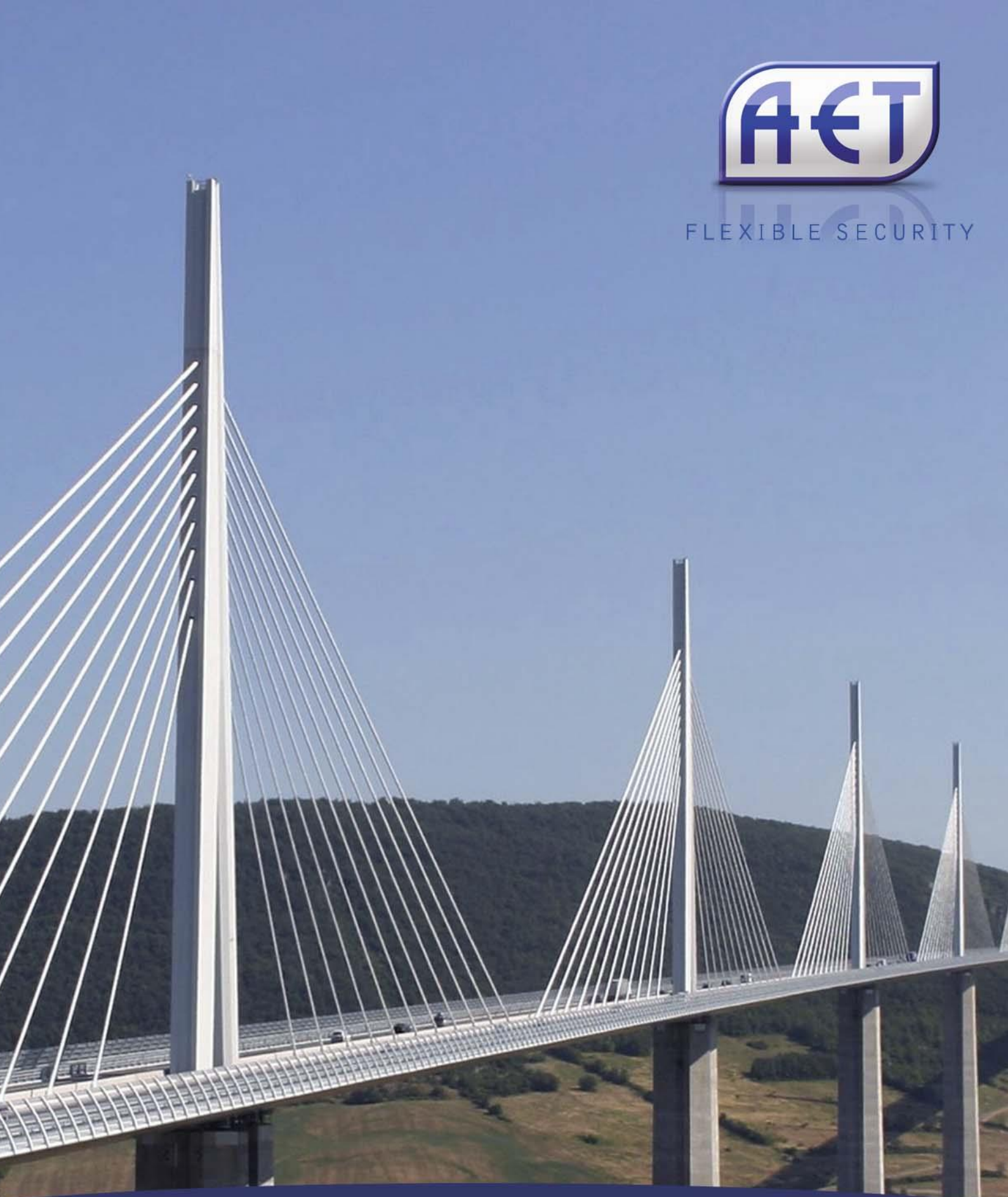

SAFESIGN
IDENTITY CLIENT

SafeSign IC

Manual de Usuário

Aviso

Este documento contém informação de natureza proprietária. Nenhuma parte deste manual pode ser reproduzida ou transmitida em nenhum formato ou de nenhuma forma eletrônica, mecânica ou outra, incluindo a fotocópia e a gravação para qualquer outra finalidade que não o uso pessoal do adquirente sem autorização por escrito da A.E.T. Europe B.V.. Os indivíduos ou organizações que tenham autorização escrita da A.E.T. Europe B.V. para receber esta informação podem apenas utilizá-la para fins de avaliação e orientação.

Toda a informação aqui contida ou é pública ou propriedade detida pela A.E.T. Europe B.V. a qual detém em exclusivo os direitos de patente ou qualquer outra protecção da propriedade intectual relacionada com esta informação. Esta informação está sujeita a alterações bem como a A.E.T. Europe B.V. reserva-se o direito a, sem aviso, fazer alterações aos seus produtos, em resultado de progressos tecnológicos, métodos de fabrico ou questões de segurança.

A instalação ou uso dos produtos da A.E.T. Europe B.V. estão sujeitos a aceitação dos termos e condições contidas no contrato de licenciamento que acompanha cada produto. Nada nesta informação deve ser interpretado como implicando ou garantindo quaisquer direitos, de licença, concessão ou quaisquer outros, a pretexto de direitos de propriedade intelectual e/ou industrial ou relacionado com qualquer informação da A.E.T. Europe B.V..

Os produtos criptográficos estão sujeitos a restrições de exportação e importação, estando obrigado a obtenção prévia das respectivas licenças, antes da expedição deste produto.

A informação contida neste documento é fornecida tal qual, sem garantias de qualquer espécie. A menos que expressamente acordado por escrito, a A.E.T. Europe B.V. não garante a exatidão da informação aqui contida. O documento pode conter inexatidões técnicas ou erros tipográficos. Periodicamente serão efectuadas alterações à informação contida neste. A A.E.T. Europe B.V. mais reserva o direito de, em qualquer altura proceder a quaisquer alterações ou desenvolvimentos das especificações e informações aqui descritas.

A A.E.T. EUROPE B.V. REFUTA, POR ESTE MEIO TODAS AS GARANTIAS E CONDIÇÕES RESPEITANTES À INFORMAÇÃO AQUI CONTIDA, INCLUINDO TODAS AS CONDIÇÕES DE VENDA E APTIDÕES PARA UM DETERMINADO FIM, LEGALMENTE RECONHECIDOS. EM NENHUM CASO A A.E.T. EUROPE B.V. SERÁ RESPONSÁVEL, MESMO QUE NO CONTRATO, LEI OU OUTRA, POR QUAISQUER DANOS ESPECIAIS OU INDIRECTOS DEVIDO AO USO INDEVIDO, INCLUINDO ENTRE OUTROS OS DANOS RESULTANTES DA FALTA DE USO, DADOS, BENEFÍCIOS, RECEBIMENTOS, OU DOS CLIENTES QUE POSSAM SURGIR RELACIONADOS COM A UTILIZAÇÃO OU EXECUÇÃO DA INFORMAÇÃO CONTIDA NESTE DOCUMENTO.

Créditos: Este produto inclui software criptográfico escrito por Eric A. Young (eay@cryptsoft.com). Este produto inclui software escrito por Tim J. Hudson (tjh@cryptsoft.com).

Informação do Documento

Título: SafeSign IC
Manual de Usuário

Identificador de Documento: AET_PR.SS_42.5_0001_pt

Projeto: Documentação de Usuário do SafeSign IC

Histórico de versões

Versão	Data	Autor(es)	Alterações
1.0	12-08-2013	Pedro Lopes	Versão inicial
1.1	07-11-2014	Pedro Lopes	Inclusão de informação adicional sobre Mac OS X, Linux e suporte para certificados de atributo
1.2	20-05-2015	Pedro Lopes	Inclusão do capítulo de renovações e também de uma nova funcionalidade de exportação de uma ID Digital.
1.3	26-04-2016	Pedro Lopes	Inclusão da nova funcionalidade de reciclagem do token.
1.4	08-09-2017	Pedro Lopes	Atualização da versão do kit de desenvolvimento para 5.9. Correção de bugs e melhorias nas funcionalidades de inserção da senha ao salvar o arquivo PKCS12 e inclusão da cadeia completa no arquivo PKCS12. Alteração do menu de Informação das Versões.

Glossário

Termo	Definição
PKI	Infraestrutura de Chaves Públicas (Public Key Infrastructure)
PKCS#11	Public-Key Cryptographic Standards (Utilizada para comunicar com cartões inteligentes e módulos de hardware seguros)
CSP	Cryptographic Service Providers

Índice

Lista de Figuras

Sobre o Produto

O SafeSign IC é um pacote de software que pode ser utilizado para aumentar a segurança de aplicações que suportem a utilização de tokens através de interfaces PKCS#11 ou Microsoft CryptoAPI.

O pacote inclui uma biblioteca compatível com a norma PKCS#11, juntamente como um Provedor de Serviços Criptográficos (Cryptographic Service Provider - CSP) e um Provedor de Armazenamento de Chaves (CNG Key Storage Provider - KSP), permitindo aos usuários o armazenamento de dados públicos e privados num token pessoal, quer este assuma o formato de um smart card/cartão inteligente, token USB ou cartão SIM. Para além disso, inclui também a Applet SafeSign IC PKI, possibilitando que os usuários utilizem qualquer cartão Java Card 2.1.1 / Java Card 2.2 (ou superior) compatível com o middleware SafeSign IC.

Ao combinar a observância das principais normas e protocolos adotados pela indústria com a flexibilidade e usabilidade que o caracterizam, o SafeSign IC pode ser usado com múltiplos cartões inteligentes, tokens USB, sistemas operacionais e leitoras de cartões.

O SafeSign IC permite aos usuários que inicializem e usem o token para encriptação, autenticação ou assinatura digital e inclui toda a funcionalidade necessária para a utilização de tokens de hardware numa vasta gama de ambientes PKI.

O SafeSign IC é disponibilizado através de um instalador para os seguintes ambientes Windows (com os últimos Service Packs instalados):

Windows 7, Windows 8, Windows Server 2008 e Windows Server 2012[1].

O SafeSign IC é ainda disponbilizado noutras plataformas:

Mac OS X

Linux (SuSe, RedHat, Debian, Ubuntu)

Sun® Solaris

Note-se que o SafeSign IC suporta virtualização tipo I (ou nativa/bare-metal hypervisors), ou seja, a instalação em servidores/estações de trabalho onde esteja a ser executado, por exemplo, um sistema VMware ESX, Citrix XenDesktop ou Oracle/Sun VM VirtualBox diretamente em bare-metal hypervisors. A virtualização de tipo II (ou hosted hypervisors), como o VMware Workstation, não é suportada.

[1] O Windows Server 2012 apenas funciona em processadores x64.

Sobre o Manual

Este manual está especialmente desenhado para administradores / usuários avançados do SafeSign IC para Windows, que procurem utilizar o seu token compatível com SafeSign IC para aumentar a segurança das suas comunicações via Internet e utilizá-lo para realizar operações avançadas.

Para isso este documento descreve a funcionalidade do aplicativo SafeSign IC, que lhe permite operações como a inicialização do token, de modo a preparar o mesmo para um processo de geração de par de chaves e obtenção de certificado digital.

De modo a preparar o seu token SafeSign IC para ser utilizado, deve seguir as instruções deste manual que descreve como o inicializar e efetuar diversas operações, como sejam a consulta dos conteúdos do token e a alteração do seu PIN.

Cada atividade descrita tem uma determinada sequência de passos, identificados pelos números colocados do lado esquerdo do texto, por exemplo, 1

Cada passo que requeira uma ação da sua parte encontra-se assinalado com o símbolo >

De modo a completar a atividade desejada, deverá percorrer os passos descritos e as ações que lhe forem solicitadas, considerando as notas assinaladas a negrito com e as observações assinaladas a azul com

Este documento é parte da documentação de usuário do SafeSign IC.

1 Aplicativo SafeSign IC

1.1 Introdução

O pacote de instalação do SafeSign IC instala a biblioteca PKCS#11 do SafeSign IC e o Provedor de Serviços Criptográficos (CSP), permitindo aos usuários armazenar dados públicos e privados num token pessoal, seja ele um smart card/cartão inteligente, um token USB ou um cartão SIM.

Para que o seu token compatível com o SafeSign IC interaja com as bibliotecas PKCS#11 (que suporta aplicações como Mozilla Firefox) e Microsoft CryptoAPI CSP (que suporta aplicações como o Outlook), é necessário inicializar e gerir o seu token. Isto pode ser feito através da utilização do aplicativo SafeSign IC incluído no pacote de instalação.

Para personalizar o seu token deverá inicializá-lo, o que (poderá) envolve(r) eliminar toda a informação que possa estar armazenada no token, escrever a estrutura PKCS#15 do SafeSign IC no token e (após alterar o PIN de transporte do token, se configurado) associar-lhe uma etiqueta e configurar o PIN/PUK pessoal.

1.2 Itens do menu

O menu do aplicativo oferece cinco opções:

1. Token, incluindo funcionalidades como inicializar o token e alterar o PIN;
2. IDs Digitais, incluindo funcionalidades como visualizar e importar as suas IDs Digitais e certificados de AC;
3. Auto Inscrição, para descarregar um certificado A1 ou A3 do servidor da AC;
4. Configurações, neste menu é possível instalar o SafeSign no Firefox bem como configurar um servidor de proxy para a comunicação com o servidor da AC.
5. Ajuda, para aceder a informações úteis sobre o aplicativo e ambiente da instalação.

1.2.1 Menu Token

O capítulo 3 versará sobre o menu **Token** do aplicativo, com as seguintes secções:

Seção 3.2 : Inicializar Token
Seção 3.3 : Limpar Token
Seção 3.4 : Reciclar Token
Seção 3.6 : Alterar PIN de Transporte
Seção 3.7 : Desbloquear PIN
Seção 3.8 : Alterar PUK
Seção 3.9 : Mostrar Informação de Token

Seção 3.10 : Mostrar Objetos do Token

Seção 3.11 : Mostrar Certificados de Atributo do Token

Seção 3.12 : Exportar Conteúdo do Token

Seção 3.13 : Consultar Token desconhecido

Seção 3.14 : Alterar Timeout do PIN

1.2.2 Menu IDs Digitais

O capítulo 2 versará sobre o menu de **IDs Digitais** do aplicativo:

Seção 2.1 : Transferir ID Digit

Seção 2.2 : Eliminar ID Digital

Seção 2.3 : Visualizar Certificado

Seção 2.4 : Verificar Validade

Seção 2.5 : Exportar ID Digital

1.2.3 Menu Auto Inscrição

Este capítulo explica como todo o processo de auto inscrição se desenrola:

Seção 4.1 : Pré-Requisitos

Seção 4.2 : Levantamento de um certificado de identidade do tipo A3

Seção 4.3 : Levantamento de um certificado de identidade do tipo A1

1.2.4 Menu Renovação

Todo o processo de renovação será detalhado neste capítulo:

Seção 5.1 : Pré-Requisitos

Seção 5.2 : Renovação de um certificado de identidade do tipo A3

Seção 5.3 : Renovação de um certificado de identidade do tipo A1

1.2.5 Menu de Configurações

O capítulo de configurações do SafeSign IC contém as seguintes opções:

Seção 1.4.1 : Configurar Firefox

Seção 1.4.2 : Configurar Proxy

1.2.6 Menu de Ajuda

Este capítulo faz uma breve descrição do seguinte:

Seção 1.5.1 : Sobre (o Fornecedor)

Seção 1.5.2 : Sobre o SafeSign

Seção 1.5.3 : Informação das Versões

Remoção do token

Durante todas as operações do token (como inicialização do Token, alteração de PIN, etc.) descritas neste manual, não deve remover o token da leitora de smart cards ou porta USB até que as mesmas tenham terminado. A remoção do token pode danificar os dados armazenados no mesmo.

Quando a sua leitora de smart cards tiver uma luz LED, não deve remover o smart card da leitora enquanto a luz estiver piscando ou estiver vermelha.

1.3 Leitoras e Tokens

Encontrará um atalho para o aplicativo no menu Programas, clicando em **Iniciar > Todos os programas > SafeSign Standard > SafeSign IC**:

Figura 1: Menu SafeSign IC

Quando clicar em **SafeSign IC**, o aplicativo abrir-se-á:

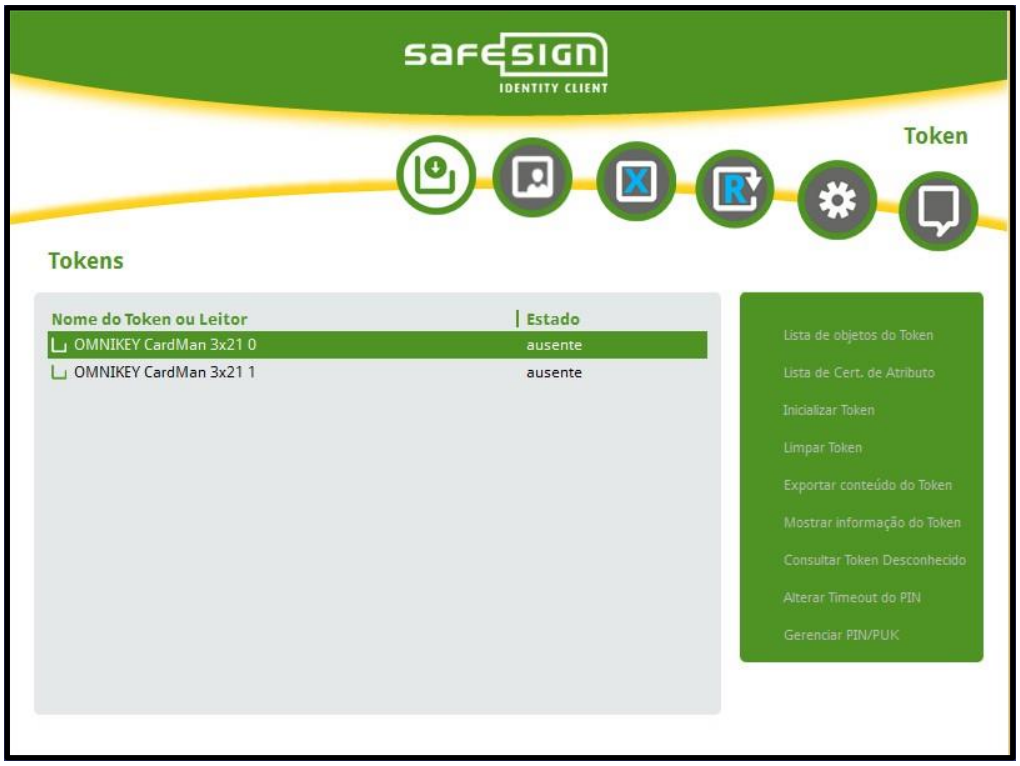

Figura 2: Aplicativo SafeSign IC: Nome da leitora

Esta janela mostra as leitoras de smart cards/tokens instalados no seu PC e o respetivo estado. Quando nenhum token está inserido numa leitora de smart cards, será listada marca/modelo da mesma (ver Figura 2).
Quando não é visível nenhuma leitora de smart cards, deverá verificar se existe alguma leitora de smart cards instalada e se a mesma está funcionando corretamente. Sem uma leitora de smart cards funcional (e os seus respetivos serviços) o SafeSign IC não pode ser usado.
De notar que é possível ter mais do que uma leitora de smart cards no seu PC, ou uma combinação de uma leitora PC/SC e um token USB.
Todas as leitoras de smart cards que estão instalados serão listadas e permitirão a inicialização de um token.

