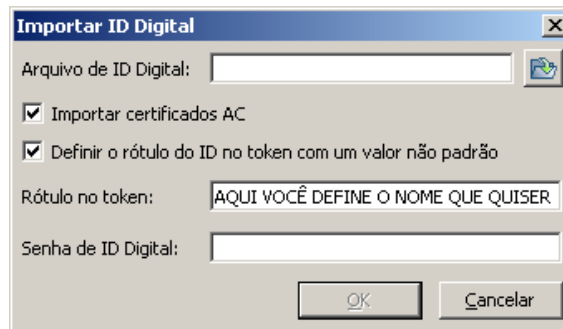
Como segue, a opção **Importar Certificados AC** é selecionada.



Se você não quiser importar certificados do cartão/token, pressione **Cancelar**.

### Ajuste do rótulo (label) do cartão/token – ID Digital – com um valor não padrão

Quando uma ID Digital é importada, você pode ajustar um valor não padrão para o nome de sua ID Digital, para isso basta selecionar “**Definir o rótulo do ID no token com um valor não padrão**” e entrar com nome desejado na caixa “Rótulo no token:” conforme abaixo mostrado:

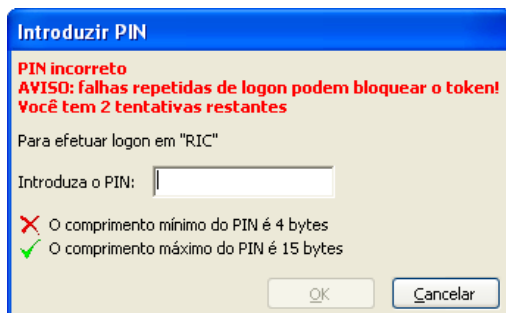


**3º** – Entre com a senha do arquivo de Código Digital:  
Clique em OK para importar o Código Digital.

### Senha Errada

A senha que foi solicitada a você, é a senha que é usada para proteger o seu certificado.

Se você inserir a senha incorreta, a seguinte mensagem irá aparecer:



Clique em **OK** para fechar a caixa de diálogo.  
Você irá começar o procedimento de importação do Certificado novamente clicando em **IDs Digitais > Importar certificado**

**4º** – Quando você clicar em **OK** depois de inserir sua senha da ID Digital, você será solicitado a inserir o PIN do seu cartão/token. Insira o PIN correto e clique em **OK**.

### Quantidade de caracteres do PIN / PUK

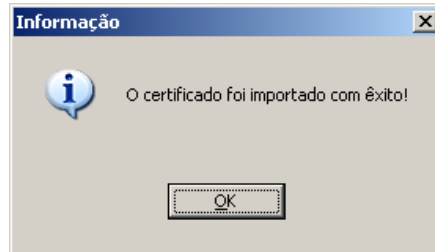
O SafeSign reforça o mínimo e o máximo de parâmetros do PIN/PUK. Se você inserir o PIN / PUK com menos que 4 bytes (caracteres) ou mais do que 8 bytes (caracteres), o aplicativo não permitirá você a clicar no botão **OK**. Somente quando você clicar no PIN / PUK com o mínimo de 4 bytes (caracteres) e o máximo de 8 bytes (caracteres) o botão de OK será habilitado



e a operação aceita. O máximo e o mínimo número de caracteres de PIN / PUK podem variar de acordo com o modelo de cartão/token que você utilizar.

5º – Após clicar **OK** depois de inserir o PIN, o Certificado será importado.

6º – Quando o Certificado for importado com sucesso, você receberá o seguinte aviso:



Clique em **OK** para fechar esta caixa de diálogo.

### Tamanho Errado de Chave

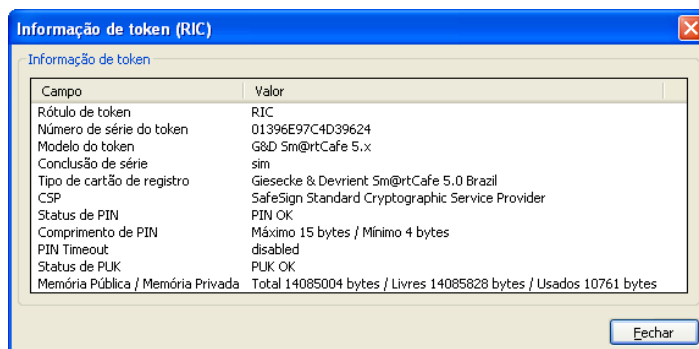
Quando você tentar importar um Certificado que não é compatível com o tamanho da chave estritamente suportado pelo cartão/token, irá aparecer uma mensagem em caixa de diálogo.

Para fechar a caixa de dialogo clique em **OK**.

### Cartão/token sem memória

Quando seu cartão/token estiver cheio, e você tiver muitos objetos para importar, um aviso será apresentado pelo aplicativo. Clique em **OK** para fechar esta caixa de dialogo.

Você deve checar na caixa de dialogo do menu **Token > Mostrar informação do token** (conforme figura abaixo) quanto ainda resta de memória disponível no cartão/token.



Após a importação do Certificado, você pode checar na Caixa de diálogo de ID Digital (**IDs Digitais > Mostrar IDs Digitais registradas**) se o mesmo foi importado corretamente.

### 2.1.3. Importando Certificados

O utilitário de Gerenciamento do cartão/token garante um armazenamento seguro e simples de seu Certificado em seu cartão/token. Pela importância das informações contidas em seu certificado e nas chaves pública e privada, o aplicativo gerencia o uso e comunicação dos dados de forma segura.

Após o uso do SafeSign em outro computador, onde um certificado AC (*root = raiz*) não está instalado, o SafeSign irá instalar o Certificado AC, criando uma cadeia confiável para seu Certificado.

O SafeSign suporta a importação de:

- Certificados DER codificados em .CER
- Certificados DER codificados em .CRT
- Certificados no formato DER

#### Nota

Os certificados AC também podem ser importados durante a inicialização do cartão/token, por favor, verifique o item 2.2.1.2.

1º – Para importar um Certificado AC, clique em **IDs Digitais > Importar certificado**.

2º – Será solicitada a localização de onde o certificado está armazenado:



Especifique o local onde o arquivo do Certificado está alocado. Selecione o arquivo por um clique, e clique **Abrir**.

