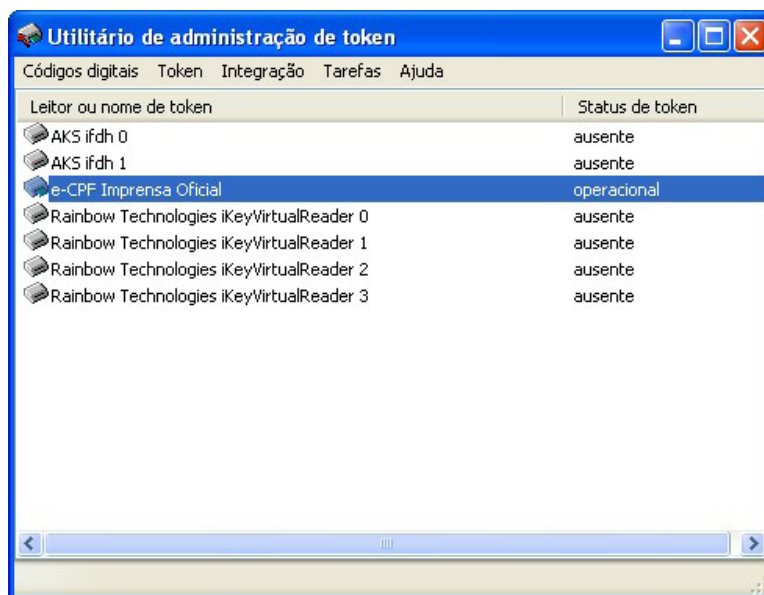


# Guia de utilização do gerenciador de Token e Smart Card



## Pré-requisitos para a instalação

### Software de Certificação Digital (Token Administration)

Para que o processo de instalação obtenha sucesso é necessário obedecer aos seguintes critérios:

- 1) Possuir direitos de administrador ou pertencer ao grupo administradores. Para verificar tal premissa, contate a equipe de suporte de sua empresa, ou profissional de sua confiança para efetuar essa constatação.
- 2) Sistemas operacionais: Windows 2000, XP, Windows Vista e Windows 7, com as atualizações determinadas pelo fabricante. Para sistemas baseados em Linux ou Macintosh, consulte suporte profissional especializado de sua confiança.
- 3) Caso existam outros *drivers* de tokens instalados que não estejam sendo utilizados, recomenda-se a desinstalação dos *drivers* antigos antes de quaisquer outros procedimentos.
- 4) É necessária ao menos uma interface USB em seu computador. Uma vez instalado o token, esse poderá ser conectado em qualquer interface USB, desde que a interface funcione.
- 5) Siga atentamente os passos do manual. A correta sequência de instalação é fundamental.

Para quaisquer esclarecimentos, favor contatar a Central de atendimento. Informações em nosso site: <http://www.imprensaoficial.com.br>.

## Glossário

**AC:** Autoridade Certificadora. É quem certifica a identidade digital de um indivíduo, um servidor confiável ou uma aplicação segura.

**AR:** Autoridade de Registro. É o local onde é obtido o seu certificado digital;

**Agente de AR:** Profissionais a serviço da AR, cujo papel consiste em validar e verificar os documentos apresentados pelo titular do certificado, submetendo essas informações à AC para que ela emita o certificado.

**Cadeia de Certificados (ou cadeia de confiança):** Conjunto de certificados de Autoridades Certificadoras as quais estabelecem a origem confiável de seu certificado digital.

**Cartão inteligente:** É um dos tipos de dispositivos de certificação digital que armazena, comumente, certificados do tipo A3/S3 e superiores. Também é conhecido por *smart card*.

**Certificados (digitais) tipo A1/S1:** Modelo de certificado digital o qual é armazenado no computador. Sua validade é de 1 (um) ano.

**Certificados (digitais) tipo A3/S3:** Modalidade de certificado digital armazenado em um dispositivo de certificação digital. É considerado mais seguro do que o certificado digital tipo A1/S1, e sua validade é de 3 (três) anos.