Nota

Neste manual, a expressão "um token numa leitora de smart cards" pode referir-se a um smart card inserido numa leitora de smart cards ou a um token USB conetado a uma porta USB.

Quando um token é inserido na leitora de smart cards, o nome do token torna-se visível. Neste caso, existem duas possibilidades[2]: ou o token está em branco, não tendo sido ainda inicializado:

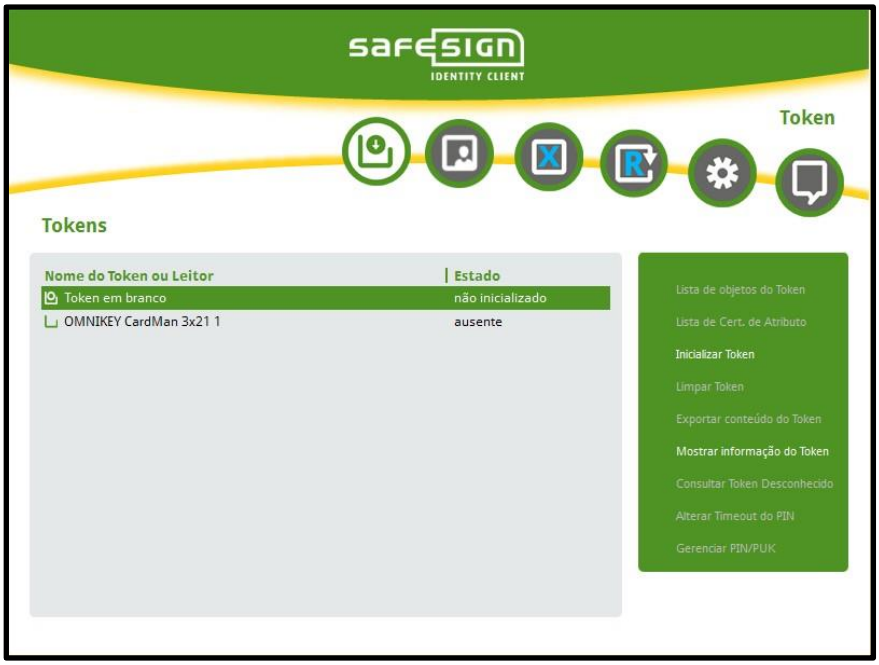

Figura 3: Aplicativo SafeSign IC: Token não inicializado

Ou o token já foi inicializado e possui uma etiqueta de token:

[2] Se o token for suportado e reconhecido. Se não for o caso, o seu token pode ser identificado como um token desconhecido (ver seção 3.13).

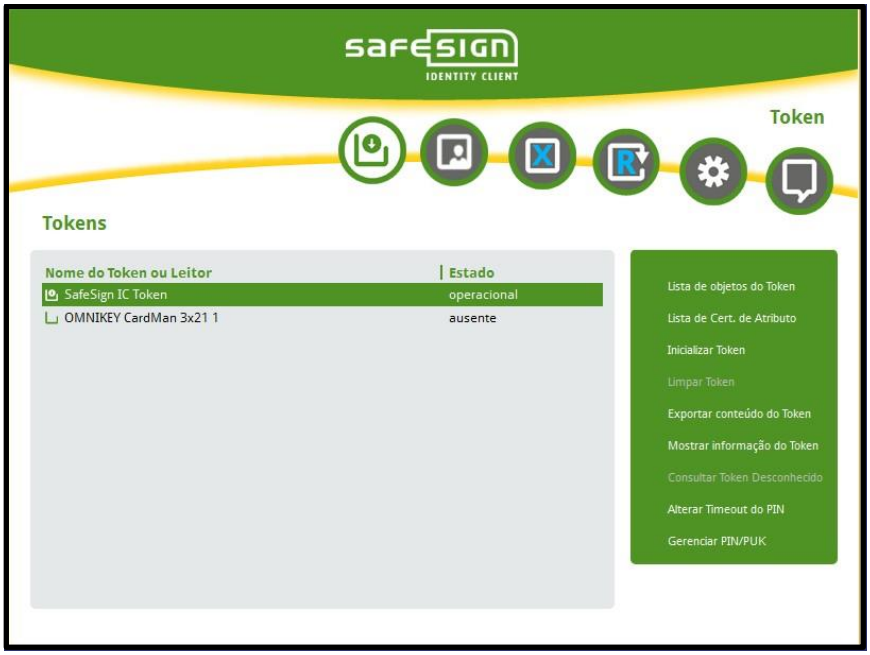

Figura 4: Aplicativo SafeSign IC: Token Operacional

Múltiplos Tokens e leitoras

É possível ter instaladas múltiplas leitoras de smart cards ou tokens USB (ou uma combinação de ambos).

Poderá ter vários cartões/tokens, por exemplo, um utilizado para o e-mail pessoal, e outro utilizado para o e-mail institucional. Ambos podem ser apresentados num só computador, em leitoras separadas, e pode usar as funcionalidades do aplicativo SafeSign IC para cada um destes cartões/tokens.

A imagem seguinte é um exemplo de como o aplicativo SafeSign IC se parece quando estão instalados simultaneamente uma leitora de smart cards e um token USB e quando ambos estão inicializados.

Figura 5: Aplicativo SafeSign IC: Múltiplos tokens operacionais

Disponibilidade do Token

Quando um token está inserido na leitora, o aplicativo SafeSign IC irá selecioná-lo automaticamente (destacando-o com uma barra colorida). Quando estão inseridos dois (ou mais) cartões nas leitoras, será selecionado o último a ser inserido (como ilustrado pela Figura 5).

Nota

Será necessário selecionar um dos tokens para executar ações tais como Alterar PIN (disponível no menu Token) ou Importar ID Digital (disponível no menu IDs Digitais). Isto faz sentido uma vez que é necessário especificar primeiro a qual token pretende alterar o PIN ou para qual deseja importar uma ID Digital.

1.4 Menu de Configurações

O menu de Configurações do aplicativo SafeSign IC permite alterar configurações da aplicação como também instalar o SafeSign no Firefox.

1.4.1 Configurar Firefox

Na janela do aplicativo SafeSign IC, selecione **Configurações > Configurar Firefox**:

Figura 6: Aplicativo SafeSign IC: Instalar o SafeSign no Firefox

Após selecionar essa opção, o instalador do Firefox é carregado:

Figura 7: Instalador Firefox: Instalar SafeSign no Firefox

A janela apresentada irá listar todas as versões do Firefox instaladas no seu sistema, para que possa identificar aquela onde pretende instalar o SafeSign IC como um módulo de segurança.

Selecione o navegador Firefox desejado a partir da lista e clique **Instalar**

Ao selecionar o Firefox a partir da lista e ao clicar **Instalar**, a biblioteca PKCS#11 do SafeSign IC será instalada como módulo de segurança nessa versão do Firefox, processo após o qual será apresentada a janela ilustrada pela Figura 8.

Figura 8: Instalador Firefox: O SafeSign foi instalado com sucesso

Clique em **Fechar**

1.4.2 Configurar Proxy

Pode ser configurado um proxy, para a comunicação com o servidor da AC. O proxy pode ser configurado acessando o menu de **Configurações > Configurar Proxy.**

Figura 9: Configurações : Configurar Proxy

Ao clicar pela primeira vez para configurar o proxy, a janela irá ser idêntica a apresentada na Figura 9. Para o proxy ser válido, será necessário preencher os dados do nome de anfitrião, porto e também qual o protocolo a ser utilizado. Como pode ver na imagem abaixo com os campos preenchidos.

Figura 10: Configurar Proxy : Inserir dados

Depois de preencher os campos, pode testar a ligação, o que originará a realização de um PING ao anfitrião no porto indicado.

- Clicar em **Testar**

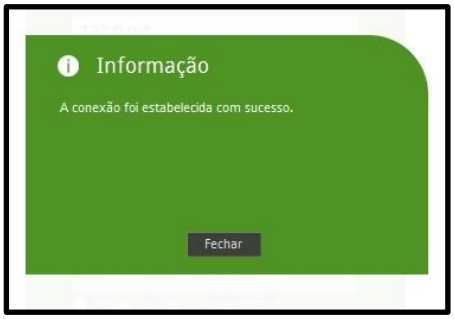

Figura 11: Configurar Proxy : Conexão establecida com sucesso

Neste caso a ligação foi estabelecida com sucesso. Mas em outros casos a ligação pode falhar como mostra na imagem seguinte.

Figura 12: Configurar Proxy : Erro ao tentar comunicar

É também possível configurar o proxy com autenticação. Nesse caso a opção "**Ativar opções de autenticação**" tem de estar ativa. Para ativar clique sobre a opção.

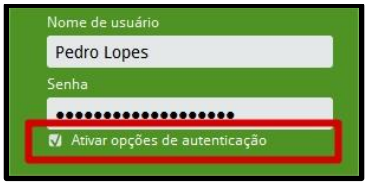

Figura 13: Configurar Proxy : Opções de autenticação ativas

Depois de ativar a opção, é permitido escrever nos campos nome de usuário e a senha.

Nota

Se testar a ligação com as opções de autenticação ativas, estas não serão verificadas. Pois o teste apenas consta em verificar se o anfitrião está na rede e se é possível estabelecer uma comunicação com o mesmo. A imagem seguinte prova desse fato.

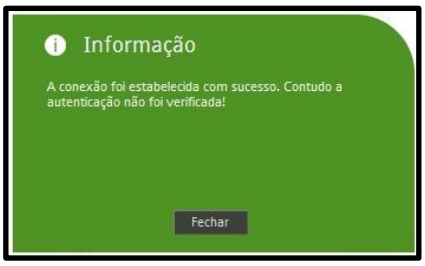

Figura 14: Configurar Proxy : Conexão com êxito, autenticação não verificada

Para os dados serem salvos é necessário que clique no botão “Salvar”. Depois de clicar e os dados guardados com sucesso é mostrada uma mensagem de sucesso.

Figura 15: Configurar Proxy : Mensagem de configurações salvas

1.5 Menu de Ajuda

O menu de Ajuda do aplicativo SafeSign IC disponibiliza os itens descritos nas seções que compõem este capítulo.

1.5.1 Sobre

Como é possível verificar na Figura 16, o item **Sobre** apresenta informações sobre o fornecedor que distribuiu o aplicativo SafeSign IC que o usuário está utilizando.

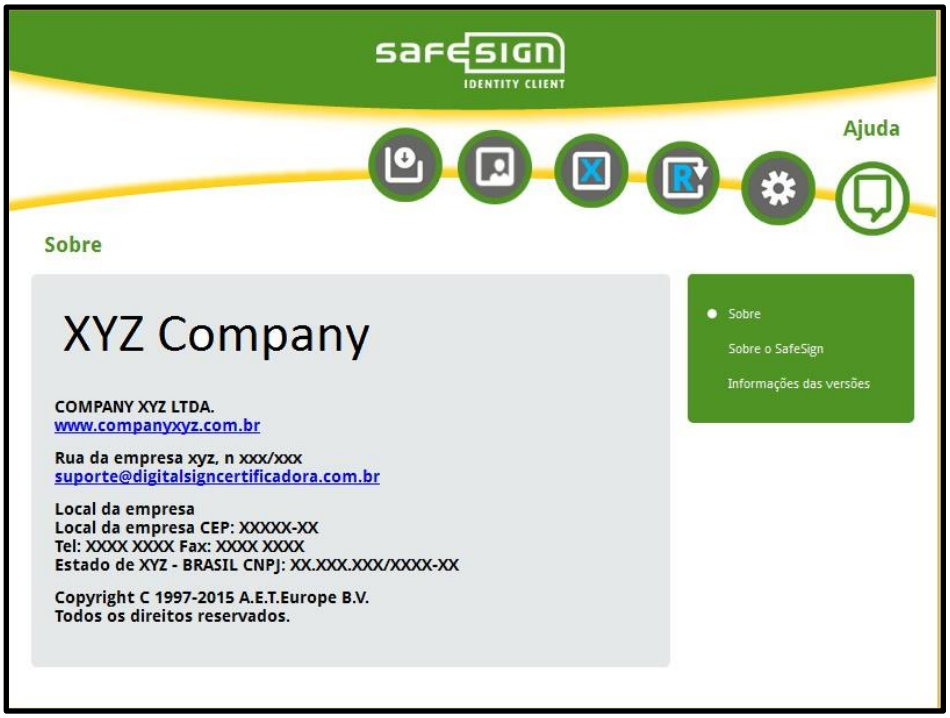

Figura 16: Aplicativo SafeSign IC: Sobre Informações do Fornecedor

1.5.2 Sobre o SafeSign

O item **Sobre o SafeSign** apresenta informações sobre o aplicativo SafeSign IC, tal como ilustrado pela Figura 17.

Figura 17: Aplicativo SafeSign IC: Menu Sobre SafeSign IC

1.5.3 Informação das Versões

O item **Informação das Versões** abre uma caixa de diálogo semelhante à Figura 18, contendo dados relevantes sobre a versão do SafeSign IC que se encontra instalada, bem como a versão das respetivas dependências.

Figura 18: Aplicativo SafeSign IC: Informação das Versões

Esta informação é particularmente útil em caso de problemas na utilização do aplicativo, permitindo que o serviço de Suporte identifique rapidamente que versão tem instalada. Também poderá guardar esta informação num ficheiro, para que possa facilmente enviar essa informação em anexo a um e-mail.
Para isso, basta clicar em **Salvar em arquivo** para gerar o respetivo arquivo (e nomeá-lo em concordância) e incluí-lo quando contatar o serviço de Suporte do seu fornecedor.

1.6 Multilíngua

Foi implementado suporte multilíngua de forma a criar maior flexibilidade tanto para o usuário como para o administrador. Pode-se supor que um administrador, e não o próprio usuário, instala o SafeSign IC num PC de um usuário, escolhendo uma determinada língua. O usuário terá sempre a liberdade de alterar a língua usada pelo aplicativo no SafeSign IC. Em termos práticos, a língua definida em Região e Idioma do computador do usuário será utilizada por omissão como a língua do SafeSign IC, sem que o usuário tenha que alterar qualquer definição para tal.

Nota

A língua do instalador passo-a-passo e dos itens do SafeSign IC no menu Iniciar pode ser selecionada durante a instalação do SafeSign IC. Contudo esta língua é estática e não pode ser alterada uma vez selecionada (sem desinstalar o SafeSign IC) devido a limitações do Windows. A língua do SafeSign IC e dos seus utilitários é dinâmica e pode ser alterada para qualquer uma das línguas suportadas.

O SafeSign IC suporta as seguintes línguas:

- Inglês
- Árabe
- Português: Brasil

A Figura 19 ilustra o aspecto do aplicativo SafeSign IC quando se encontra a ser utilizado em idioma Inglês.

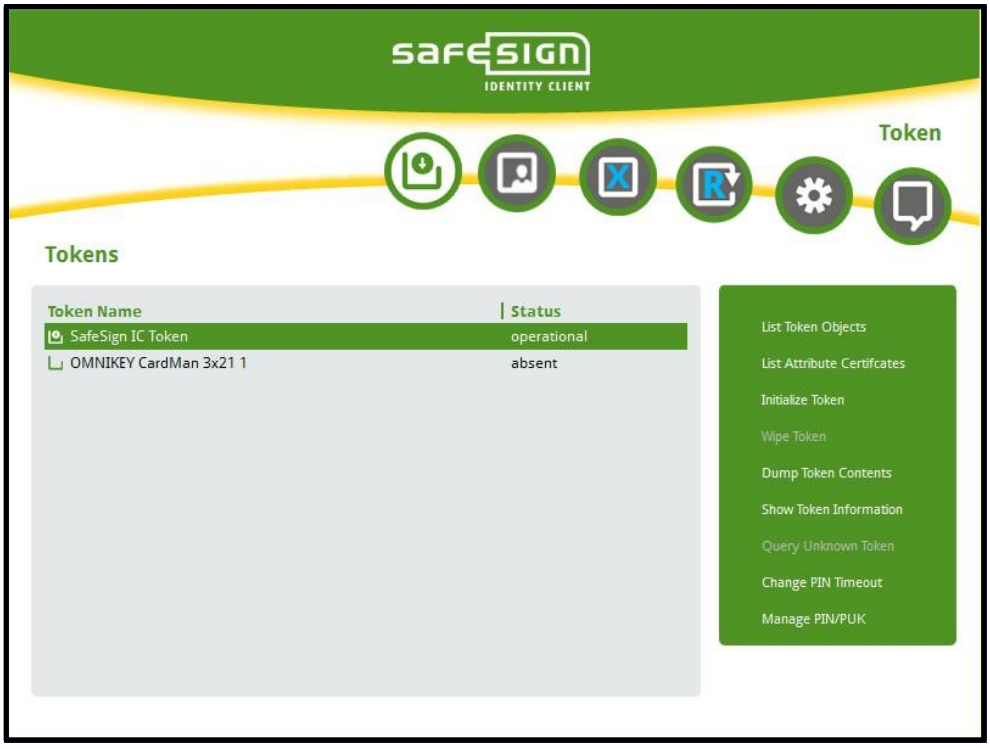

Figura 19: Aplicativo em Idioma Inglês

Para além disso, o aplicativo também se encontra disponível em Árabe, como é visível na figura que se segue.