3º – Depois de selecionar o certificado para ser importado, você deverá inserir o PIN do seu cartão/token:

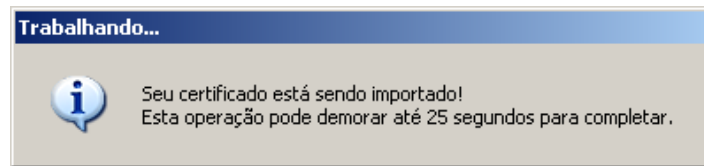


Digite o PIN e clique em **OK** para fechar esta caixa de dialogo.

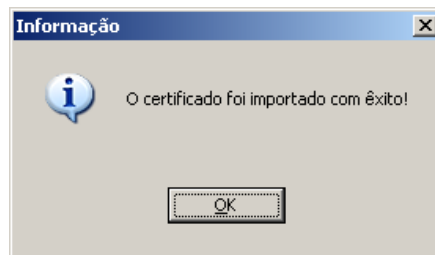
### Quantidade de caracteres do PIN / PUK

O SafeSign reforça o mínimo e o máximo de parâmetros do PIN/PUK. Se você inserir o PIN / PUK com menos de 4 bytes (caracteres) ou mais do que 8 bytes (caracteres), você não conseguirá clicar no botão **OK**. Somente quando você clicar no PIN / PUK com o mínimo de 4 e o máximo de 15 bytes (caracteres) é que o botão de OK será habilitado e a operação aceita. O máximo e o mínimo de caracteres para PIN / PUK que podem ter valores diferentes de acordo com o cartão/token que está sendo utilizado.

4º – Após clicar em **OK**, o arquivo do certificado será importado.



5º – Quando o Certificado for importado, você será notificado.



Clique em **OK** para fechar esta caixa de dialogo e encerrar a operação.

### 2.1.4. Sair

O item **Sair** do menu fecha o aplicativo de gerenciamento do cartão/token.

## 2.2. Opção de menu: Token

### 2.2.1. Inicializar token

O primeiro passo depois da instalação é a inicialização do seu cartão/token (caso o mesmo não esteja inicializado).

Os valores descritos no Token durante a inicialização não deverão ser mudados durante o tempo de vida do cartão/token. Isto significa que o durante o tempo de vida do seu cartão/token, o mesmo guardará o perfil que foi criado durante a inicialização.

Os cartões do tipo JavaCard permitem ser reinicializados, dependendo da inicialização que for utilizada. Cartões Java com chave de produção não podem ser reinicializados novamente nem tratados, após a série de inicialização ser concluída.

Quando você inicializa um cartão/token, o SafeSign detecta o modelo do cartão/token que você inseriu e determina o melhor perfil para inicializá-lo. Antes da inicialização do dispositivo, por favor, tenha cuidado ao considerar que a disponibilidade do perfil depende do tipo de cartão/token que está sendo utilizado. Se um perfil particular não está disponível, isto provavelmente significa que o perfil desejado não pode ser utilizado no modelo de cartão/token (porque não há um espaço disponível dentro do dispositivo com as chaves públicas e privadas para que o perfil seja ajustado). Se o perfil não estiver disponível (o botão de perfil do cartão/token permanecerá cinza).

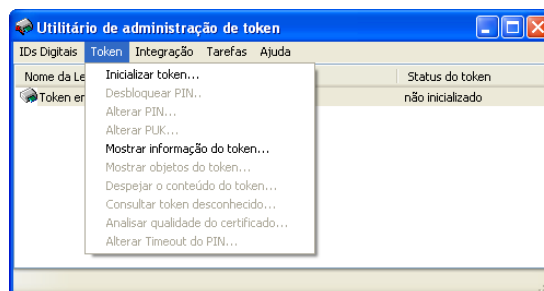
Note que para os usuários finais são recomendados os perfis padrões, sob as orientações do administrador do sistema.

A seguir, o item 2.2.1.1 descreverá como inicializar um cartão/token. Siga as instruções para inicializar seu cartão/token pela primeira vez.

O item 2.2.1.2 descreverá como importar um certificado AC durante uma inicialização do cartão/token.

#### 2.2.1.1. Inicialização do token

1º – Um cartão/token não inicializado, será identificado através do Gerenciador de cartão/token SafeSign, como “Token em branco – não inicializado” e somente o item “Inicializar token” e “Mostrar informação do token” estarão disponíveis:



Para inicializar o cartão/token, clique em **Token > Inicializar token** (conforme imagem acima).

A seguinte caixa de diálogo será apresentada para inicializar o seu cartão/token:

**Inicializar token**

Modelo do token: G&D 5m@rtCafe 5.x

Perfil do token: Perfil padrão

Rótulo do token: RIC

Introduza o PUK:

Confirmar PUK:

Introduza o PIN:

Confirmar PIN:

Importar certificados AC:

O rótulo de token deve conter alguns caracteres  
 O comprimento mínimo do PUK é 4 bytes  
 O comprimento máximo do PUK é 15 bytes  
 PUK igual ao PUK confirmado  
 O comprimento mínimo do PIN é 4 bytes  
 O comprimento máximo do PIN é 15 bytes  
 PIN igual ao PIN confirmado

OK Cancelar

O campo Modelo do token identificará o tipo de cartão/token que você inseriu e está querendo inicializar.

2º – Para inicializar o seu cartão/token, você precisará inserir algumas informações e, uma vez devidamente preenchidos os campos, o símbolo passará a ser .

### Campos utilizados para o processo de inicialização do cartão

- Modelo do token: apenas mostra o tipo de cartão/token consultado
- Perfil do token: pode haver mais de uma opção, além do perfil padrão, caso o token permita
- Rótulo do token: define o nome (*label* ou rótulo) que será definido para o seu cartão/token
- Introduza o PUK: senha de segurança utilizada para quando for bloqueado o seu PIN
- Confirmar PUK: repete-se a senha para garantir o armazenamento correto no seu cartão
- Introduzir PIN: senha de usuário utilizada p/ acesso seguro aos certificados e chaves de seu token
- Confirmar PIN: repete-se a senha para garantir o armazenamento correto no seu token

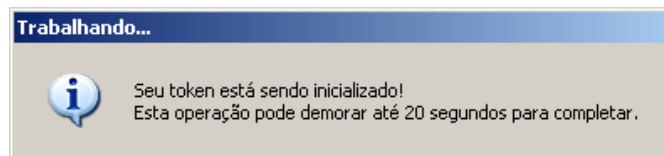
### Campos de requerimento

Os campos de requerimento são utilizados para garantir o correto preenchimento mínimo das informações exigidas na tela de “Inicializar token”. Tais requisitos são necessários para que se garanta que o usuário tenha preenchido pelo menos o campo Rótulo do token, que será o rótulo a ser colocado em seu cartão/token, bem como se as senhas de PIN e PUK tenham sido preenchidas com as quantidades mínima e máxima de caracteres.