**Dispositivo de certificação digital:** Contém seu certificado digital e será solicitado sempre nas operações em que a identidade digital seja solicitada. Pode ser um token USB (semelhante a um *pen drive*), um cartão inteligente (*smart card*) ou mesmo o computador (para certificados A1/S1). É igualmente conhecido por *mídia*.

**Driver:** Programa necessário para que um dispositivo seja reconhecido pelo Sistema Operacional, de forma que funcione de acordo com o esperado.

**Identidade Digital:** É a sua identificação (RG, CPF, RNE, etc.) no mundo digital.

**PIN:** *Senha* de acesso ao dispositivo de certificação digital (token USB ou cartão). O PIN será bloqueado após 3 (três) tentativas de acesso incorretas e só poderá ser desbloqueado quando da utilização de cartões com a inserção do PUK.

**Código(s) de emissão 1 e 2:** *Senhas* utilizadas na geração do certificado digital. As mais comuns são do tipo A1/S1.

**PUK:** *Senha* de desbloqueio do PIN. Em alguns dispositivos de certificação digital, o PUK é solicitado para desbloquear o PIN e atribuir um novo. Consulte o manual do dispositivo para verificar se ele possui essa funcionalidade.

**Safesign:** Programa gerenciador de cartões. Produzido pela AET Europe© é utilizado no gerenciamento da maioria dos cartões inteligentes no mercado.

**Senha de administrador:** Compara-se ao PUK. Dependendo do dispositivo, é essa a nomenclatura utilizada. Veja a definição de PUK.

**Senha de revogação:** É uma senha fornecida pelo titular do certificado digital durante a etapa de solicitação, e normalmente encerra de 6 a 12 caracteres. Sua função consiste em revogar o certificado digital pela internet.

**Titular do certificado:** A pessoa que efetivamente terá a posse do certificado digital.

**Senha de usuário:** Compara-se ao PIN. Sua nomenclatura está intimamente ligada às características do dispositivo. Veja a definição de PIN.

**Token USB:** É um dos dispositivos de certificado digital, e normalmente contém certificados A3/S3. Assemelha-se a um *pen drive*.

**Para iniciar o programa Safesign siga os seguintes passos:**

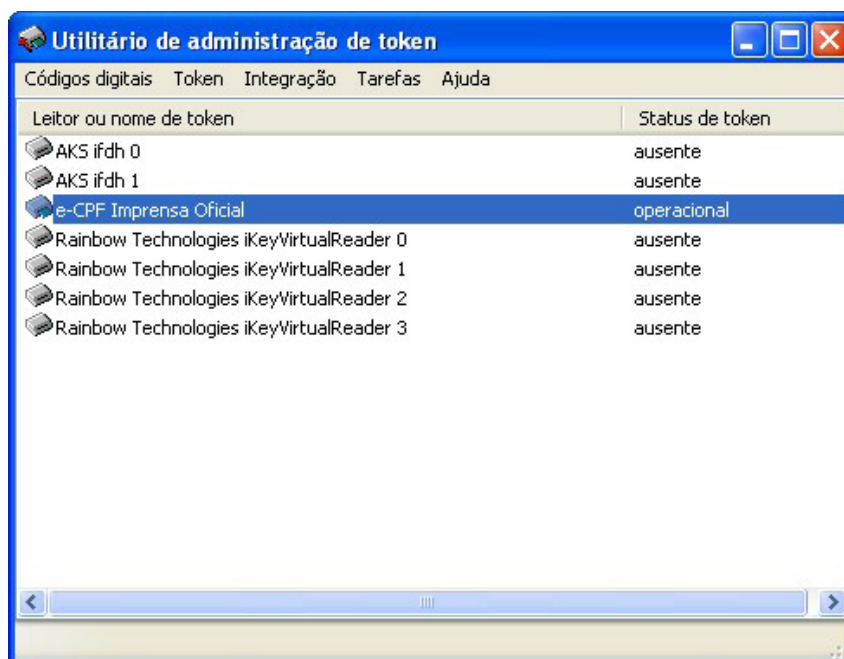
Para iniciar o programa Safesign siga os seguintes passos:

Coloque o cartão na leitora.