Figura 20: Idioma Árabe

O usuário pode definir o idioma que preferir para o SafeSign IC e seu aplicativo, em **Iniciar > Painel de Controlo > Região e Idioma**, selecionando no campo **Formato** a língua pretendida:

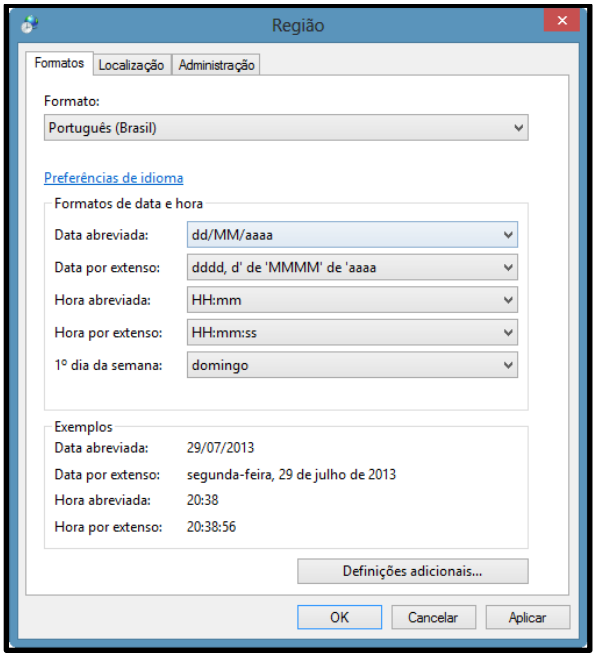

Figura 21: Região e Idioma: Formato

Para definir o idioma do sistema (para programas não Unicode) de forma a aplicar-se a todos os usuários, é necessário definir/alterar o idioma do sistema (na aba **Administração**).

Nota

Quando não está definido um idioma específico ou quando o idioma selecionado não é suportado pelo SafeSign IC, o idioma definido por defeito para o SafeSign IC será o Inglês.

Também poderá precisar de selecionar a combinação de idioma de entrada e layout do teclado.

Nota

Apesar de ter sido testada a visualização correta de caracteres específicos de uma determinada língua no Instalador passo-a-passo e no aplicativo do SafeSign IC, o formato e visualização do idioma pode divergir nas várias plataformas utilizadas e pode depender do pacote de idiomas e versão do sistema operacional utilizados.

De realçar que para determinadas aplicações, como o Microsoft VPN, o SafeSign IC não influencia o idioma das caixas de diálogo, pelo que mesmas surgirão na língua do sistema operacional instalado.

2 Menu IDs Digitais

O aplicativo SafeSign IC permite aos usuários identificar as IDs Digitais existentes no token. O termo ID Digital refere-se a um par de chaves (chave privada e chave pública) e um certificado, que podem ser usados para operações como assinatura digital e cifra.

O menu **IDs Digitais** abre uma caixa de diálogo que mostra as IDs Digitais que estão armazenadas no token e que foram registadas na certificate store local. A janela de *IDs Digitais* mostra também os certificados registados na Microsoft Personal Certificate Store que não estão no token.

Nota

Pode demorar algum tempo até que as IDs Digitais fiquem registadas e sejam visíveis na caixa de diálogo de *IDs Digitais*, dependendo da quantidade de objetos no token e da velocidade da leitora de tokens utilizado.

Quando não existem IDs Digitais, a caixa de diálogo de IDs Digitais estará vazia e terá a seguinte aparência:

Figura 22: IDs Digitais: Sem IDs Digitais Pessoais

Quando uma ID Digital tiver sido gerada ou importada para o token, a caixa de diálogo de IDs Digitais ficará com a seguinte aparência (se a ID Digital estiver selecionada, como abaixo):

Figura 23: IDs Digitais: ID Digital armazenada no token

Esta janela identifica as IDs Digitais pessoais e os detalhes da ID Digital, i.e. os conteúdos do certificado.

Quando uma ID Digital (mostrada a partir de **IDs Digitais Pessoais**) está no token, é identificada pelo seguinte símbolo:

Quando uma ID Digital ou um Certificado de AC não estão no token (mas está na *Microsoft Certificate Store*) ou quando o token foi removido, isso será identificado pelo símbolo seguinte:

Registo de Certificados

Em versões anteriores do SafeSign Identity Client (≤ 3.0.45), os certificados eram registados pelo SafeSign Identity Client Store Provider. Quando o token era removido, o registo dos certificados era cancelado. Por isso, quando o token era removido, a caixa de diálogo Mostrar IDs Digitais Registadas mostraria apenas as IDs Digitais disponíveis na Microsoft Personal Certificate Store.

A partir da versão 3.0.45 do SafeSign identity Client, os certificados são registados pelo Microsoft Certificate Propagation Service, que não cancela o registo dos certificados. Consequentemente, o ícone do computador na caixa de diálogo IDs Digitais pode referir-se tanto a um certificado num token que foi removido como a um certificado no disco rígido local, tendo sido ambos registados na Microsoft personal Certificate Store. Contudo, quando o token foi removido, não poderá executar operações como Eliminar IDs Digitais.

A caixa de diálogo *IDs Digitais* também indica se um certificado está prestes a expirar ou se já expirou. Neste caso, o texto dos certificados será apresentado a vermelho.

Ao visualizar um certificado prestes a expirar, a caixa de diálogo *Certificado* fica com a seguinte aparência:

Figura 24: Ver detalhes de ID Digital: O Certificado expirou ou vai expirar nos próximos 30 dias

Figura 25: Ver detalhes de ID Digital: O Certificado expirou.

Para mais informações acerca da expiração de certificados, consultar a Secção 2.4.

A caixa de diálogo **IDs Digitais** também permite ao usuário executar uma série de operações relacionadas com as IDs Digitais armazenadas no token (através dos botões no canto inferior direito da caixa de diálogo):

Seção 2.1 : Transferir ID Digital
Seção 2.2 : Eliminar ID Digital
Seção 2.3 : Ver detalhes de ID Digital
Seção 2.4 : Verificar Validade
Seção 2.5 : Exportar ID Digital

2.1 Transferir ID Digital

Nota

Esta funcionalidade apenas é exibida no sistema operativo Windows.

É possível transferir (mover) uma ID Digital para um token, por exemplo quando se tem um certificado pessoal (com uma chave privada correspondente a este certificado) na Microsoft Certificate Store. Isto melhora significativamente a segurança da sua ID Digital, agora protegida por autenticação por dois fatores: para aceder à ID Digital, precisará de ter em sua posse o token e saber o PIN do token.

Note que ao transferir a ID Digital para o token, a chave privada será movida para o token e deixará de estar armazenada no seu disco rígido.

Note que pode apenas transferir a sua ID Digital quando a chave privada está marcada como exportável, o que pode depender da forma como obteve o certificado[3].

Quando uma ID Digital (em **IDs Digitais Pessoais**) não está no token (mas sim na Microsoft Certificate Store), será identificada com o símbolo:
Selecione a ID Digital que pretende transferir para o token:

[3] No Windows Server 2003, não é possível marcar a chave privada como exportável para o template Utilizador de Smart Card, quando o propósito do certificado for ”assinatura e autenticação por smartcard”.

Figura 26: IDs Digitais: Transferir ID para o token

Clique **Transferir ID Digital** para mover a ID Digital da sua localização inicial para o token[4]
Ser-lhe-á pedido que confirme se pretende transferir a ID Digital com os dados especificados:

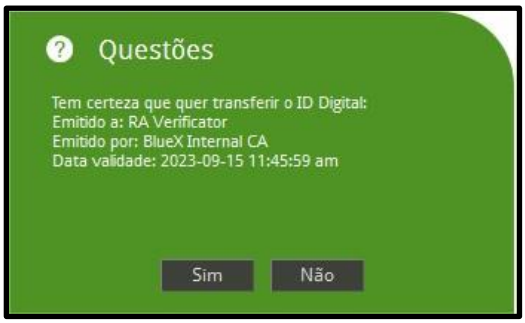

Figura 27: Transferir ID para o token: Pergunta

- Clique **Sim** para transferir a ID Digital especificada para o token
- Se clicar **Não**, o processo de transferência da ID Digital será interrompida e a ID Digital não será transferida.

Ser-lhe-á questionado se os certificados de AC pertencentes à ID Digital (“trust chain”) deverão ser importados também:

[4] O botão Transferir ID Digital só ficará disponível quando a ID ainda não está no token, mas está (registada) na Microsoft Personal Certificate Store (e tem uma chave privada associada armazenada no disco rígido local).

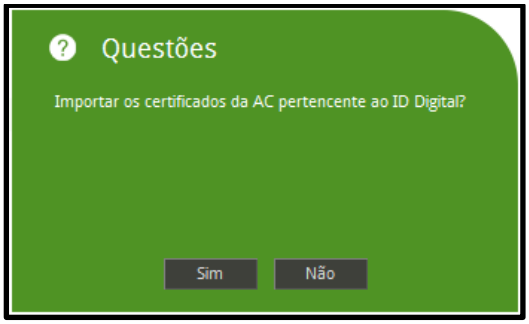

Figura 28: Transferir ID para o token: Pergunta certificados CA

- Clique **Sim** se pretender importar os certificados de AC pertencentes à ID Digital
- Se clicar **Não**, os certificados de AC pertencentes à ID Digital não serão importados para o token (mas o processo de transferir a ID Digital prosseguirá).

Será pedido o PIN do token:

Figura 29: Transferir ID para o token: Inserir PIN

Insira o PIN correto do token e clique **Confirmar**

A ID Digital será transferida:

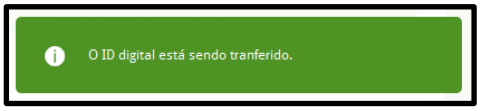

Figura 30: Transferir ID para o token: Transferindo

Quando uma ID Digital é transferida com sucesso para o Token, surge a seguinte notificação:

Figura 31: Transferir ID para o token: Sucesso

A ID Digital está agora no token:

Figura 32: IDs Digitais: IDs Digitais Pessoais no token

Se tiver clicado **Sim** na caixa de diálogo para importar para o token certificados de AC pertencentes à ID Digital (Figura 32), os certificados de AC das IDs Digitais também estarão no token (como indicado na imagem acima).

Chave privada não exportável

Quando a chave privada pertencente à ID Digital não é exportável, a transferência falha e surge a seguinte mensagem de erro:

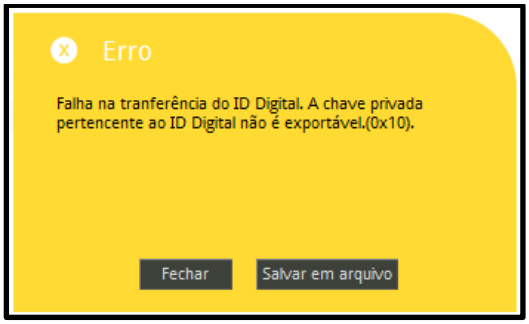

Figura 33: Transferir ID para o token: Erro

- Clique **Fechar** para fechar esta caixa de diálogo
- Clique **Salvar para Ficheiro** para salvar a mensagem de erro para um ficheiro.

Caminho do Certificado

Quando o certificado da AC não está disponível (quer no token quer na Microsoft Certificate Store), a caixa de diálogo de informação do certificado fica com a seguinte aparência:

Figura 34: IDs Digitais: Sem Cadeia de Certificados

2.2 Eliminar ID Digital

É possível eliminar uma ID digital armazenada no token através do botão **Eliminar ID Digital** (Figura 23). Note que com o Aplicativo SafeSign IC, pode eliminar apenas IDs Digitais Pessoais no token. Não poderá eliminar IDs Digitais mostradas na caixa de diálogo *IDs Digitais* que estão na Certificate Store, como indicado pelo símbolo (nesse caso, o botão **Eliminar ID Digital** ficará esbatido).

Nota

Ao eliminar uma ID Digital, todos os seus objetos (chave pública, chave privada e certificado) serão eliminados do token.

Se um par de chaves tiver mais que um certificado (como no caso de renovação de certificado, em que o mesmo par de chaves é usado para gerar um certificado), a caixa de diálogo IDs Digitais mostrará duas IDs Digitais. Eliminar uma delas não elimina o par de chaves partilhado, e eliminará apenas o certificado, de forma a que o outro certificado (e a respetiva certificate chain) possa continuar a ser usado.

Ao clicar no botão **Eliminar ID Digital**, é pedido que confirme se pretende mesmo eliminar a ID Digital com os dados especificados:

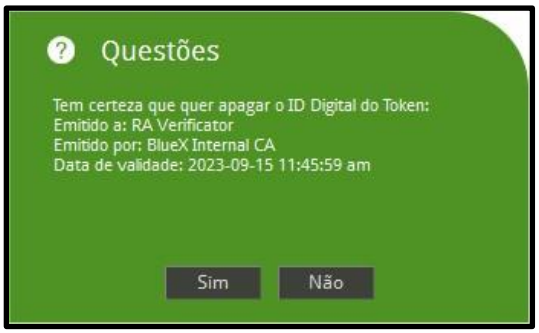

Figura 35: IDs Digitais: Tem a certeza que deseja eliminar o ID Digital

- Clique **Sim** para eliminar a ID Digital, e ser-lhe-á pedido de seguida que insira o PIN do seu token
- Se clicar **Não**, o processo de eliminação da ID Digital será cancelado e a ID Digital não será eliminada

Ao clicar **Sim** (Figura 35), ser-lhe-á pedido que insira o PIN do seu token:

Figura 36: Eliminar ID Digital: Insira PIN

Insira o PIN correto e clique **Confirmar**

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido5. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Ao inserir o PIN correto, a ID Digital será eliminada:

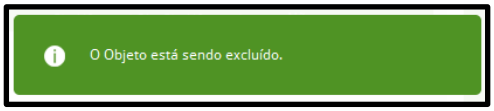

Figura 37: Eliminar ID Digital: A Eliminar

Quando a ID Digital tiver sido eliminada com sucesso, surgirá a seguinte janela informativa:

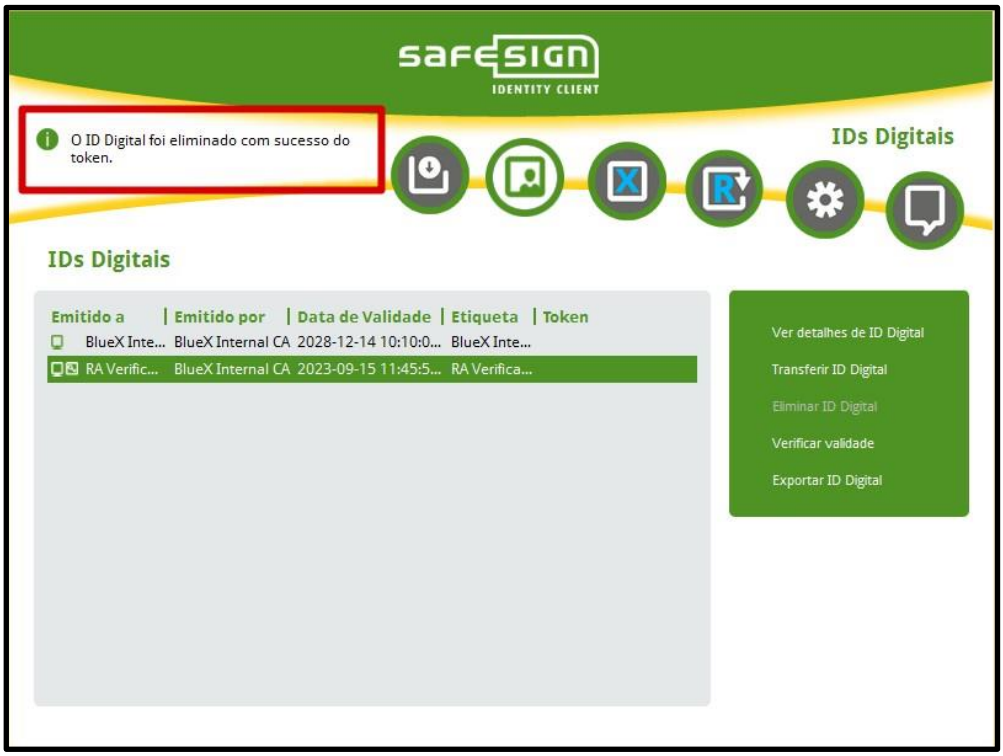

Figura 38: Eliminar ID Digital: Sucesso

A ID Digital e a respetiva cadeia de certificação foram removidas do token.

[5] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

2.3 Visualizar Certificado

O botão **Ver Certificado** permite visualizar os conteúdos de IDs Digitais Pessoais, bem como dos certificados CA, quando selecionados.

Note que pode também visualizar o conteúdo do certificado ao fazer duplo clique sobre qualquer uma das IDs Digitais listadas em **IDs Digitais Pessoais** ou sobre qualquer certificado listado em **Certificate chain**.

Ao clicar em **Ver Certificados** quando uma ID Digital Pessoal estiver realçada, surge a seguinte caixa de diálogo:

Figura 39: Ver Certificado: Informação do Certificado

Esta caixa de diálogo mostrará a informação disponível acerca do certificado.
Também fornecerá informação adicional quando aplicável, como informação de quando o certificado expirará (Figura 24), de quando o certificado já expirou (Figura 25), de quando a cadeia de certificados completa não foi encontrada ou uma combinação destas informações.
Clique **Fechar** para fechar a caixa de diálogo.
Clique **Salvar para Arquivo** para salvar o certificado no computador

Salvar para Arquivo

Pode salvar a informação do certificado para um ficheiro, clicando **Salvar para arquivo**.