Na figura abaixo é mostrado o preenchimento correto de uma tela para inicialização do cartão/token. Note que todos os requisitos apontados nos campos de requerimento estão :

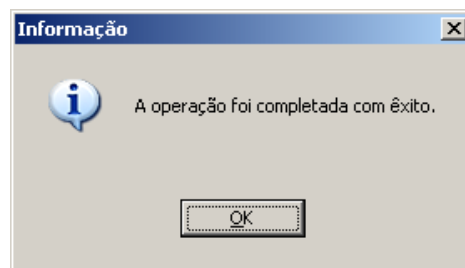
Uma vez todos os campos devidamente preenchidos como na figura acima, clique em **OK** para começar a inicialização do seu cartão/token através do SafeSign.

**3º** – Após clicar **OK**, você será informado que seu cartão/token está sendo inicializado:



Não interrompa ou remova seu cartão/token durante o processo de inicialização. Se você possui uma leitora de cartões com uma luz visível na parte superior, você tem que aguardar a luz indicar que o processo de leitura/gravação do cartão terminou e, desse modo, saber se ele está sendo utilizado ou não.

**4º** – Quando a operação de inicialização for concluída, aparecerá a seguinte tela:



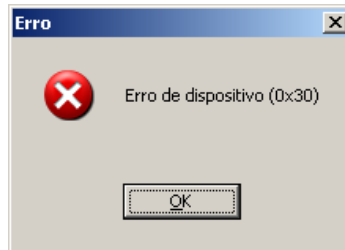
Clique em **OK** para concluir e fechar esta caixa de diálogo.

Quando você inicializar o seu cartão/token, o rótulo/nome que você configurou deverá aparecer na janela do utilitário SafeSign, e uma vez que seu

cartão/token for inicializado, todas as operações de IDs Digitais estarão disponíveis no menu do aplicativo.

### **Erro de Dispositivo**

Caso a inicialização do cartão/token falhe, você será avisado através de uma janela de mensagem.



Clique em **OK** para fechar esta caixa de dialogo.

Verifique se as propriedades de sua leitora estão **OK** e se o cartão inserido é o correto. Verifique também se as senhas de PIN e PUK foram devidamente preenchidas.

Uma vez realizada as devidas verificações, tenha certeza que o cartão/token está inserido na leitora de cartões e clique novamente em **OK** para novamente tentar inicializar o seu cartão/token.

#### **2.2.1.2. Importar certificados AC**

O Utilitário de Gerenciamento de cartão/token (SafeSign), está ativado para importar certificados AC, sendo que existem duas maneiras de se fazer isso:

**Opção 1** – Você pode fazer a importação de certificado de AC através do menu reservado somente para esta ação. Veja detalhes no item “**2.1.3. Importando Certificados**”

**Opção 2** – Outra forma é durante a inicialização do cartão/token, através da opção “**Importar certificados AC**” que aparece na tela “**Inicializar token**”, bastando realizar a seleção do diretório onde o certificado AC está armazenado.

#### **Formato do certificado AC**

O SafeSign suporta a importação de:

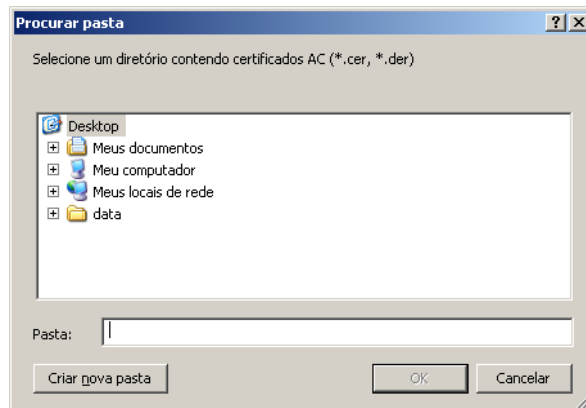
- Certificados DER codificados em .CER
- Certificados DER codificados em .CRT
- Certificados no formato DER

Selecione a pasta ou diretório em que o certificado AC está armazenado. Os arquivos possuem a extensão de \*.cer ou \*.crt ou \*.der.

1º – Na Caixa de diálogo de inicialização do cartão/token, a opção **importar certificados AC** permite você selecionar uma pasta ou diretório onde o certificado AC está armazenado:



2º – Após o clique no ícone para armazenar, a caixa de dialogo “Procurar pasta” aparecerá:



Selecione o diretório e clique em **OK**.

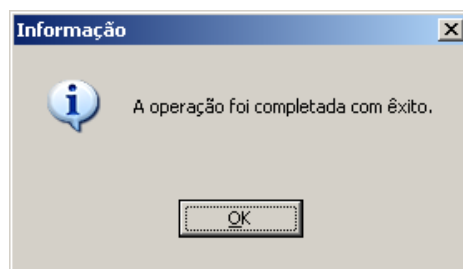
Note que todos os certificados deverão estar contidos no diretório selecionado para serem importados.

Em seguida, basta clicar em **OK** para inicializar o cartão/token.

3º – Após você clicar **OK**, seu cartão/token será inicializado.

Não interrompa ou remova seu cartão/token durante o processo de inicialização. Se você possui uma leitora de cartões com uma luz visível na parte superior, você tem que aguardar a luz indicar que o processo de leitura/gravação do cartão terminou e, desse modo, saber se ele está sendo utilizado ou não.

4º – Quando a operação de inicialização for completada, você será notificado.



Clique em **OK** para fechar esta caixa de dialogo.

### 2.2.2. Alterar PIN e Alterar PUK

O Utilitário de Gerenciamento de cartão/token SafeSign permite que o usuário altere o PIN e o PUK de seu cartão/token.