**Menu Iniciar / Todos os Programas (Programas) / SafeSign Standard/  
Administração de Token** Ou clique em:

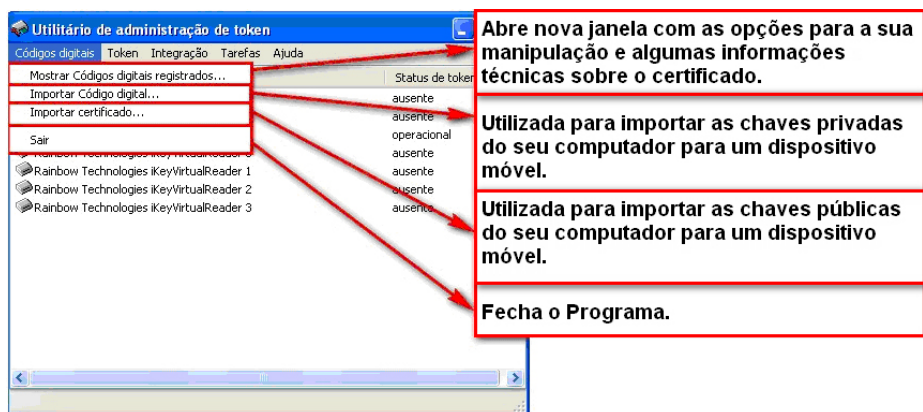


Ao dar início ao programa, nova tela se abrirá:



## Guia de utilização do gerenciador de Token e Smart Card

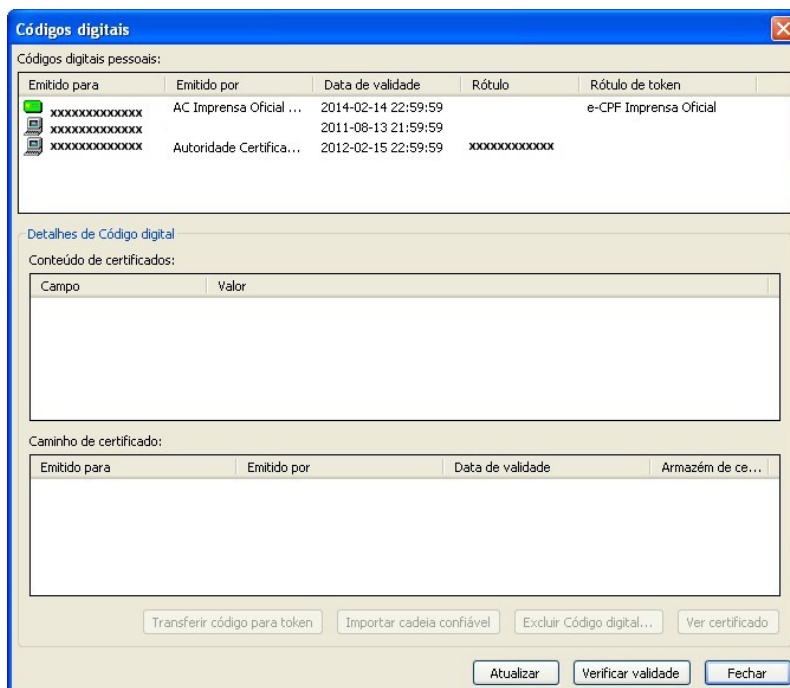
Maio/2011



## Códigos digitais

### Mostrar códigos digitais registrados...

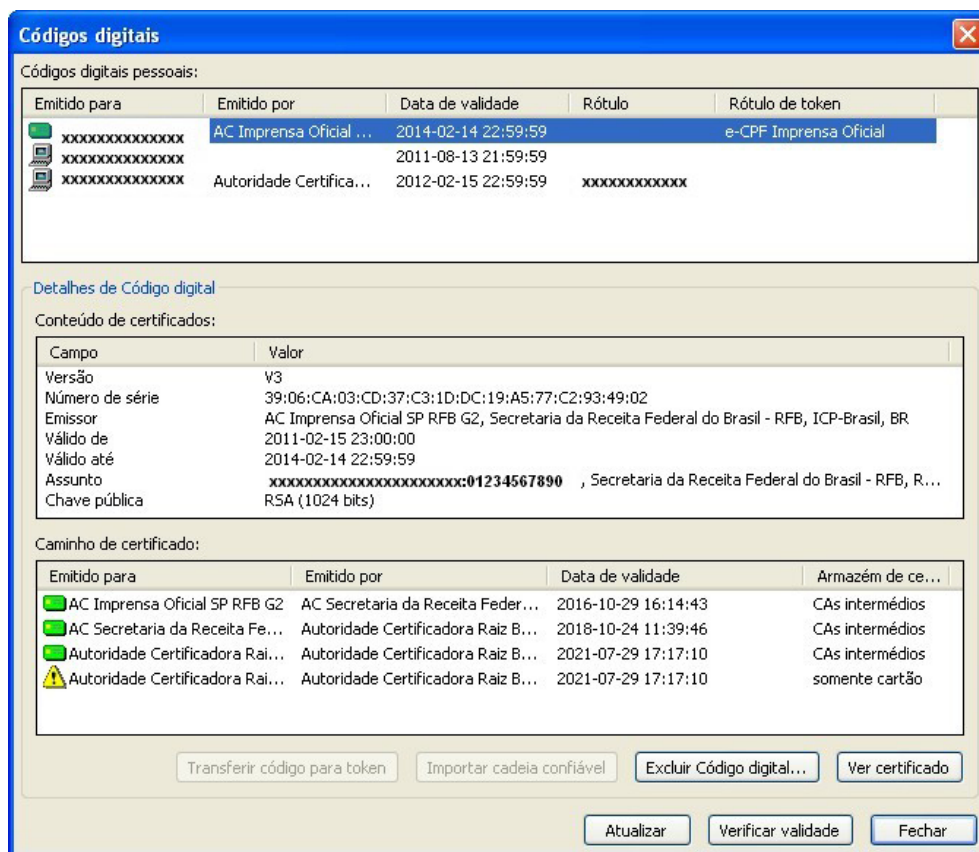
Ao escolher esta opção, a janela apresentará o item. *Alguns dados desta tela podem diferenciar:*



## Guia de utilização do gerenciador de Token e Smart Card

Maio/2011

Selecionando um dos certificados na primeira janela, outras informações constam sobre o mesmo:



Dependendo do tipo do certificado, algumas opções abaixo podem ficar desabilitadas para uso.

The screenshot shows the 'IDs Digitais' application window. It contains a table of digital IDs and a section for detailed certificate information. Red boxes and arrows highlight the following buttons and their functions:

- Transferir ID para token**: Não utilizado.
- Importar cadeia confiável**: Não utilizado.
- Excluir ID Digital...**: Mostrará novos certificados que tenham sido instalados após abertura da janela.
- Ver Certificado**: Mostra os dados do certificado detalhadamente.
- Atualizar**: Verifica todos os certificados e indica quais os que vão expirar nos próximos 30 dias.
- Verificar validade**: Verifica todos os certificados e indica quais os que vão expirar nos próximos 30 dias.
- Fechar**: Fecha a janela.

**JAMAIS utilize essa opção, pois todos e quaisquer dados contidos no cartão serão apagados. Seu certificado será deletado.**

## Importar código digital...

Essa opção é utilizada para importar determinado certificado digital de um arquivo armazenado no seu computador para um dispositivo móvel (Token ou Smart Card).

## Importar certificado...

Essa opção é utilizada para importar a chave pública do seu computador para um dispositivo móvel (Token ou Smart Card).



### Token

Jamais utilize essa opção, pois todos os dados do seu dispositivo serão apagados, inutilizando seu certificado.

Em caso de bloqueio do PIN, a opção é habilitada para uso. É necessário então digitar a senha de desbloqueio do PIN, ou seja, a senha PUK.

Utilize essa opção quando for necessário alterar a senha PIN.

Não utilizado.

Utilize essa opção quando for necessário alterar a senha PUK.