Ao clicar **Salvar para arquivo**, é-lhe permitido salvar o ficheiro como tipo de ficheiro de certificado (*.cer):

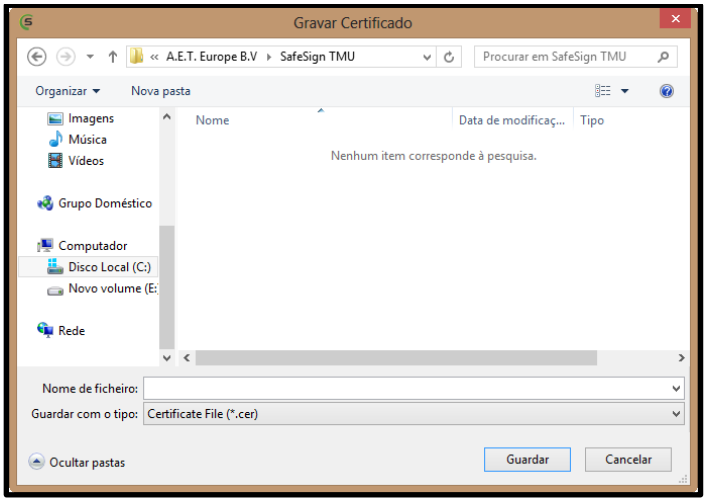

Figura 40: Ver Certificado: Guardar Certificado

Selecione um nome e uma localização para salvar o ficheiro, e em seguida clique **Salvar**

2.4 Verificar Validade

Pode verificar o estado relativamente ao prazo em que as IDs Digitais no token expiram, clicando no botão **Verificar Validade**.

Figura 41: Menu Verificar Validade

Quando nenhum certificado estiver prestes a expirar / tenha expirado, surge a seguinte caixa de diálogo:

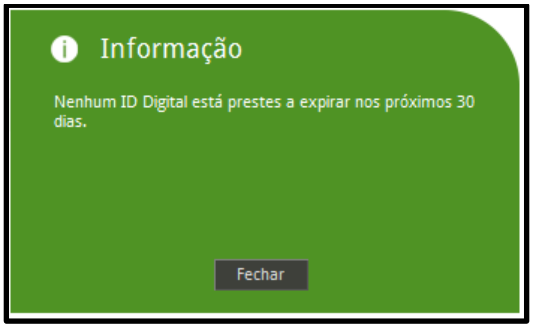

Figura 42: Verificar Validade

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

Quando houver certificados prestes a expirar / expirados, a caixa de diálogo de *Aviso de Expiração de Certificado* surgirá:

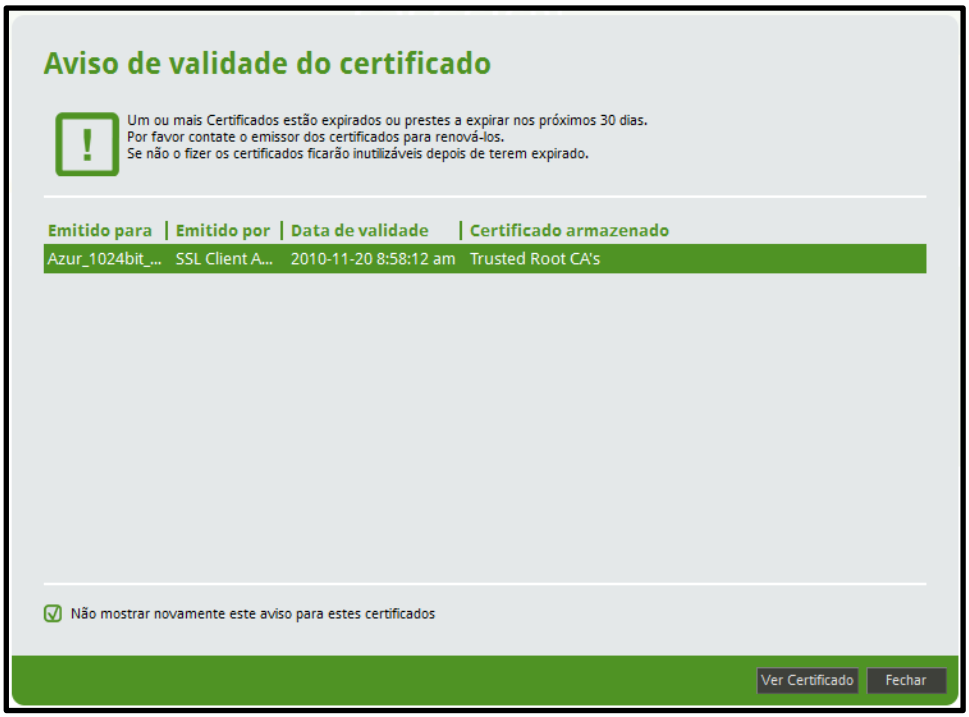

Figura 43: Verificar Validade: Alerta de Validade do Certificado

Esta caixa de diálogo mostrará os certificados que expiram nos próximos [x] dias (30 dias no exemplo) bem como os certificados que já expiraram[6].

Por defeito, o prazo para despoletar o aviso está definido em trinta (30) dias.

[6] Tal como a Microsoft mantém certificados expirados na Certificate Store.

Aviso de Expiração do Certificado

A caixa de diálogo de Aviso de Expiração de Certificado surge por defeito sempre que o token é inserido e tenha certificados que expirem no período de tempo especificado. Nesse caso, surge a seguinte caixa de diálogo:

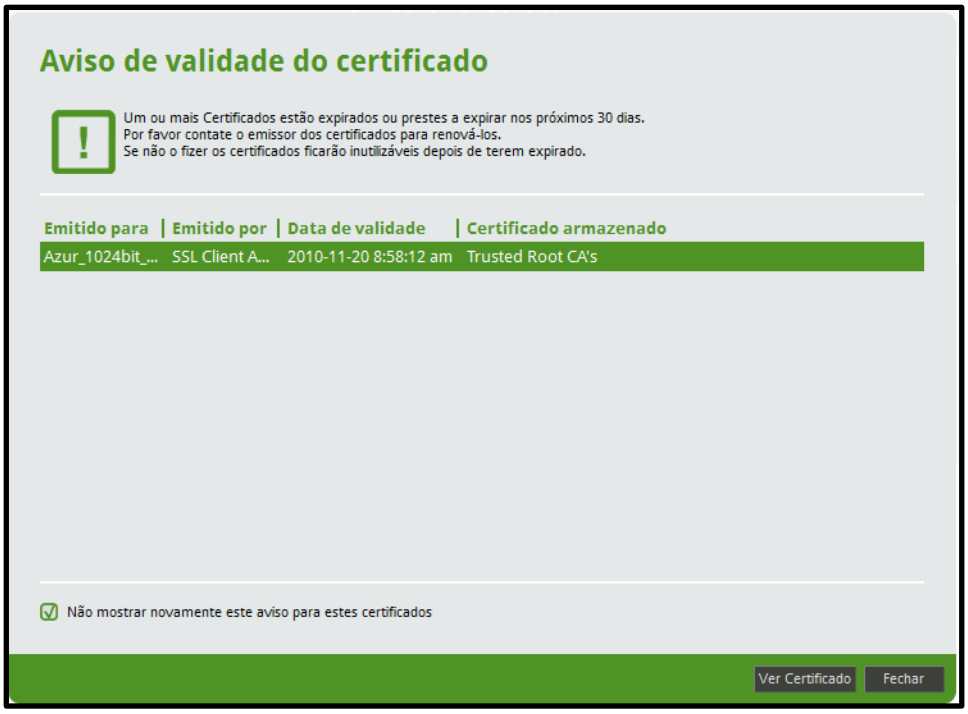

Figura 44: Alerta de Validade do Certificado

Nota

Note que se selecionar "Não voltar a mostrar este aviso para estes certificados", este aviso não será mostrado novamente para os certificados listados e não poderá ser reativado para esses certificados.

Se selecionar os certificados que estão prestes a expirar, pode visualizar os conteúdos do certificado tal como registado na Certificate Store, ao fazer duplo clique sobre o mesmo ou clicando em Ver Certificado.

Clicar no botão **Fechar** fechará a caixa de diálogo de Validade do Certificado.

2.5 Exportar ID Digital

Nota

Esta funcionalidade apenas é exibida no sistema operativo Windows.

Exportar um ID Digital, fornece a possibilidade do usuário salvar um ID Digital no formato de arquivo .p12.

A opção apenas fica visível se o usuário selecionar uma ID Digital que:

- Esteja instalada na Microsoft Certificate Store
- Tenha uma chave privada associada ao ID Digital

Quando uma ID Digital (em **IDs Digitais Pessoais**) não está no token (mas sim na Microsoft Certificate Store) e com uma chave privada associada, será identificada com o símbolo: .
Selecione a ID Digital que pretende exportar para arquivo e **clique** em Exportar ID Digital no menu do lado direito.

Figura 45: Menu : Exportar ID Digital

Ao clicar em **Exportar ID Digital**, uma caixa de diálogo será apresentada para que a localização do arquivo seja escolhida, como também a senha com qual o arquivo irá ficar. A senha pode conter caracteres alfanuméricos.

Figura 46: Selecionar pasta destino e senha do arquivo .p12

- Clique **Confirmar** para transportar a ID Digital especificada para o arquivo
- Se clicar **Cancelar**, o processo de exportação da ID Digital será interrompido e a ID Digital não será exportada.

Ao clicar em **Confirmar**, será iniciado o processo de exportação:

Figura 47: Exportação da ID Digital para arquivo

Se o processo acabou com sucesso, uma mensagem de sucesso é apresentada, no entanto se algo não correr como previsto (p.e. não ter permissões na localização escolhida previamente), uma mensagem de erro é apresentada ao usuário.

Figura 48: ID Digital exportada com sucesso

Figura 49: Erro ao exportar uma ID Digital

3 Menu Token

O menu **Token** do Utilitário inclui as seguintes funcionalidades:

Seção 3.2 : Inicializar Token

Seção 3.3 : Limpar Token

3.1 Seção 3.4 : Reciclar Token

No aplicativo é possível fazer a reciclagem do token. A funcionalidade apenas ficará disponível se o token suportar a reciclagem e esgotar as tentativas do PIN e PUK da mídia.
Para simular uma reciclagem é necessário colocar o token no estado de bloqueado, ou seja, a introdução de 3 vezes consecutivas o PIN e o PUK errado.

Figura 72: Menu Reciclar Token ativo

Ao pressionar o menu “**Reciclar Token**” é apresentada uma questão para o usuário confirmar a reciclagem.

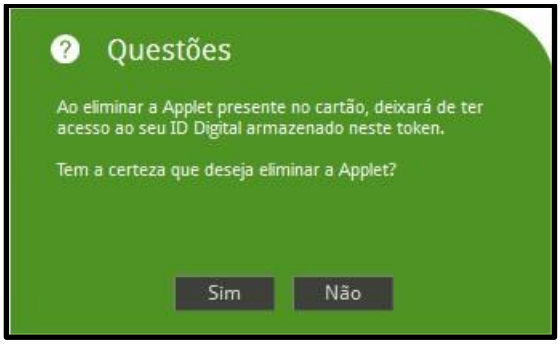

Figura 73: Confirmação da eliminação da applet

Ao clicar em **SIM**, receberá a informação de que o seu Token está sendo reciclado:

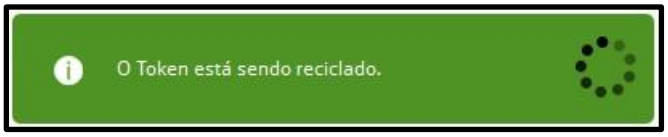

Figura 74: O seu token está sendo reciclado

Apenas alguns tokens suportam a reciclagem

O SafeSign Identity Client permite a reciclagem do token apenas se este o suportar. Para identificar se o seu token ou quais os tokens disponíveis com esta opção, contate com o seu fornecedor de mídia.

Depois da reciclagem do token é exibida uma tela para inicializar o mesmo. Para ver em mais detalhe o processo de inicialização do token ler capitulo 3.2.

Alterar PIN

Seção 3.6 : Alterar PIN de Transporte

Seção 3.7 : Desbloquear PIN

Seção 3.8 : Alterar PUK

Seção 3.9 : Mostrar Informação de Token

Seção 3.10 : Mostrar Objetos do Token

Seção 3.11 : Mostrar Certificados de Atributo do Token

Seção 3.12 : Exportar Conteúdo do Token

Seção 3.13 : Consultar Token desconhecido

Seção 3.14 : Alterar Timeout do PIN

3.2 Inicializar Token

O primeiro passo após instalar o SafeSign Identity Client é inicializar o seu token (se ainda não tiver sido inicializado).

Os valores escritos no token durante a inicialização não podem ser alterados durante o tempo de vida do token. Isto significa que durante o seu tempo de vida, o token guarda as definições criadas durante a inicialização.

Note contudo, a diferença entre tokens de teste (completo) e tokens de produção (completo):

- Para tokens de teste, é possível alterar as definições do token durante a reinicialização do token (i.e. substituir a estrutura PKCS#15 existente com uma estrutura PKCS#15 nova ou atualizada).
- Para tokens de produção, não é possível alterar as definições uma vez que estas tenham sido configuradas durante a inicialização. Poderá apenas apagar os seus conteúdos, mantendo no entanto a estrutura PKCS#15 escrita no token durante a inicialização.

Pode visualizar a definições do Token em Token > Mostrar Informação de Token (Seção 3.9).

Nota

Tokens de Teste (completos) são normalmente usados apenas para teste e avaliação. Normalmente os tokens fornecidos aos usuários são tokens de produção (completos), que podem já ter a applet SafeSign Identity Client instalada (no caso de Java cards) e podem até já estar inicializados. Do mesmo modo, é recomendado que, para Java cards, o jogo de chaves GlobalPlatform predefinido seja alterado para um jogo de chaves específico personalizado pelo usuário, de forma a que a(s) applet(s) não possam ser removidas (sem o conhecimento deste jogo de chaves).

Nota

Como o correto funcionamento do SafeSign Identity Client depende de um token smart card ou USB produzido apropriadamente, a AET reforça que os tokens smart cards / USB produzidos para utilização no SafeSign Identity Client por fornecedores que não sejam aprovados pela AET e que não cumpram as nossas políticas de Qualidade (que exigem que a applet seja pré-instalada num ambiente seguro e um jogo de chaves personalizado) não são elegíveis para qualquer suporte pela AET em caso de problemas, mesmo que o usuário tenha celebrado um Acordo de Manutenção e Suporte SafeSign Identity Client.

Ao inicializar um token, o SafeSign Identity Client deteta o modelo do token inserido e determina o perfil mais adequado para inicializar o token. Antes de inicializar um token, por favor tenha em atenção que os perfis disponíveis dependem do tipo de token utilizado.

Se determinado perfil não estiver disponível, isso significa que esse perfil provavelmente não estará disponível para esse token (porque ele não possui espaço suficiente para as definições de espaço público e privado desse perfil).

Se não estiver disponível nenhum perfil (a linha de perfil de token fica esbatida), isto significa que provavelmente não tem permissões suficientes para definir um perfil. Dependendo das permissões do usuário, poderá conseguir selecionar apenas o perfil definido pelo administrador. Note que é recomendado que os usuários finais selecionem o perfil predefinido, a não ser que o administrador dê instruções em contrário.

As secções seguintes descrevem diferentes cenários:

Seção 3.2.1 : Como inicializar um token ainda não inicializado (tanto de teste como de produção).

Seção 3.2.2 : Como reinicializar um token inicializado (apenas token de teste).

Seção 3.2.3 : Como importar um certificado de AC durante a inicialização / limpeza do Token.

Seção 3.2.4 : Como ver o contador de Reciclagem da applet.

3.2.1 Inicializar um Token

Quando ainda não tiver inicializado o seu token (quer seja um token de teste ou de produção) o token será identificado no Aplicativo SafeSign IC, como um "*Token em branco – não inicializado*" e apenas estarão disponíveis as opções *Inicializar Token* e *Mostrar informação de Token*:

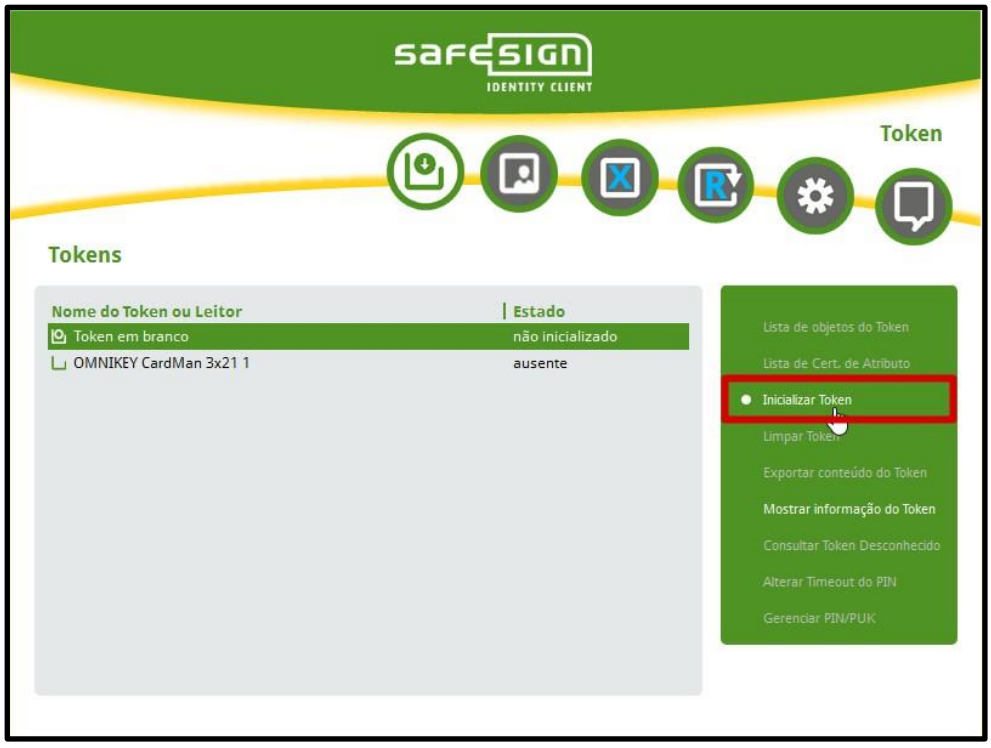

Figura 50: Utilitário de Token: Inicializar Token

Para inicializar o Token, clique **Token** > **Inicializar Token** (como demonstra a figura acima)

Nota

Quando o seu token de teste já tiver sido inicializado com uma etiqueta de Token, PUK e PIN, poderá reinicializar o token. Consulte a seção 3.1.2.