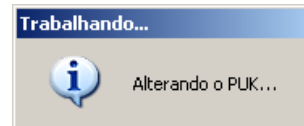
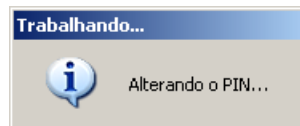
**1º** – Para realizar esta ação, selecione no menu “**Cartão**”, o item “**Alterar PIN**” ou o “**Alterar PUK**”.

A janela acima será aberta identificando o rótulo do cartão/token no qual você deseja alterar o PIN / PUK.

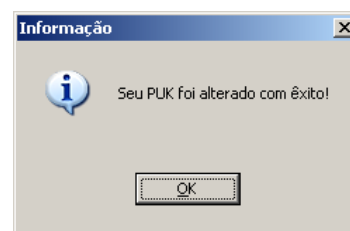
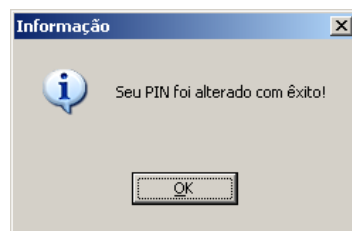
### Quantidade de caracteres do PIN / PUK

O SafeSign reforça o mínimo e o máximo de caracteres para o PIN / PUK. Se você inserir o PIN / PUK com menos de 4 bytes (caracteres) ou mais do que 8 bytes (caracteres), o aplicativo não permitirá que você clique no botão **OK**. Somente quando você digitar um PIN / PUK com o mínimo de 4 e o máximo de 8 bytes (caracteres) é que o botão de **OK** será habilitado e a operação aceita. O número mínimo e máximo de caracteres para o PIN / PUK dependerá da configuração presente no cartão/token utilizado.

**2º** – Uma vez preenchidas as informações da caixa de alteração do PIN / PUK, clique em OK para que o PIN / PUK seja modificado.



**3º** – Quando o PIN / PUK for devidamente alterado você receberá o seguinte aviso.



Clique em **OK** para fechar esta caixa de diálogo.

### Importante - Bloqueio do PIN:

Caso você tente por várias vezes sucessivas acessar o conteúdo protegido do cartão com um PIN diferente do que estiver cadastrado em seu cartão/token, você acabará bloqueando o seu PIN.

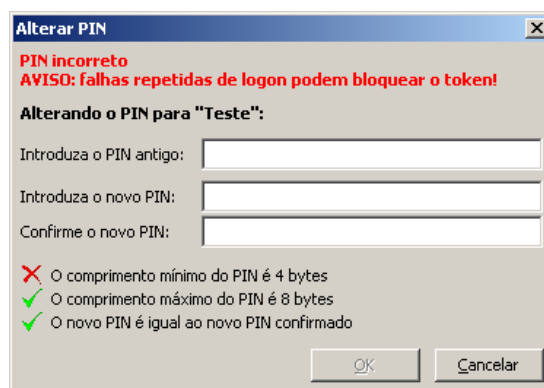
A única forma de desbloqueá-lo será através do uso do PUK e acessando o menu Token > Desbloquear PIN (veja mais detalhes no item 2.2.3).

### Importante - Bloqueio do PUK:

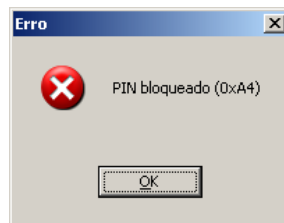
Caso você tente por várias vezes sucessivas utilizar um PUK diferente do que estiver cadastrado em seu cartão/token, você acabará bloqueando todo o seu cartão/token e isso acarretará na perda de todo o conteúdo de seu dispositivo, ou seja, você perderá os certificados e chaves que existirem no dispositivo.

### 2.2.3. Desbloquear PIN

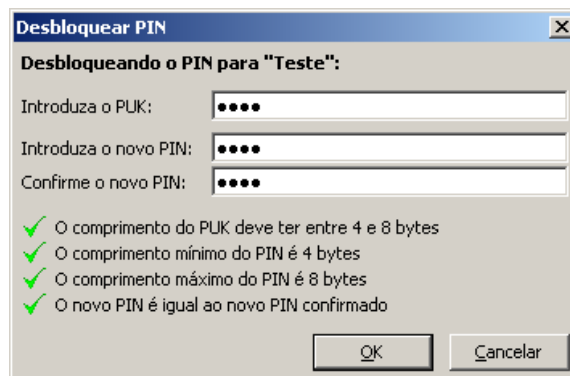
Toda vez que você digitar o PIN incorreto, o aplicativo o alertará através da seguinte mensagem:



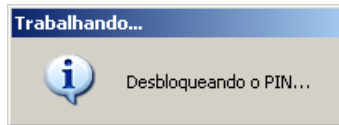
Uma vez esgotadas as tentativas incorretas de entrada do PIN, o aplicativo informará sobre o bloqueio do PIN:



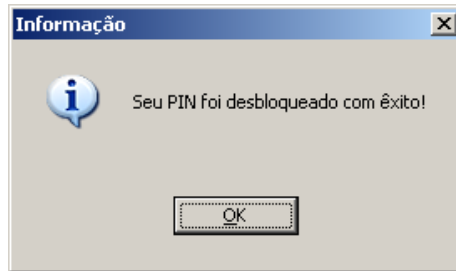
Para desbloquear o PIN, basta que o usuário tenha em mãos a informação do PUK e selecione o item do Menu – **Token > Desbloquear PIN**.



A tela acima será mostrada e, preenchendo-a com a senha de PUK e a nova senha de PIN definida pelo usuário, clique em OK para o SafeSign realizar a ação de desbloqueio do PIN:



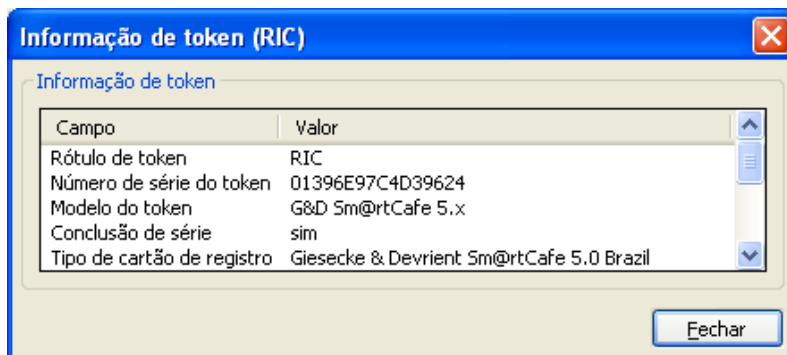
Ao término da ação, uma mensagem de sucesso no desbloqueio será informada e o cartão ficará pronto para uso.