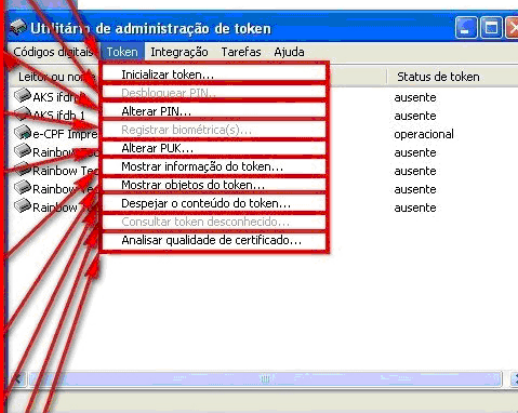
Mostra com detalhes técnicos todas as informações inseridas no token.

Abre nova janela e mostra todos os dados inseridos no dispositivo móvel.

Divulga os dados dos seus certificados. Não é recomendável utilizar essa opção.

Não utilizado.

Analisa a procedência e qualidade dos certificados inseridos dos dispositivos.



### Inicializar Token...

**JAMAIS** utilize essa opção. Esse procedimento apaga todos os dados do seu dispositivo e inutiliza seu certificado.

### Desbloquear PIN...

Opção utilizada para desbloqueio do PIN.

Quando a senha (PIN) é digitada erradamente por 5 (cinco) vezes, o software bloqueia o acesso do cartão. Embora a opção possa ser habilitada para uso, faz-se necessário digitar a senha de desbloqueio do PIN, ou seja, a senha PUK.

**ATENÇÃO: A senha PUK não pode ser digitada erradamente por 5 (cinco) vezes. Isso bloqueia o cartão por completo e implica a emissão de um novo certificado, o qual deve ser pago.**

### **Alterar PIN...**

Opção disponível para alteração da senha PIN.

Você deve digitar a senha PIN antiga, e nos outros dois campos abaixo introduza a nova senha PIN.

Confirmadas as ações, o PIN é alterado para uso normal.

### **Alterar PUK...**

Opção disponível para alterar a senha PUK.

Você deve digitar a senha PUK antiga, e nos outros dois campos abaixo introduza a nova senha PUK.

Confirmadas as ações, o PUK é alterado para uso normal.

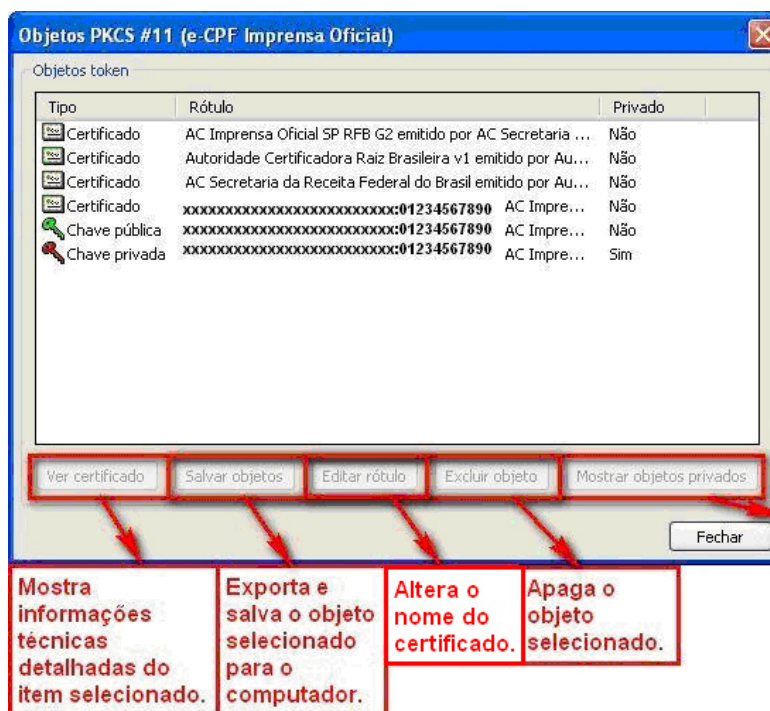
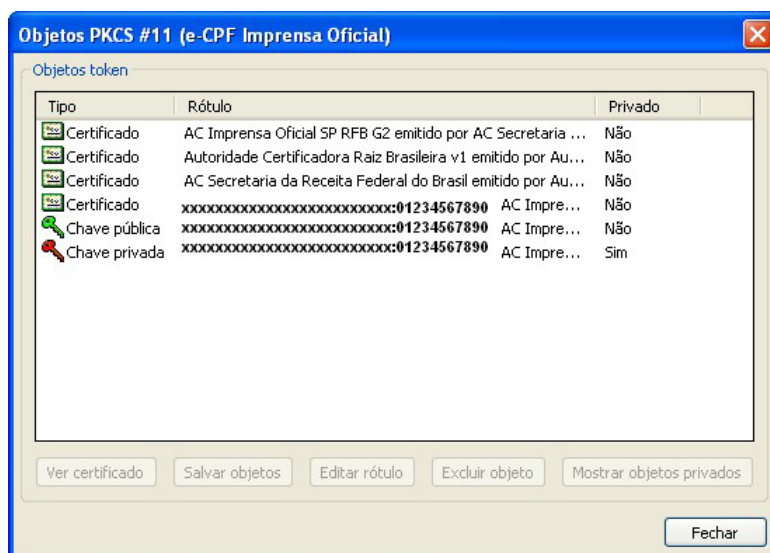
### **Mostrar informações do Token...**