Quando o seu token de produção já tiver sido inicializado com uma etiqueta de Token, PUK e PIN, poderá apagar o token. Consulte a seção 3.2.

A caixa de diálogo *Inicializar Token* é despoletada, permitindo que inicialize o seu token:

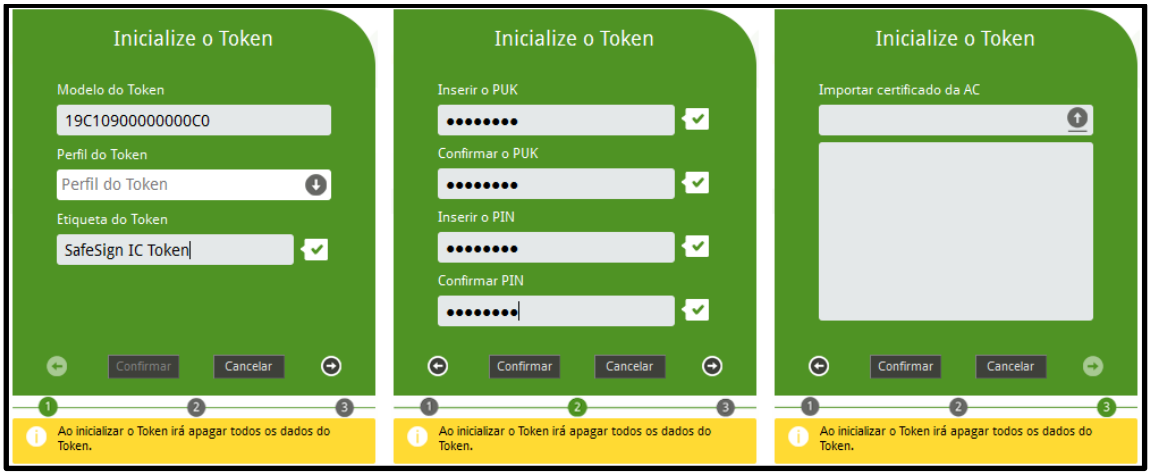

Figura 51: Utilitário de Token: Inicializar Token

A caixa *Modelo do token* identifica o tipo de token inserido e prestes a ser inicializado.

A lista de Perfis de To*ken* permitirá selecionar qual o perfil a utilizar para inicializar o token. Note que esta lista pode estar esbatida, se o usuário não tiver permissões para fazer este tipo de alterações.

Applet SafeSign instalada em produção

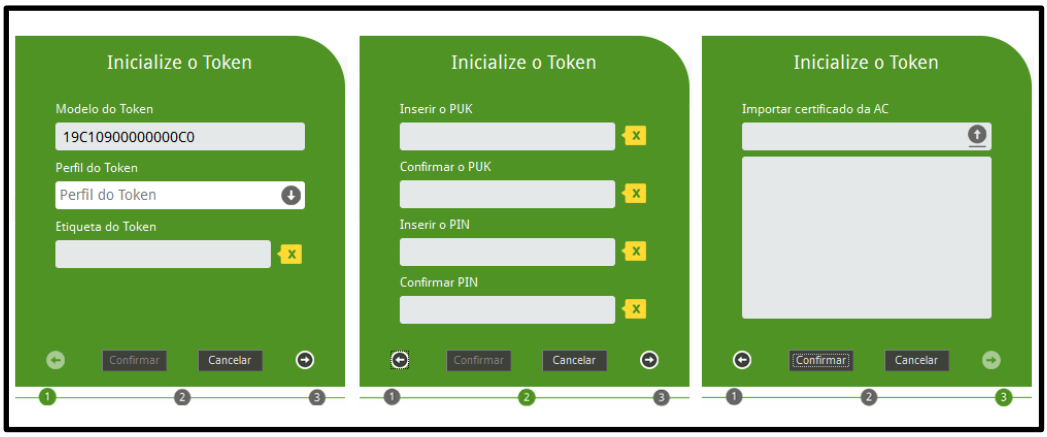

Figura 52: Utilitário de Token: Caixa de diálogo Inicializar Token para cartões de produção

Para inicializar o seu token, precisa garantir determinados requisitos. Quando cumprir um determinado requisito, o sinal **incorreto** passa a **correto**.

Preencha os campos pedidos como demonstrado de seguida, tendo em conta as chamadas de atenção e os requisitos abaixo:

Campo	Requisitos
Perfil do Token	Podem estar disponíveis diferentes perfis de token, dependendo do tipo de token que tenha inserido. Selecione o perfil que melhor se adequa às suas necessidades. Para os cartões Java Card v2.2+, só está disponível um perfil, denominado “Perfil padrão”.
Etiqueta do Token	A etiqueta do token tem que conter alguns caracteres obrigatoriamente, não pode estar em branco; O número máximo de caracteres é 32
Inserir PUK	O tamanho mínimo do PUK é de 4 caracteres, e o comprimento máximo do PUK é de 8 – 15 caracteres
Confirmar PUK	O PUK a confirmar deverá ser igual ao novo PUK definido.
Inserir PIN	O tamanho mínimo do PIN é de 4 caracteres, e o comprimento máximo do PIN é de 8 – 15 caracteres
Confirmar PIN	O PIN a confirmar deverá ser igual ao novo PIN definido.

Tabela 1: Utilitário de Token: Campos Inicializar Token

Requisitos do Campo

Tanto o rótulo do token como os códigos PIN e PUK podem ser constituídos na íntegra ou parcialmente por carateres alfanuméricos, i.e. letras (tanto letras minúsculas com maiúsculas), números, carateres especiais / símbolos (tais como @, # e &) e espaços em branco.

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um comprimento inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido. Apenas quando inserir um PIN / PUK com o comprimento exigido é que este será aceite. Note que ambos os comprimentos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Quando todos os campos estiverem preenchidos de acordo com os requisitos, conforme demonstrado na imagem seguinte:

Figura 53: Utilitário de Token: caixa de diálogo de Inicializar Token

Clique em **OK** para começar a inicializar o seu Token SafeSign Identity Client.
Ao clicar em **OK**, receberá a informação de que o seu Token está a ser inicializado:

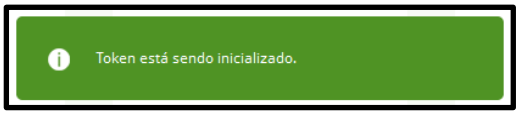

Figura 54: Inicializar Token: O seu token está a ser inicializado

Não interrompa nem remova o seu token SafeSign Identity Client token durante o processo de limpeza. Se tiver uma leitora smart card com um LED, deverá ficar atento ao LED da sua leitora smart card para ver se esta está ocupada ou não.

Quando a inicialização é finalizada, surgirá a seguinte notificação:

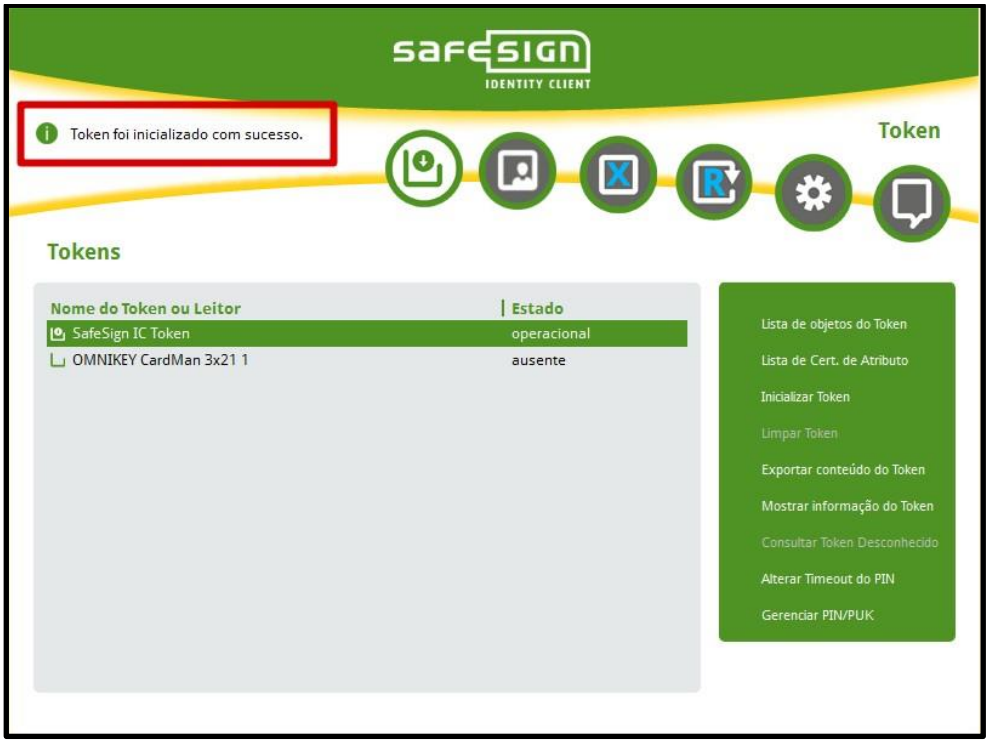

Figura 55: Inicializar Token: A operação foi concluída com sucesso

Quando o token é inicializado, o nome do token aparecerá na janela de token:

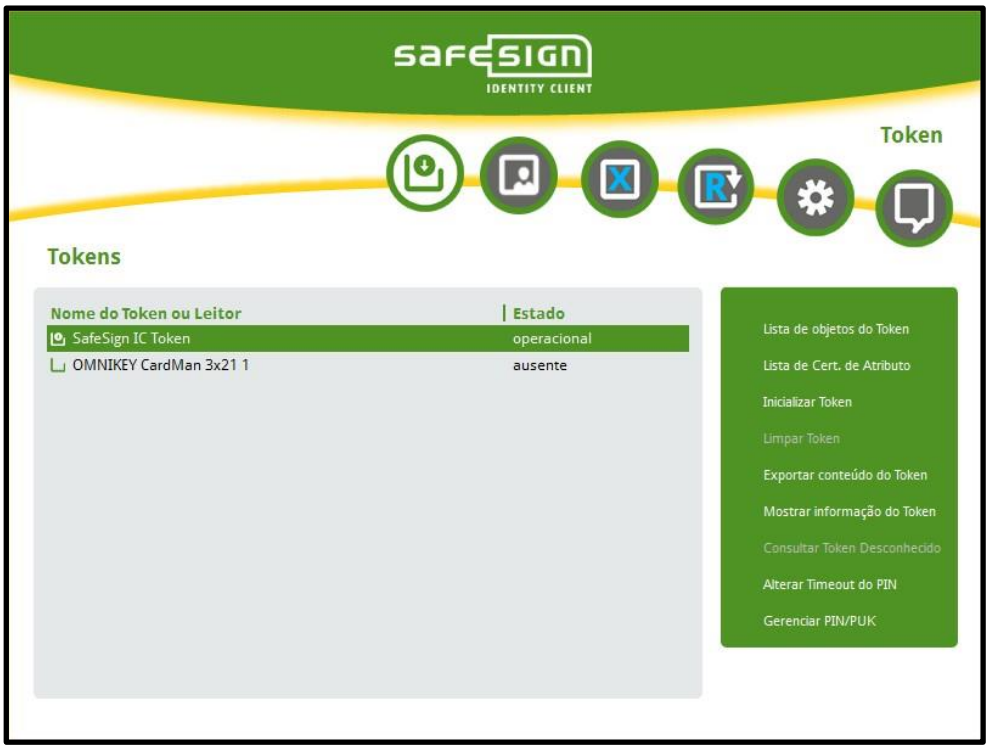

Figura 56: Utilitário de Token: Token operacional

Assim que o seu token estiver inicializado, todas as operações do menu **IDs Digitais** e **Token** ficarão disponíveis.

Erro do Dispositivo

Quando a operação de Inicialização do Token falhar, surge o seguinte caixa alerta:

Figura 57: Erro: Erro do Dispositivo 0x48

Verifique se a sua leitora smart card está a funcionar corretamente e se tem o token correto. Assegure-se de que o token está inserido na leitora de smart card e clique em **OK** para voltar a tentar inicializar o token. Este erro pode também ocorrer quando não existe espaço livre no cartão (para as definições selecionadas).

Clique **Fechar** para fechar esta caixa de diálogo.

3.2.2 Reinicialização do token

Quando o seu token já foi inicializado, pode ser novamente inicializado, se o token for de teste.

Note que que quando reinicializar o seu token, todos os dados que possam estar armazenados no seu token serão eliminados. Um aviso refente a isto será incluído na caixa de diálogo *Inicializar Token*:

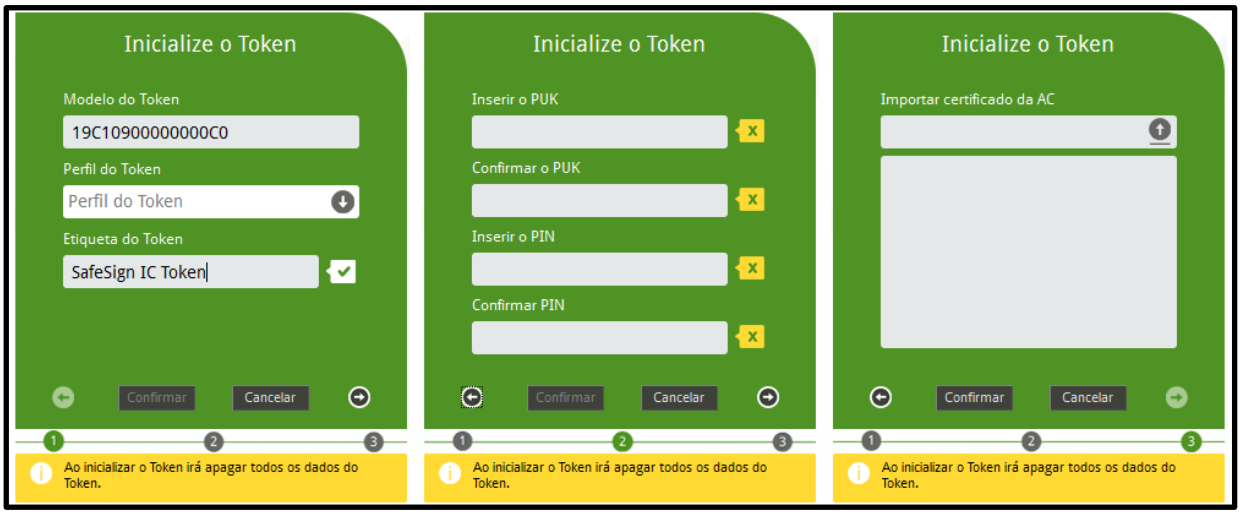

Figura 58: Utilitário de Token: Alerta Inicializar Token

3.2.3 Importar Certificados AC

O aplicativo Safesign IC permite-lhe importar certificados de *Autoridade de Certificação* (AC).
Pode fazê-lo de duas maneiras:

1. A partir do item *Importar Certificado* do menu Token → Listar Objetos do Token, permitindo-lhe selecionar um único certificado de AC para importação (“um de cada vez”), como descrito na seção 3.10.4.;
2. Durante a inicialização do token, selecionando um diretório onde estão armazenados um ou múltiplos certificados de AC (“todos de uma vez”), como descrito nesta seção.

Formato dos certificados de AC

O SafeSign IC suporta a importação de certificados de AC armazenados em arquivos:

- Com extensões .pem, .cer, .crt ou .der;
- Codificados em formato DER ou PEM.

Selecione a pasta onde estão os certificados de AC e altere a extensão de *.cer para *.crt ou *.der conforme necessário.