#### 2.2.4. Mostrar informação do token

Selecione o item do Menu – **Token > Mostrar informação do token.**

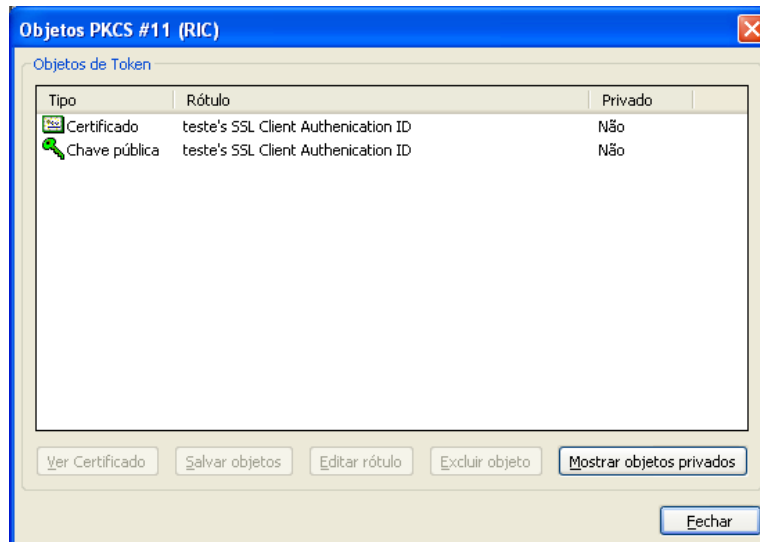
Esta ação mostrará as informações de seu cartão/token, inclusive informando sobre a situação atual do PIN e do PUK do cartão, uma vez que estando OK os mesmos estão aptos para o uso correto do cartão/token.



#### 2.2.5. Mostrar objetos do token

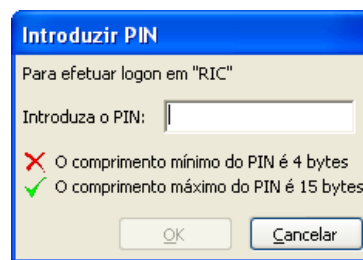
Selecione o item do Menu – **Token > Mostrar objetos do token.**

O item mostrar objetos do cartão/token permite a visualização dos certificados e chaves existentes no mesmo. Logo após a abertura da janela, apenas os itens existentes na memória pública do cartão/token são visualizados, ou seja, apenas os certificados e a chave pública são visualizados conforme a figura abaixo:

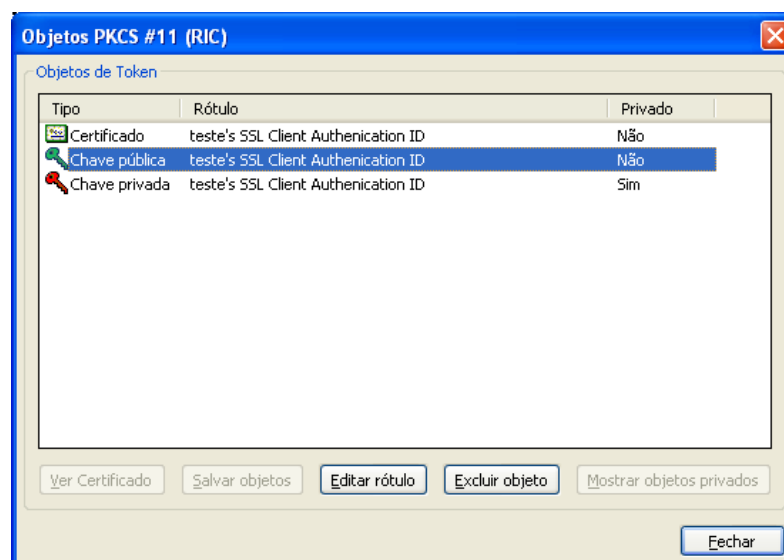


- Para que seja visualizada a chave privada contida na memória privada do cartão/token, é necessário que seja selecionado o ícone “**Mostrar objetos privados**” na janela de “**Objetos PKCS#11**” acima visualizada.

Será solicitada a senha de PIN para realizar este acesso à área privada do dispositivo:



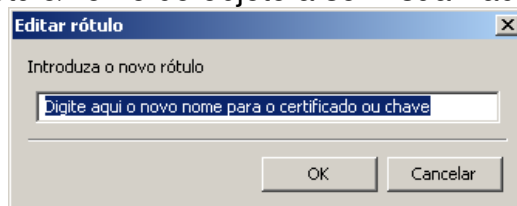
Uma vez digitado o PIN correto e clicado em OK, o SafeSign mostrará na tela “**Objetos PKCS#11**” as informações dos objetos também armazenados na memória privada do cartão/token:



- Selecionando-se um item, como por exemplo, um certificado, o ícone “**Ver Certificado**” será habilitado e permitirá a visualização dos detalhes do certificado conforme já apresentando no item 2.1.1.4.

Selecionando-se qualquer item, as demais opções desta janela serão habilitadas e cada permite que o usuário realize as seguintes funções:

- Opção “**Salvar Objetos**”: permite que os certificados (pois não é possível extrair as chaves do cartão/token) possam ser armazenados em seu computador ou em qualquer outro dispositivo de armazenamento.
- Opção “**Editar rótulo**”: permite que um certificado ou uma chave tenha seu rótulo alterado. Após o clique neste ícone, uma janela surgirá para que o usuário altere o rótulo/nome do objeto a ser visualizado pela aplicação:

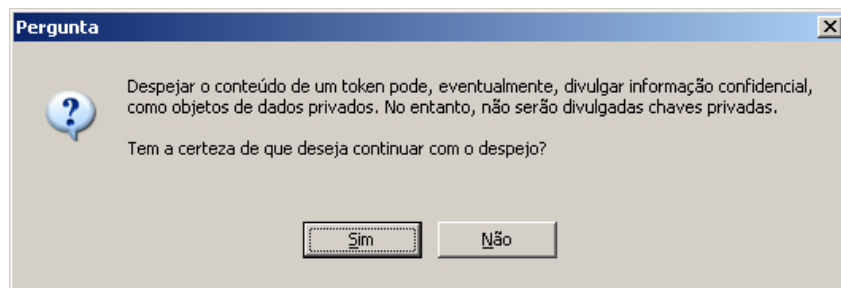


- Opção “**Excluir objeto**”: permite que um certificado ou uma chave seja excluído do cartão/token. Note que caso uma chave associada a um certificado ou o próprio certificado for apagado, o usuário perderá a funcionalidade de utilizar o seu certificado no cartão/token, ou seja, o usuário perderá o seu certificado digital.