Mostra, com detalhes técnicos, informações inseridas dentro do Token.

### **Mostrar objetos do Token...**

Abre nova janela e mostra todos os dados inseridos dentro do dispositivo móvel:

## Guia de utilização do gerenciador de Token e Smart Card Maio/2011



Dependendo da chave ou certificado selecionado, algumas opções serão habilitadas ou não.

**ATENÇÃO:** O uso da opção **EXCLUIR OBJETO** poderá inutilizar o certificado. Em caso de exclusão de chaves, será necessário emitir um novo certificado mediante pagamento. **JAMAIS utilize essa opção.**

### **Despejar o conteúdo do Token...**

Divulga dados dos seus certificados para fins de suporte. Não é recomendável utilizar essa opção.

### **Consultar Token desconhecido**

Não utilizado.

### **Analisar qualidade de certificado...**

Analisa a procedência e qualidade dos certificados introduzidos no dispositivo. É necessário utilizar o PIN para ter acesso a essa opção.

## **Integração**

### **Instalar o SafeSign no Firefox:**

Não utilizado.

### **Instalar o SafeSign no Entrust:**

Não utilizado.

## **Tarefa**

### **Gerenciar Tarefa:**

Tarefas agendadas para serem executadas quando o cartão é inserido na leitora. Exemplo: verifica e avisa a validade do certificado no cartão.

## **Ajuda**

### **Informação das Versões:**

Exibe dados técnicos sobre a versão do software instalado.

## **Sobre:**

Exibe dados sobre a versão, sem especificações técnicas.

## **Condições de uso**

### Condições gerais

#### Garantia:

A garantia conferida ao Smart Card é de 1 (um) ano a contar da data da nota fiscal. Caso haja necessidade, compareça na AR em que seu certificado foi obtido e traga o Smart Card, leitora, a nota fiscal e descrição do defeito constatado.

O smart card e leitora que apresentarem visíveis sinais de mau uso – partes quebradas, cabos rompidos (se aplicável), conectores amassados, etc. – não serão substituídos. Caso efetuada a substituição, o item substituído será o disponível em estoque, de características técnicas e funcionais iguais ou superiores ao anterior.

Para minimizar problemas de funcionamento, os pré-requisitos deverão ser atendidos.

O programa de gerenciamento Token Administration não tem garantias contra defeitos de fabricação. Dessa forma, substituições não são previstas nem efetuadas. O programa SafeSign Token Administration foi e é exhaustivamente testado em configurações variadas, sem apresentar problemas de incompatibilidade com outros aplicativos. Entretanto, nem todas as situações podem ser previstas e, caso o aplicativo apresente problemas em seu sistema, favor contatar primeiramente o suporte técnico de sua confiança e, caso não seja encontrada uma solução, contate-nos por intermédio da central de atendimento.