Na caixa de diálogo *Inicializar Token*, a opção **Importar certificados de AC** permite selecionar um diretório onde o(s) certificado(s) de AC está(ão) armazenado(s):

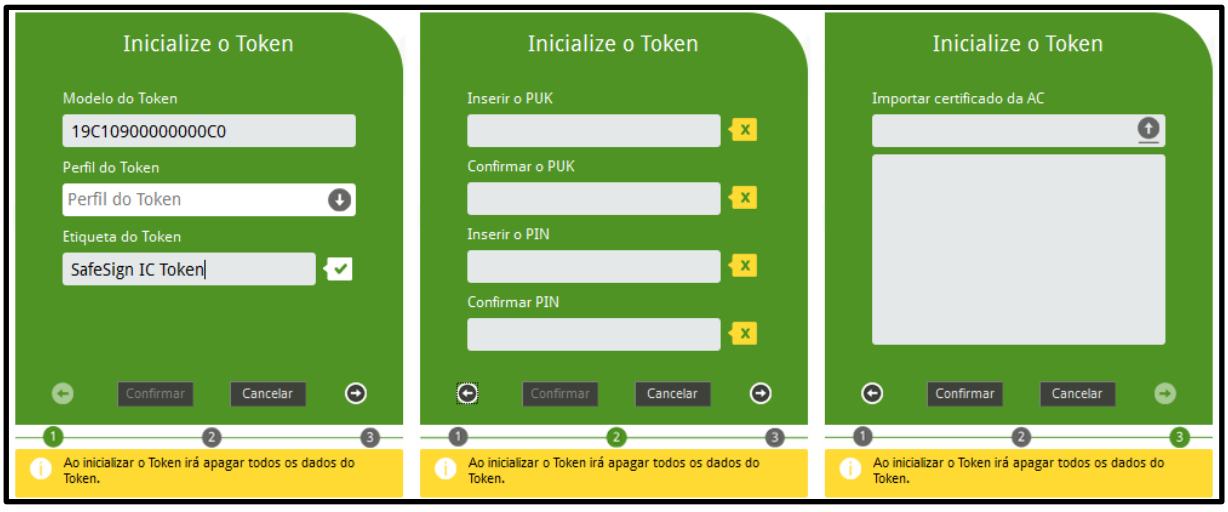

Figura 59: Utilitário de Token: caixa de diálogo *Inicializar Token*

Preencha todos os campos de acordo com os requisitos (como descrito na seção 3.2.1) e clique no ícone **navegar** para selecionar a uma diretoria onde os certificados AC onde estão localizados.
Ao clicar no ícone navegar, aparecerá a caixa de diálogo *Procurar uma pasta*, que permitirá selecionar uma diretoria contendo Certificados CA:

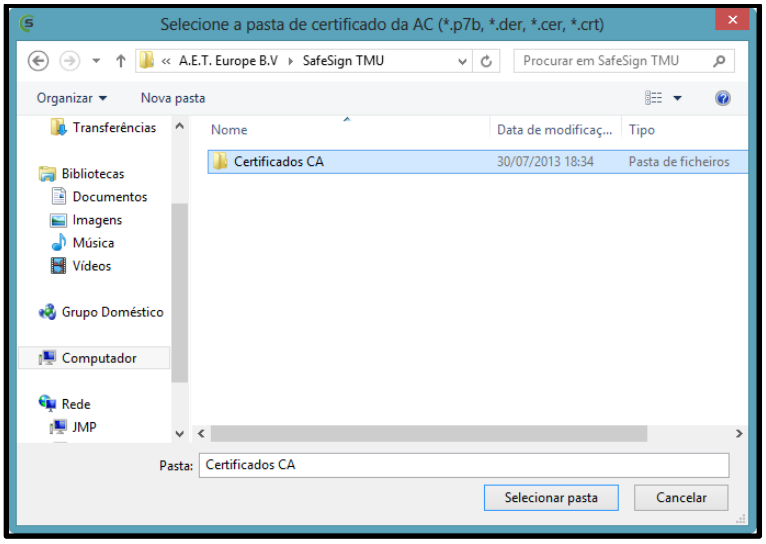

Figura 60: Procurar Pasta

Selecione a diretoria e clique em OK

Ao clicar **OK**, a diretoria será indicada na caixa correspondente:

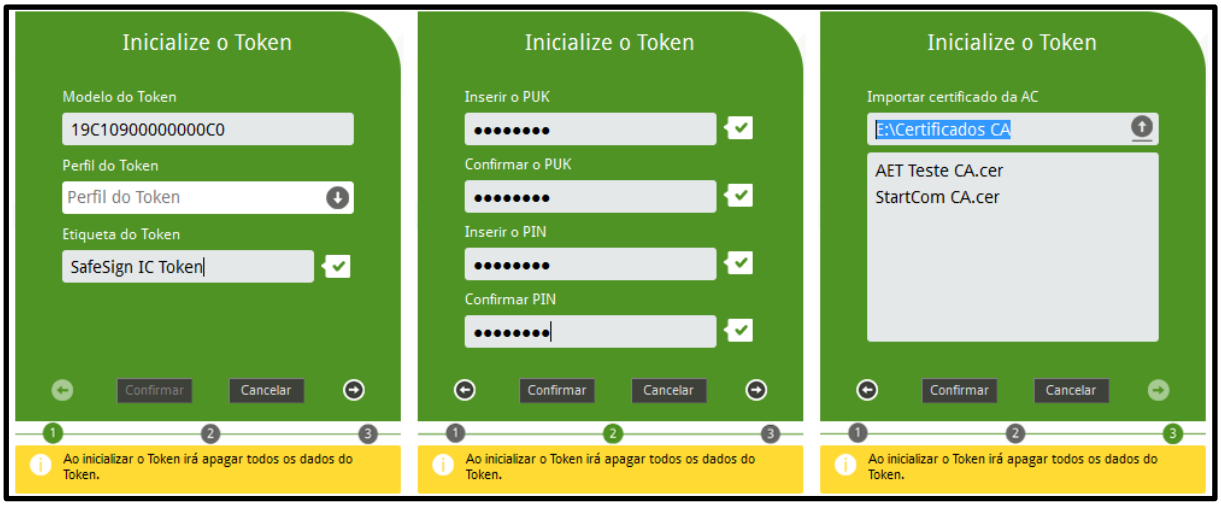

Figura 61: Inicializar Token: Importar Certificados CA

Note que **todos** os certificados de AC presentes na diretoria serão importados.

Clique OK para inicializar o token

Ao clicar em **OK**, o seu token será inicializado:

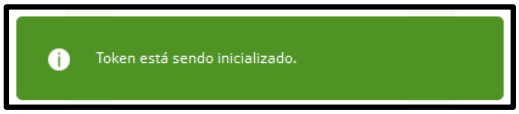

Figura 62: Utilitário de Token: o token está a ser inicializado

Não interrompa ou remova o seu token SafeSign Identity Client token durante o processo de inicialização. Se tiver uma leitora smart card com um LED, deverá ficar atento ao LED da sua leitora smart card para ver se esta está ocupada ou não.

Quando o(s) certificado(s) são importados como parte do processo de inicialização surgirá a seguinte caixa de diálogo:

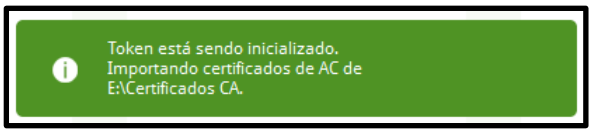

Figura 63: Utilitário de Token: A Importar certificados CA

Quando a inicialização é finalizada, surgirá a seguinte notificação:

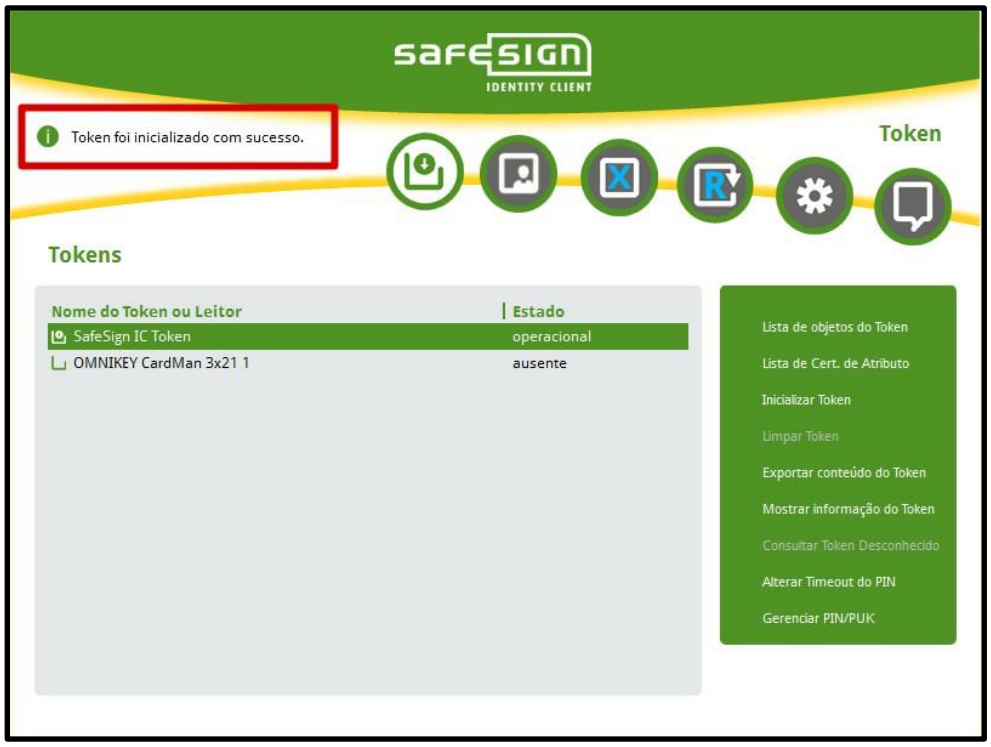

Figura 64: Utilitário de Token: Operação concluída com sucesso

Erro de Dispositivo

Quando a operação de inicialização do token falha, surge o seguinte aviso:

Figura 65: Erro: Erro do Dispositivo 0x30

Verifique se a sua leitora está a funcionar corretamente e se inseriu o cartão correto. Assegure-se de que o token está inserido na leitora de smart cards e clique Fechar para voltar a tentar inicializar o token. Este erro também pode ocorrer quando não há espaço suficiente no cartão (para o perfil selecionado).

Clique **Fechar** para fechar esta janela

Clique **Salvar para Ficheiro**, para salvar a mensagem de erro no computador

3.2.4 Versão da Applet e Reciclagem do Contador

Para que a funcionalidade de reciclagem possa ser ativada, é necessária uma applet especial, com parâmetros específicos de instalação (que não se enquadram no âmbito deste documento). Quando esta applet é instalada corretamente, a caixa de diálogo de *Informação do Token* mostra a versão da applet e o número de tentativas de reciclagem disponíveis:

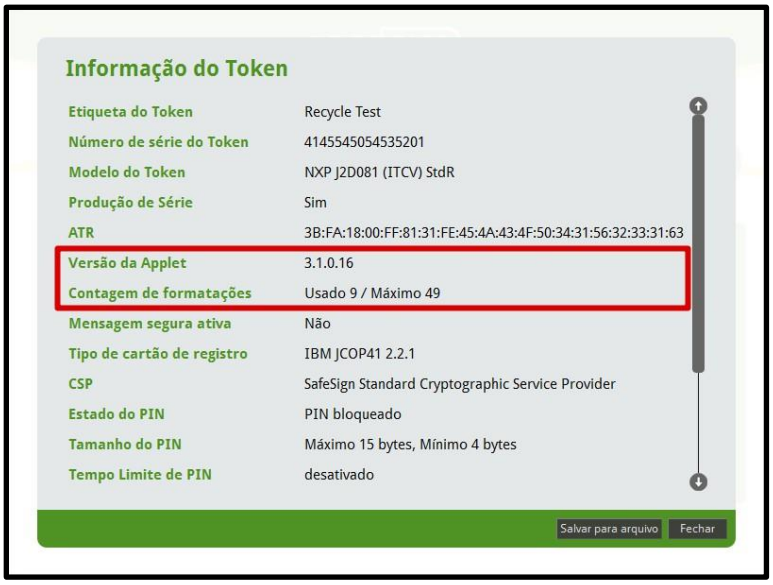

Figura 66: Informação do Token: Contador de Reciclagem

O número total de tentativas de reciclagem disponível no exemplo é 49.

3.3 Limpar Token

Quando um token de produção foi inicializado, só será possível limpar o token (e não reinicializá-lo).

Nesse caso, o menu Token mostra a opção Limpar Token (em vez de Inicializar Token, como na Figura 50). Ao clicar nessa opção, abrir-se-á a seguinte janela:

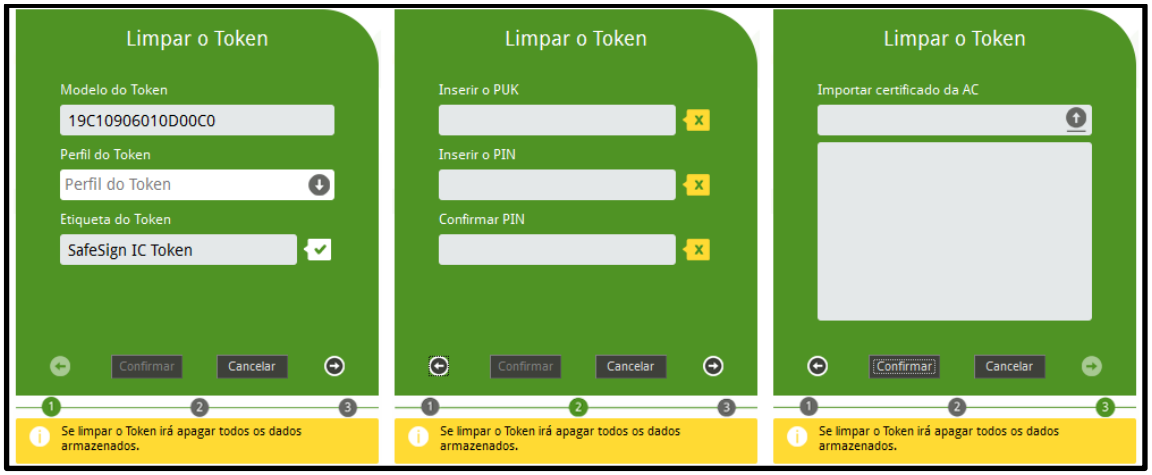

Figura 67: Utilitário de Token: Caixa de diálogo Limpar Token

Note que o rótulo do token no exemplo acima é o rótulo antigo do token inicializado. Note que a opção Perfil de Token pode não estar disponível para si.
Note que quando limpar o seu token, todos os dados que possam estar armazenados no seu Token serão eliminados. A caixa de diálogo da opção Limpar Token mostra um aviso neste sentido.

Para limpar o seu token, deve-se satisfazer um número de requisitos. Quando satisfizer determinado requisito, o sinal (**incorreto**) torna-se (**correto**)

Deve preencher os seguintes requisitos, tendo em conta as advertências e requisitos anteriores:

Campo	Requisitos
Rótulo do Token	O rótulo do token tem que conter alguns caracteres obrigatoriamente, não pode estar em branco; O número máximo de caracteres é 32
Inserir PUK	O tamanho mínimo do PUK é de 4 caracteres, e o comprimento máximo do PUK é de 8 – 15 caracteres. O PUK inserido deve ser o PUK atual / existente.
Inserir PIN	O tamanho mínimo do PIN é de 4 caracteres, e o comprimento máximo do PIN é de 8 – 15 caracteres
Confirmar PIN	O PIN a confirmar deverá ser igual ao novo PIN definido

Tabela 2: Utilitário de Token: Limpar campos do Token

Requisitos do Campo

Tanto o rótulo do token como os códigos PIN e PUK podem ser constituídos na íntegra ou parcialmente por carateres alfanuméricos, i.e. letras (tanto letras minúsculas com maiúsculas), números, carateres especiais / símbolos (tais como @, # e &) e espaços em branco.

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um comprimento inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão **OK** nas instâncias em que o PIN / PUK é pedido[7]. Apenas quando inserir um PIN / PUK com o comprimento exigido é que este será aceite. Note que ambos os comprimentos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Quando todos os campos estiverem preenchidos de acordo com os requisitos, conforme demonstrado na imagem seguinte:

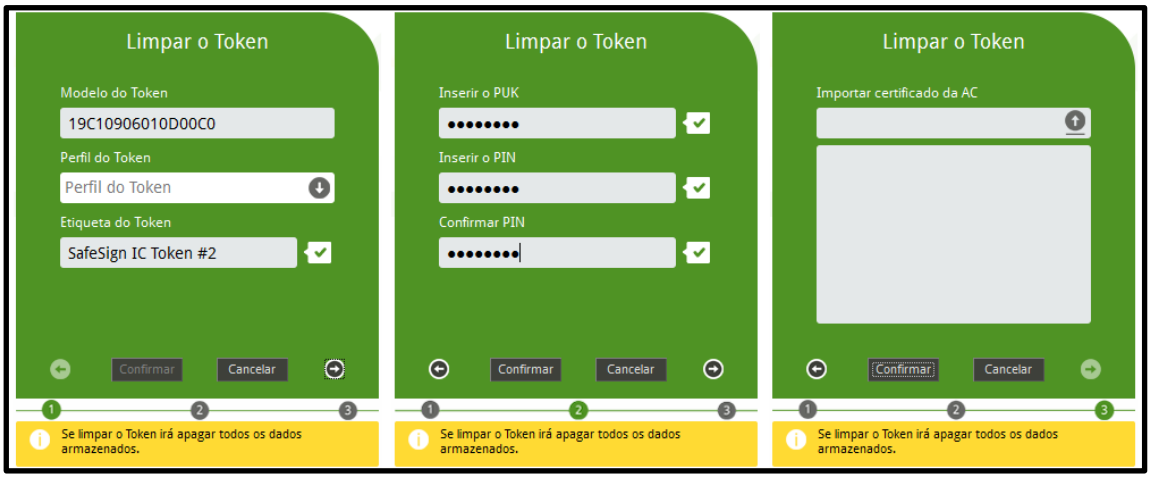

Figura 68: Utilitário de Token: Caixa de diálogo Limpeza do Token concluída

Clique em **OK** para começar a limpar o seu Token SafeSign Identity Client.
Ao clicar em **OK**, receberá a informação de que o seu Token está a ser limpo:

Figura 69: O seu token está a ser limpo

Não interrompa ou remova o seu token SafeSign Identity Client token durante o processo de limpeza. Se tiver uma leitora smart card com um LED, deverá ficar atento ao LED da sua leitora smart card para ver se esta está ocupada ou não.