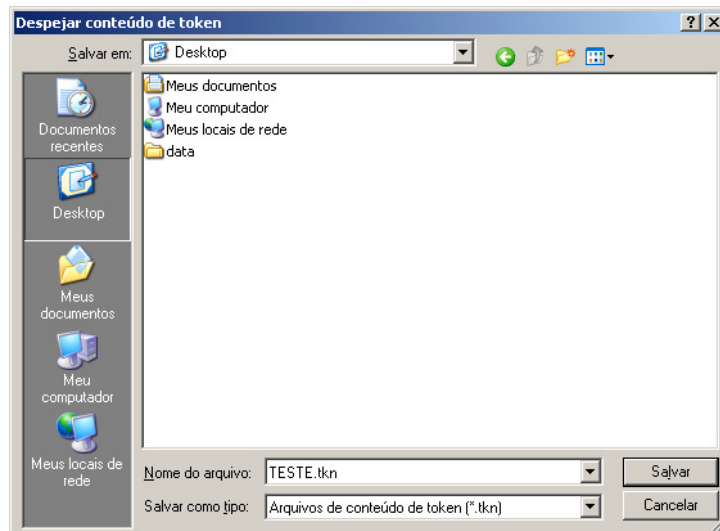
## 2.2.6. Copiar o conteúdo do token para um arquivo

Esta opção do menu permite que as informações existentes no cartão/token sejam copiadas para um arquivo, todavia as chaves privadas são informações que não se podem extrair do cartão/token, as informações que serão armazenadas neste arquivo serão os objetos de dados, certificados e chaves públicas que por ventura estejam no dispositivo no momento que você utilizar esta opção do menu.

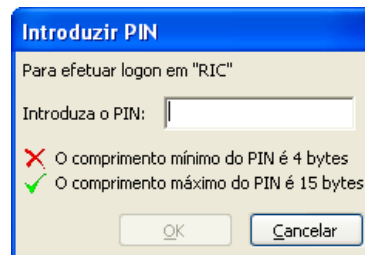
Com seu cartão/token conectado, selecione a opção **Token > Despejar o conteúdo do token** a seguinte mensagem aparecerá:



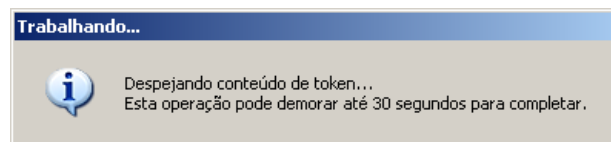
Clique em SIM e a seguinte tela aparecerá para que seja definido o local de armazenamento do arquivo, bem como o nome que deseja para este arquivo:



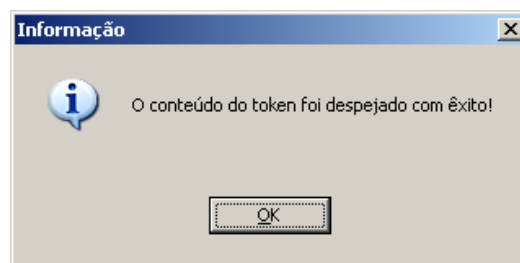
Uma vez definido o nome, no exemplo acima foi “TESTE.tkn”, basta clicar em Salvar. O PIN será exigido para continuidade do processo, digite-o na caixa de texto “**Introduzir PIN**” e clique em OK.



O processo de criação e armazenamento do arquivo será executado:



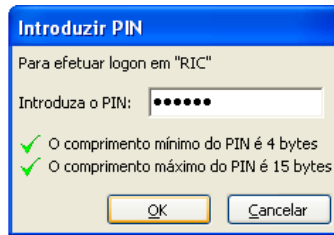
Ao término do processo, uma mensagem de sucesso será informada conforme a figura abaixo e o arquivo estará no local especificado:



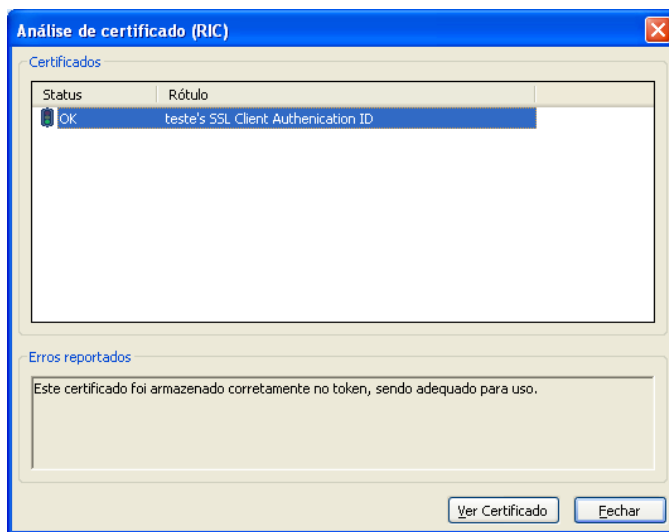
### 2.2.7. Analisar qualidade do certificado

Esta opção do menu faz com que o aplicativo SafeSign rastreie os certificados e chaves armazenadas no cartão/token e determine quais são válidos e quais estão aptos para uso de acordo com as regras de utilização dos mesmos (para assinatura, criptografia e demais aplicabilidades do certificado digital).

Estando com seu cartão/token conectado e selecionando a opção **Token > Analisar qualidade do certificado** a solicitação de PIN aparecerá na tela.