Quando a inicialização é finalizada, surgirá a seguinte notificação:

[7] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

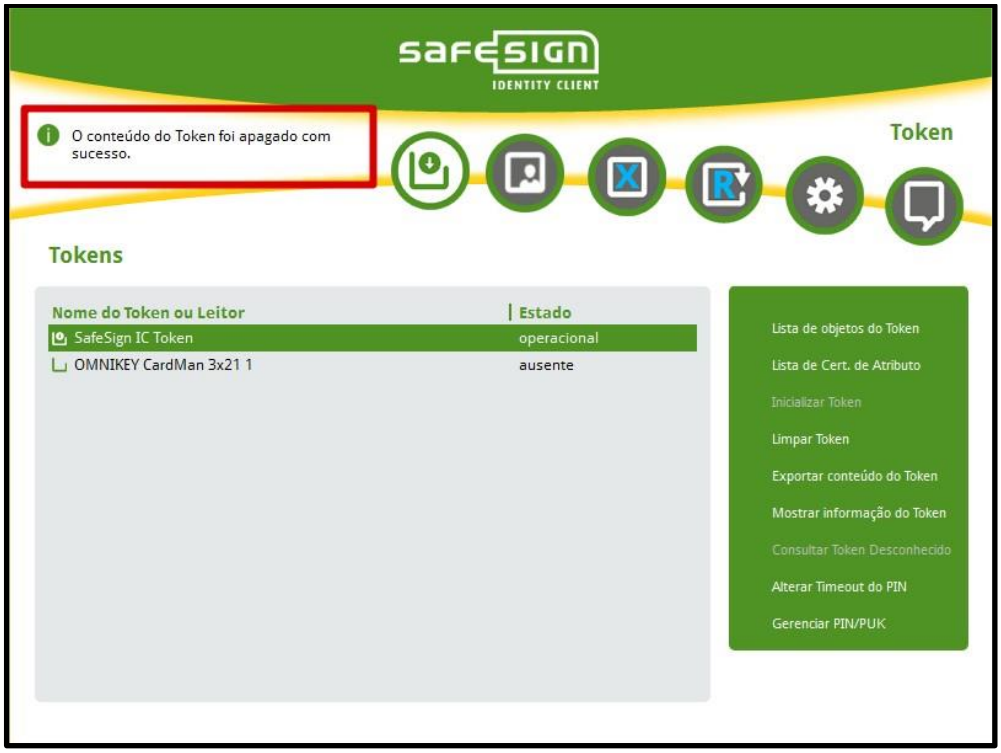

Figura 70: A operação foi concluída com sucesso

Quando o token é limpo, o (novo) nome do token aparecerá na janela de token:

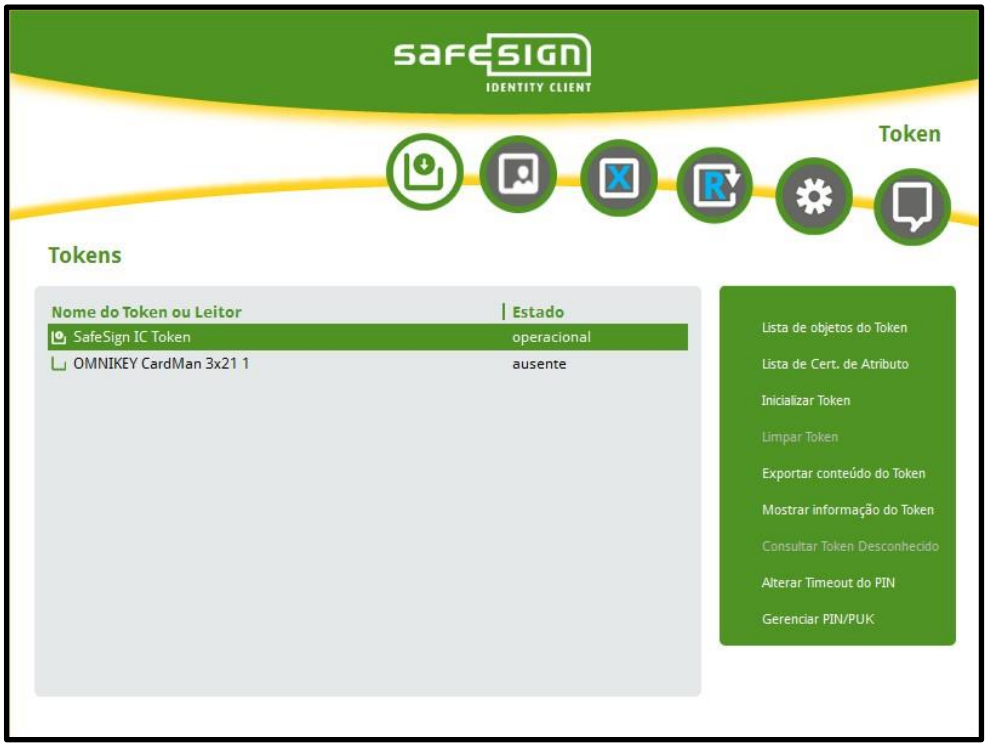

Figura 71: Token operacional

Assim que o seu token estiver limpo, todas as operações do menu **IDs Digitais** e **Token** ficarão disponíveis.

3.4 Reciclar Token

No aplicativo é possível fazer a reciclagem do token. A funcionalidade apenas ficará disponível se o token suportar a reciclagem e esgotar as tentativas do PIN e PUK da mídia.
Para simular uma reciclagem é necessário colocar o token no estado de bloqueado, ou seja, a introdução de 3 vezes consecutivas o PIN e o PUK errado.

Figura 72: Menu Reciclar Token ativo

Ao pressionar o menu "**Reciclar Token**" é apresentada uma questão para o usuário confirmar a reciclagem.

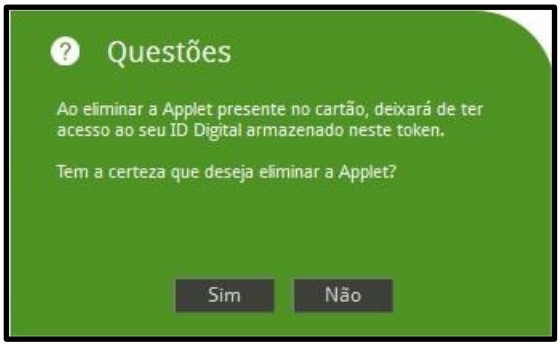

Figura 73: Confirmação da eliminação da applet

Ao clicar em **SIM**, receberá a informação de que o seu Token está sendo reciclado:

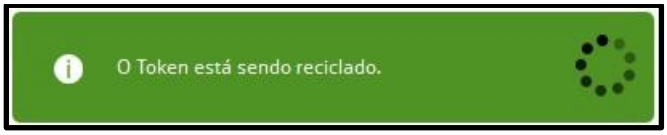

Figura 74: O seu token está sendo reciclado

Apenas alguns tokens suportam a reciclagem

O SafeSign Identity Client permite a reciclagem do token apenas se este o suportar. Para identificar se o seu token ou quais os tokens disponíveis com esta opção, contate com o seu fornecedor de mídia.

Depois da reciclagem do token é exibida uma tela para inicializar o mesmo. Para ver em mais detalhe o processo de inicialização do token ler capitulo 3.2.

3.5 Alterar PIN

O Aplicativo SafeSign IC permite-lhe alterar o PIN do seu Token SafeSign Identity Client.
Para tal, selecione *Gerir PIN / PUK* do menu **Token**. Isto abrirá a seguinte caixa de diálogo:

Selecione a opção **Alterar PIN**

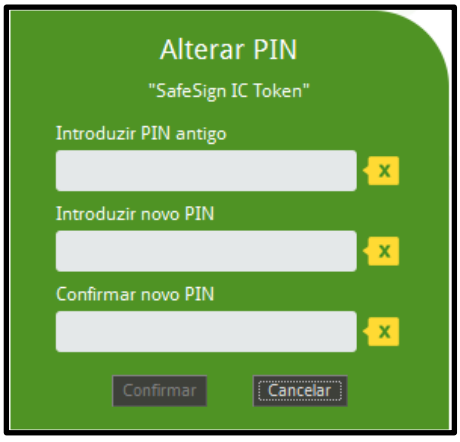

Figura 75: Utilitário de Token: Alterar PIN

Esta caixa de diálogo vai identificar o token para o qual quer alterar o PIN (“SafeSign IC Token” no exemplo).
Introduza o PIN antigo, o novo PIN e confirme o novo PIN.
Apenas quando introduzir corretamente o PIN antigo e o novo PIN (respeitando os requisitos de tamanho do PIN), ficará disponível o botão **OK**.

Introduza o PIN antigo, o novo PIN e confirme o novo PIN. De seguida clique **OK** para alterar o PIN

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Quando o PIN for alterado com sucesso, a seguinte caixa de diálogo aparecerá:

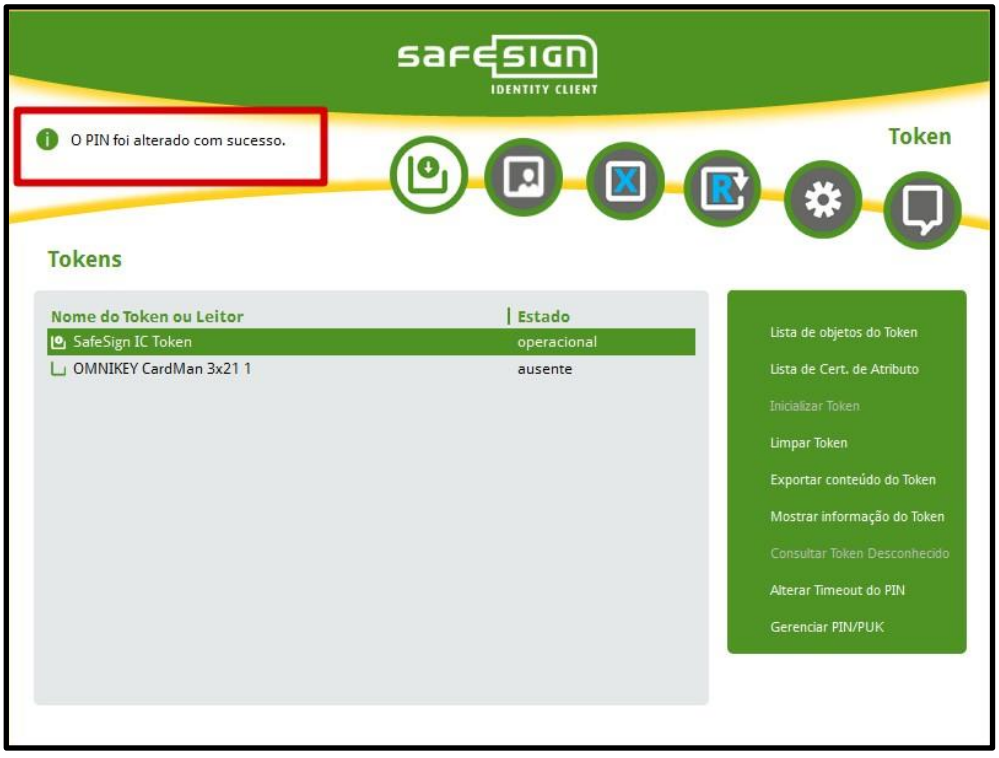

Figura 76: Utilitário de Token: O seu PIN foi alterado com sucesso

3.5.1 Informação do PIN

Sempre que inserir o seu PIN no Token SafeSign Identity Client, quer seja quando lhe for pedido em aplicações (e.g. na caixa de diálogo *Introduza o PIN* para aplicações Microsoft) ou no Utilitário de Token SafeSign Identity Client, o SafeSign Identity Client dar-lhe-á informação relativamente ao status do PIN.
Note que tem apenas **três** tentativas para inserir o PIN[8] correto e que o SafeSign Identity Client regista as tentativas e dará informação do estado do PIN. Se inserir um PIN incorreto três vezes, o token será BLOQUEADO e deverá recorrer à opção (**Gerir PIN/PUK > Desbloquear PIN)** do menu **Token** (conforme descrito na seção 3.7).

[8] Note que o seu administrador pode ter alterado o número máximo de tentativas de entrada correta do PIN.

A contagem de entradas de PIN incorreto será reiniciada para três tentativas se inserir o PIN correto após ter inserido um PIN incorreto, não mais de três vezes.
Na caixa de diálogo *Informação de Token* (**Token > Mostrar Informação de Token**), é mostrado o estado do PIN. Existem quatro cenários possíveis:

1. PIN está "*OK*" (como na Figura 77 abaixo):

Figura 77: Informação do Token: Estado do PIN

2. "*O PIN foi inserido incorretamente pelo menos uma vez*"
3. "*Resta uma tentativa para inserir o PIN correto*"
4. PIN foi "*BLOQUEADO*"
5. "*Desconhecido*"

Do mesmo modo, ao executar uma operação dentro do Aplicativo SafeSign IC SafeSign Identity Client, como *Alterar o PIN* (ou qualquer outro item em que é necessária a entrada de PIN), ser-lhe-á dada informação sobre o estado do PIN na caixa de diálogo respetiva. Também aqui são possíveis quatro notificações:

1. Quando o PIN está OK (nunca foi inserido um PIN incorreto):

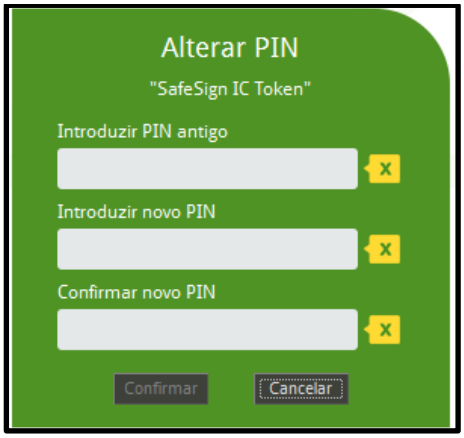

Figura 78: Utilitário de Token: *Alterar PIN*

2. Quando foi inserido um PIN incorreto:

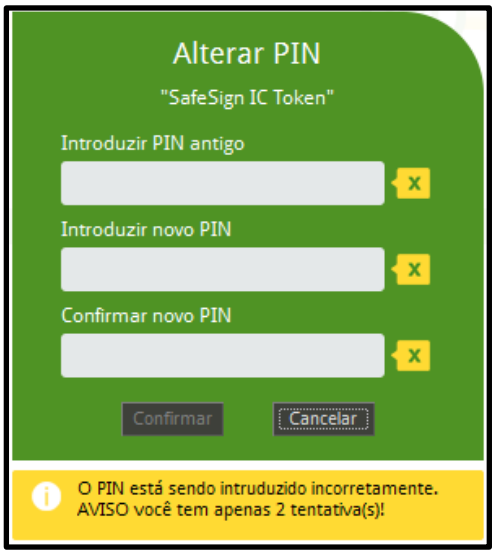

Figura 79: Alterar PIN: PIN incorreto

3. Quando resta apenas uma tentativa para inserir o PIN correto:

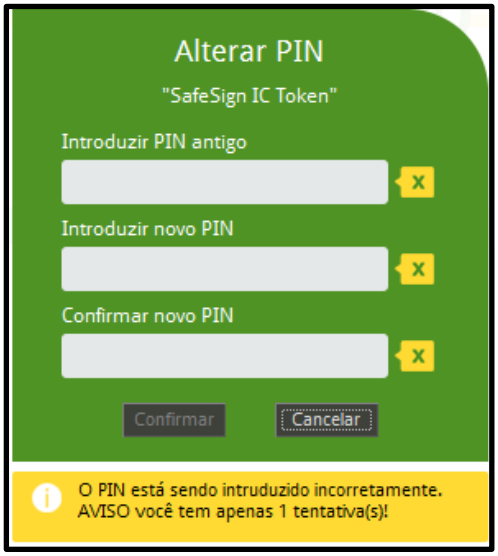

Figura 80: Alterar PIN: Resta-lhe apenas uma tentativa!

4. Quando o PIN foi bloqueado:

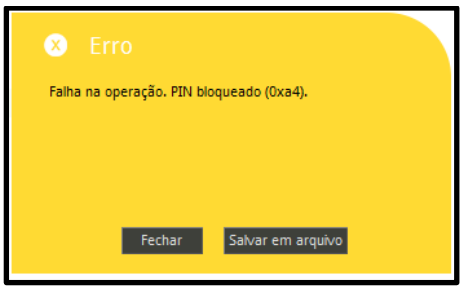

Figura 81: Alterar PIN: PIN bloqueado

3.6 Alterar PIN de Transporte

O PIN de transporte é um PIN temporário do token, que tem de ser alterado na primeira utilização do token. A definição de um PIN de transporte pode ser útil por motivos de segurança, por exemplo, quando quer ter a certeza que um usuário (conscientemente) define o seu próprio PIN antes de qualquer operação.

Note-se que o menu *Alterar PIN de Transporte* ficará disponivel apenas quando o token tem o PIN Transporte ativo. Se não, em sua vez, o menu de *Alterar o PIN* estará ativo.

Se o PIN de transporte está ativo, a informação do token a ser mostrada será:

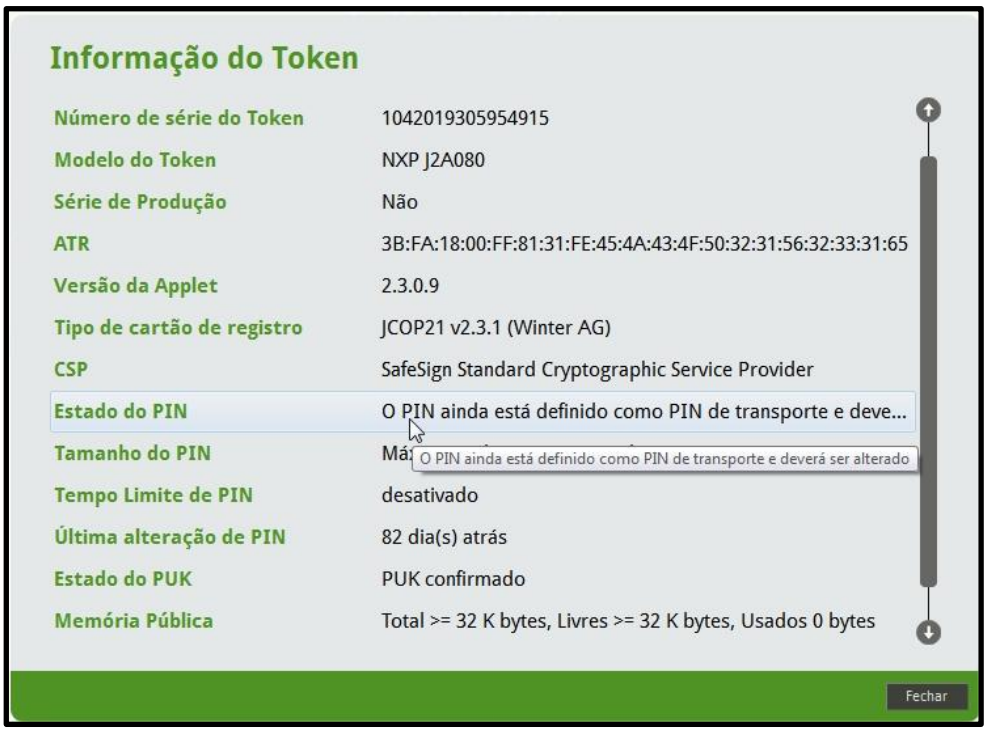

Figura 82: Alterar PIN de transporte : O PIN ainda está definido como PIN de transporte

Para alterar o PIN de Transporte clique no menu **Tokens > Gerenciar PIN/PUN** como mostra na imagem abaixo.