Digite o PIN e clique em OK para que a seguinte tela apareça:



Na figura anterior, vemos um certificado armazenado no cartão/token apto para o uso (está com o status OK), por conter os seus respectivos pares de chaves pública e privada.

Clicando no certificado, a mensagem visualizada pelo aplicativo é de que este certificado foi armazenado corretamente no cartão/token, sendo adequado para uso.

Caso, queira visualizar os detalhes do certificado selecionado, basta clicar no ícone "Ver Certificado" e seguir os mesmos passos apresentados no item 2.1.1.4 deste manual.

## 2.2.8. Alterar tempo de expiração do PIN

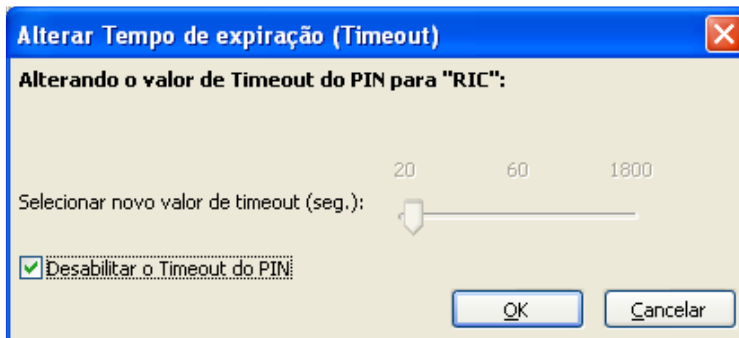
Este item refere-se a uma funcionalidade específica presente em certos cartões Java, uma vez que tal função permite que os cartões controlem o tempo limite de expiração do PIN via aplicação SafeSign.

O uso desta funcionalidade permite que, mesmo após o usuário habilitar o PIN do cartão para assinar um documento ou, por exemplo, autenticar-se em uma ambiente web após um período entre 20 e 1.800 segundos, o cartão exige, para

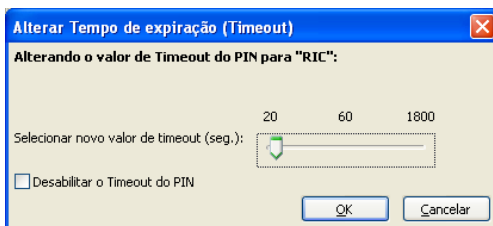
uma nova assinatura ou autenticação, que novamente seja inserido o PIN. Isso impedirá, por exemplo, que o usuário esqueça o cartão habilitado em seu computador e, saindo da frente de seu computador, outra pessoa utilize este cartão uma vez que o mesmo já esteja com o PIN habilitado e por não existir um tempo de expiração (*timeout*) no cartão/token.

Caso seu cartão permita o uso desta funcionalidade, o menu **Cartão > Alterar tempo de expiração do PIN** ficará habilitado para seleção no SafeSign.

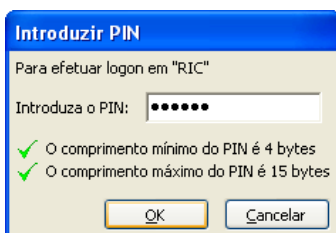
Clicando nesta opção a seguinte tela aparecerá:



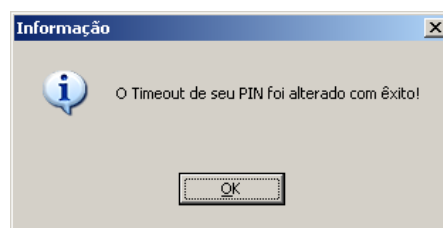
Caso o usuário queira habilitar o tempo de expiração, definindo um tempo de 1200 segundos para expiração do PIN, basta configurar a tela da seguinte forma:



Clique em OK e será exigido o PIN para que a alteração seja efetuada:



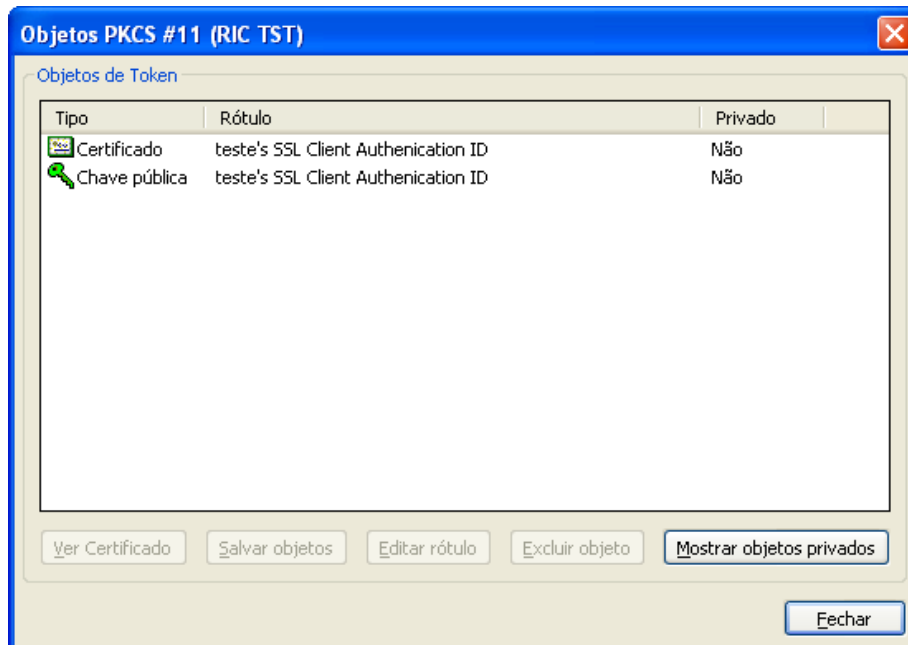
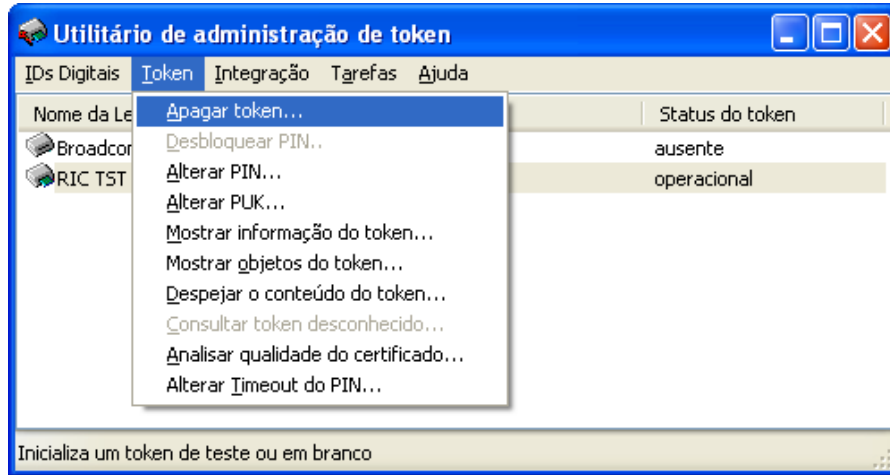
Uma vez confirmado o PIN, a alteração do tempo de expiração será concluída e o usuário receberá a seguinte mensagem:



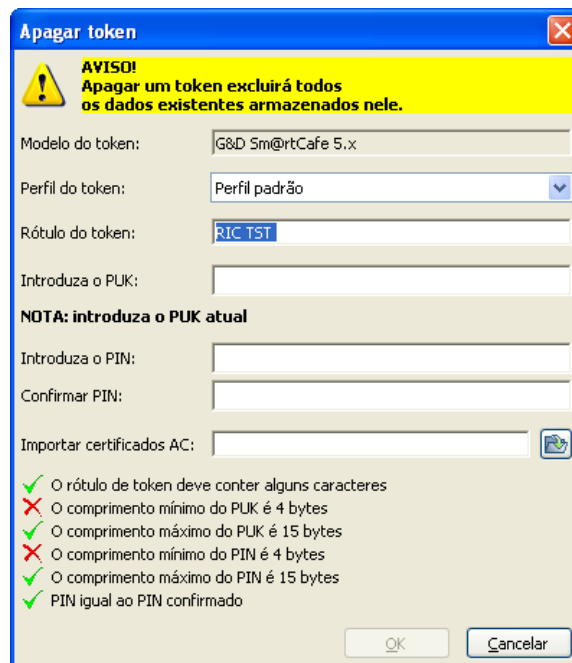
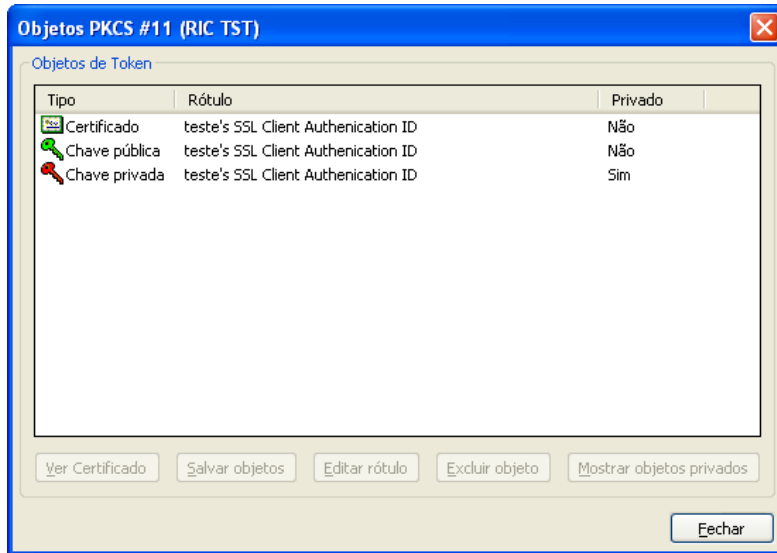
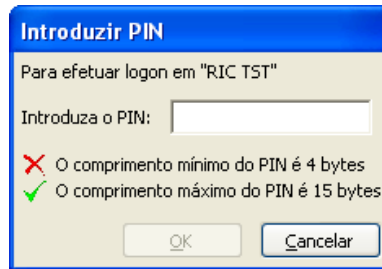


## 2.2.9 Apagar Objetos do token

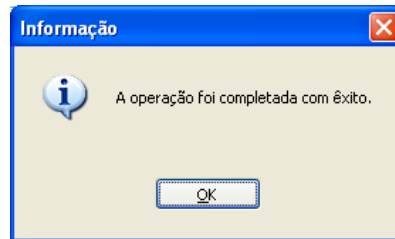
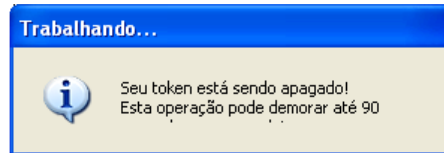
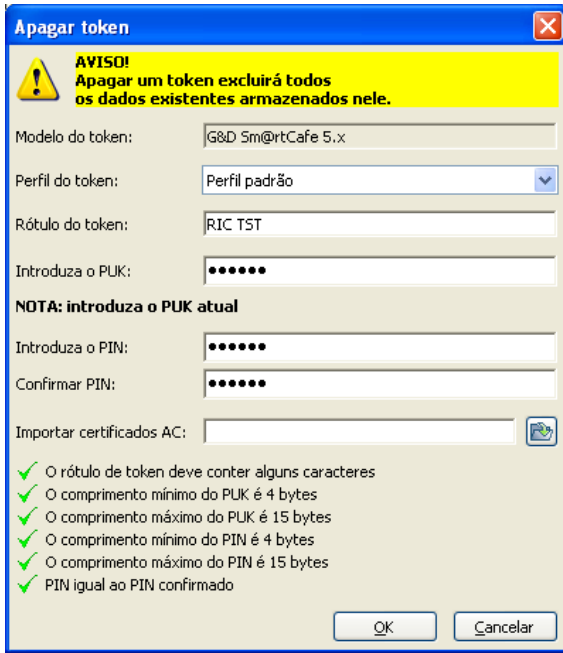
As figuras abaixo exibem os objetos antes de ser utilizada a opção de apagar token.



Para exibir objetos privados é exigido o PIN



Após carregado a tela de apagar token, deve-se informar o PUK e o PIN, após isto será executado o comando e todos os dados armazenados serão apagados.



Após a operação acima, conforme tela abaixo todos os objetos foram apagados, ou seja, o certificado e seus pares de chaves correspondentes.