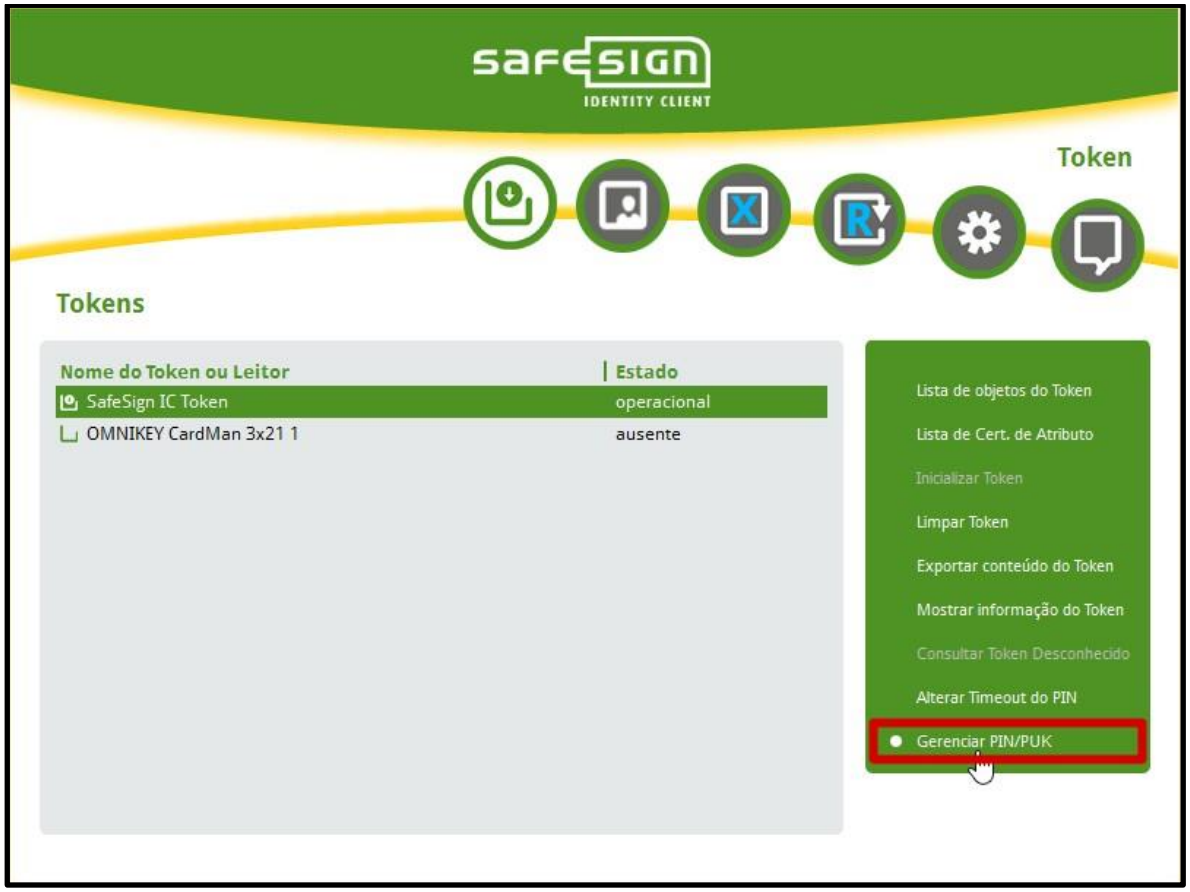

Figura 83: Alterar PIN de Transporte : Menu Gerenciar PIN/PUK

Na aplicação, o menu de *Alterar o PIN* não está disponível. A opção que está disponível é *Alterar o PIN de Transporte*:

Figura 84: Menu Alterar PIN de transporte

- Selecionar **Alterar PIN de Transporte**
- Clicar em **Confirmar**

A caixa para alterar o PIN é apresentada:

Figura 85: Alterar PIN de Transporte : Alterar PIN de Transport

- Digite o PIN de Transporte correto, um novo PIN (pessoal) e confirme o novo PIN.
- Depois de todos os campos estarem válidos, clicar em **Confirmar**

O PIN de Transporte será alterado para o novo PIN inserido,após o qual será informado.

3.7 Desbloquear PIN

O Utilitário de Administração de Token SafeSign Identity Client permite desbloquear o PIN do seu Token SafeSign Identity Client (quando este está bloqueado, como na Figura 81).

Note que o item *Desbloquear PIN* só estará disponível quando o PIN estiver bloqueado. Se não for o caso, o item aparecerá esbatido.

A Seção 3.7.1 descreve este processo.

3.7.1 Desbloquear usando o PUK

Para desbloquear o PIN, selecione *Desbloquear PIN* do menu **Token**.

Surgirá a seguinte caixa de diálogo:

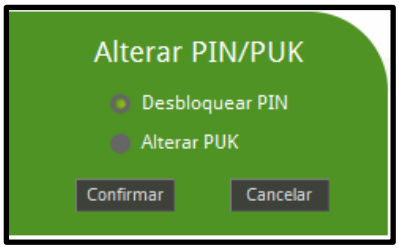

Figura 86: Selecionar opção Desbloquear PIN

Figura 87: Aplicativo SafeSign IC: Desbloquear PIN

Esta caixa de diálogo identifica o token cujo PIN pretende desbloquear (“SafeSign IC Token” no exemplo acima).
Insira o PUK, um novo PIN e confirme o novo PIN.
Apenas quando inserir o PUK correto e o novo PIN coincida com a respetiva confirmação, preenchendo os requisitos de tamanho do PIN, o botão **OK** ficará disponível.
Clique **OK** para desbloquear o PIN

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido9. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Quando o PIN tiver sido desbloqueado com sucesso, surgirá a seguinte notificação:

[9] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

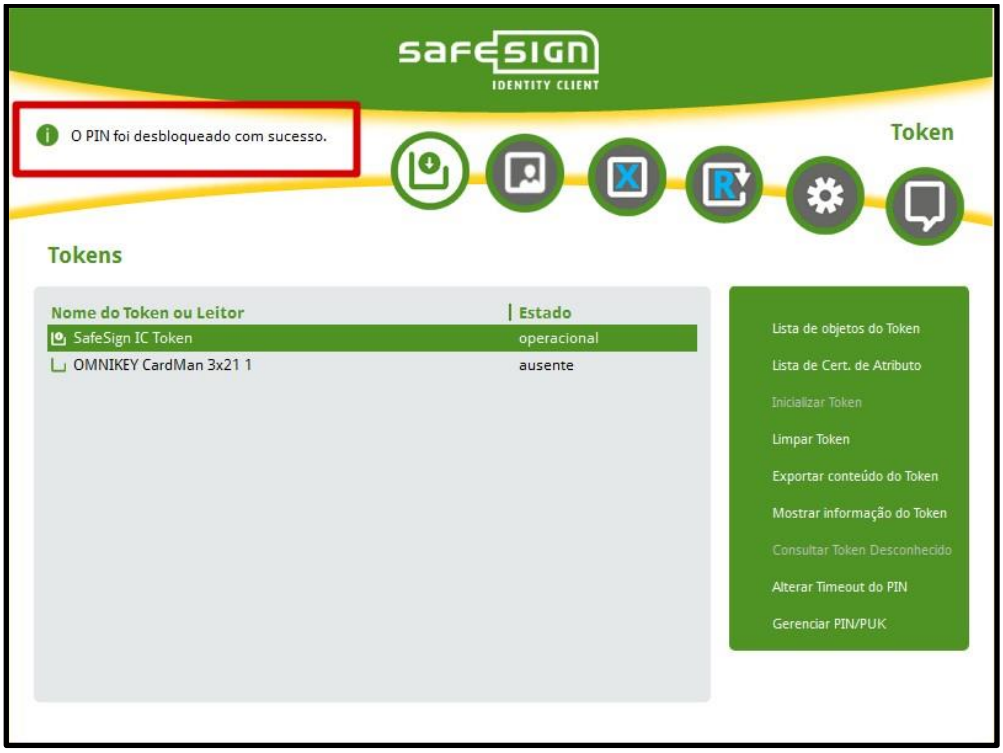

Figura 88: Desbloquear PIN: O seu PIN foi desbloqueado com sucesso

O seu PIN deverá estar agora desbloqueado e pronto para ser utilizado novamente, como poderá comprovar ao conseguir novamente usar todos os itens do menu (tais como *Importar IDs Digitais*).

3.8 Alterar PUK

O Utilitário de Token SafeSign Identity Client permite-lhe alterar o PUK do seu Token SafeSign Identity Client.

Para tal, selecione (**Gerir PIN/PUK > Alterar PUK**) do menu **Token**. Isto abrirá a seguinte caixa de diálogo:

Figura 89: Gerir PIN/PUK

Figura 90: Utilitário de Token: Alterar PUK

Esta caixa de diálogo vai identificar o token para o qual quer alterar o PUK (“SafeSign IC Token” no exemplo).

Introduza o PUK antigo, o novo PUK e confirme o novo PUK.

Apenas quando introduzir corretamente o PUK antigo e o novo PUK (respeitando os requisitos de tamanho do PUK), ficará disponível o botão **OK**.

Clique **OK** para alterar o PUK

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido[10]. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Quando o PUK for alterado com sucesso, surgirá a seguinte notificação:

[10] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

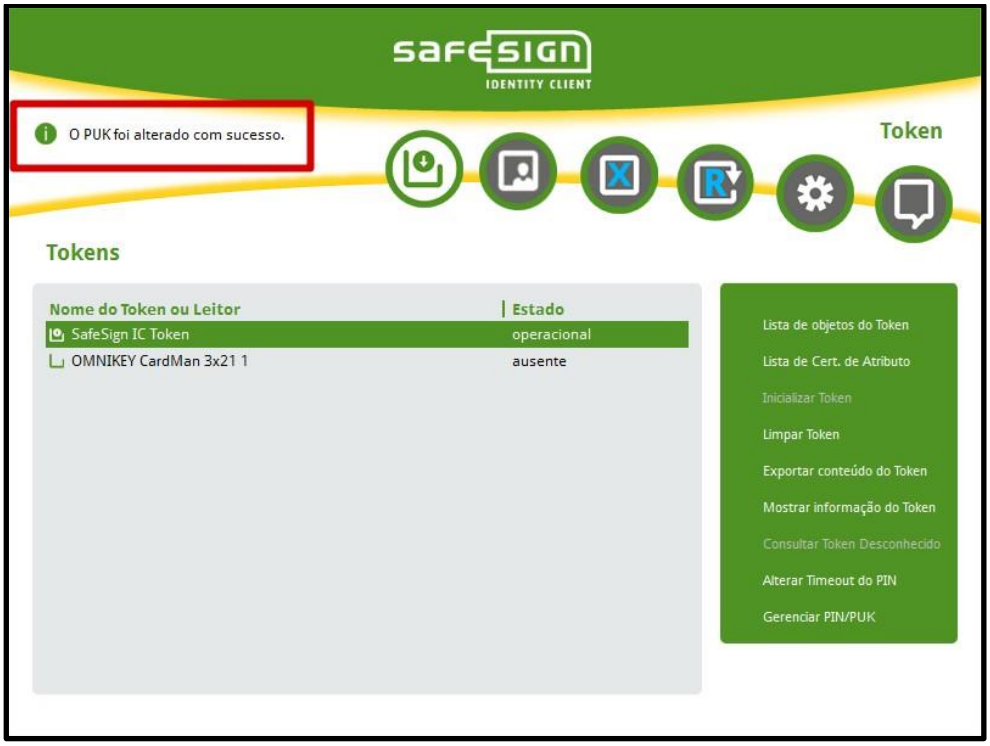

Figura 91: Alterar PUK: O seu PUK foi alterado com sucesso

3.8.1 Informação do PUK

Sempre que inserir o seu PUK no Token SafeSign Identity Client, que provavelmente que lhe será pedido nos itens Alterar PIN ou Alterar PUK do Aplicativo SafeSign IC, o SafeSign Identity Client dar-lhe-á informação relativamente ao estado do PUK.

Note que tem apenas **três** tentativas para inserir o PUK[11] correto e que o SafeSign Identity Client regista as tentativas e dará informação do estado do PUK. Se inserir um PUK incorreto três vezes, o token será BLOQUEADO.

A contagem de entradas de PUK incorreto será reiniciada para três tentativas se inserir o PUK correto após ter inserido um PUK incorreto (mas não mais de três vezes).

Nota

Se inserir um PUK incorreto três vezes, o PUK será bloqueado e não pode ser desbloqueado. Para um token de teste, isto implica que volte a inicializar o token, perdendo todos os dados armazenados no token. Para um token de produção, o seu token torna-se inútil, uma vez que não pode eliminar os conteúdos do token já que precisaria do PUK para o fazer.

Na caixa de diálogo *Informação de Token* (**Token > Mostrar Informação de Token**), é mostrado o estado do PUK. Existem cinco cenários possíveis:

1. PUK está "*OK*" (como na Figura 92 abaixo)

[11] Note que o seu administrador pode ter alterado o número máximo de tentativas de entrada correta do PIN.

Figura 92: Informação do Token: Estado do PUK

2. "*O PUK foi inserido incorretamente pelo menos uma vez*"
3. "*Resta uma tentativa para inserir o PUK correto*"
4. O PUK foi "*BLOQUEADO*"
5. "*Desconhecido*"

Do mesmo modo, ao executar uma operação dentro do Utilitário de Administração de Token SafeSign Identity Client, como *Alterar PUK* (ou qualquer outro item em que é necessária a entrada de PUK), ser-lhe-á dada informação sobre o estado do PUK na caixa de diálogo respetiva. Também aqui são possíveis quatro notificações:

1. Quando o PUK está OK (nunca foi inserido um PIN incorreto):

Figura 93: Utilitário de Token: Alterar PUK

2. Quando foi inserido um PUK incorreto:

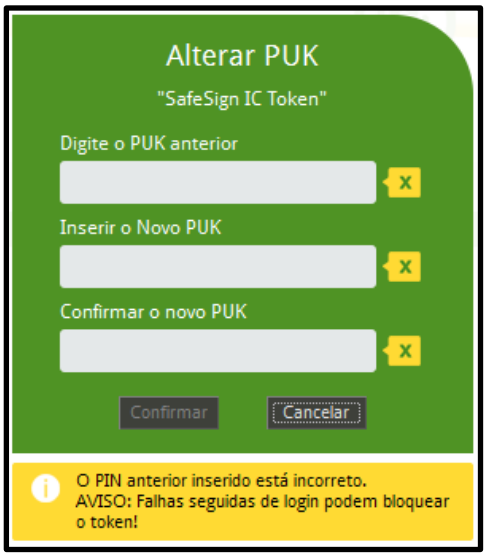

Figura 94: Alterar PUK: PUK incorreto

3. Quando resta apenas uma tentativa para inserir o PUK correto:

Figura 95: Alterar PUK: Resta-lhe uma tentativa!

4. Quando o PUK foi bloqueado:

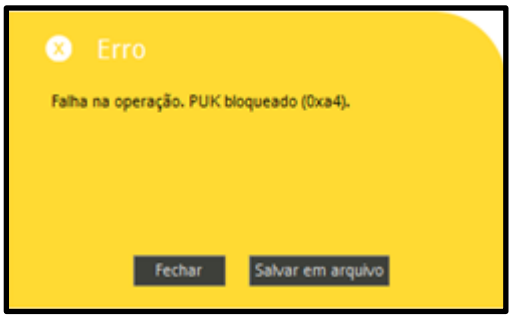

Figura 96: Alterar PUK: PUK bloqueado

Token Bloqueado

Quando o PIN do token está bloqueado, o Utilitário de Token fica com o aspeto seguinte:

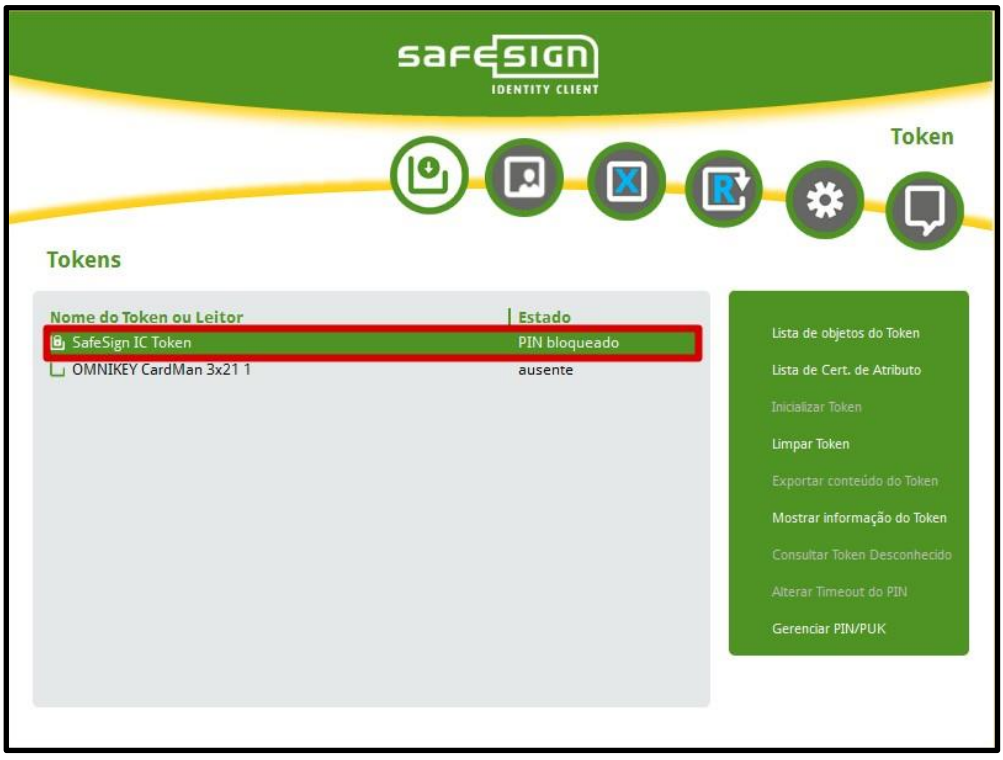

Figura 97: Utilitário de Token: PIN bloqueado

Quando o PUK do token está bloqueado, o Utilitário de Token fica com o aspeto seguinte:

Figura 98: Utilitário de Token: PUK/Token bloqueado

Note que neste caso, apenas um token de teste pode ser reinicializado (eliminando desta forma todos os conteúdos que estivessem no token e reescrevendo por complete a estrutura de ficheiros). Por sua vez, um token de produção nesta situação tornou-se inútil.

3.9 Mostrar Informação de Token

A caixa de diálogo *Informação de Token* (**Token > Mostrar Informação de Token**) apresenta informações sobre o Token inserido:

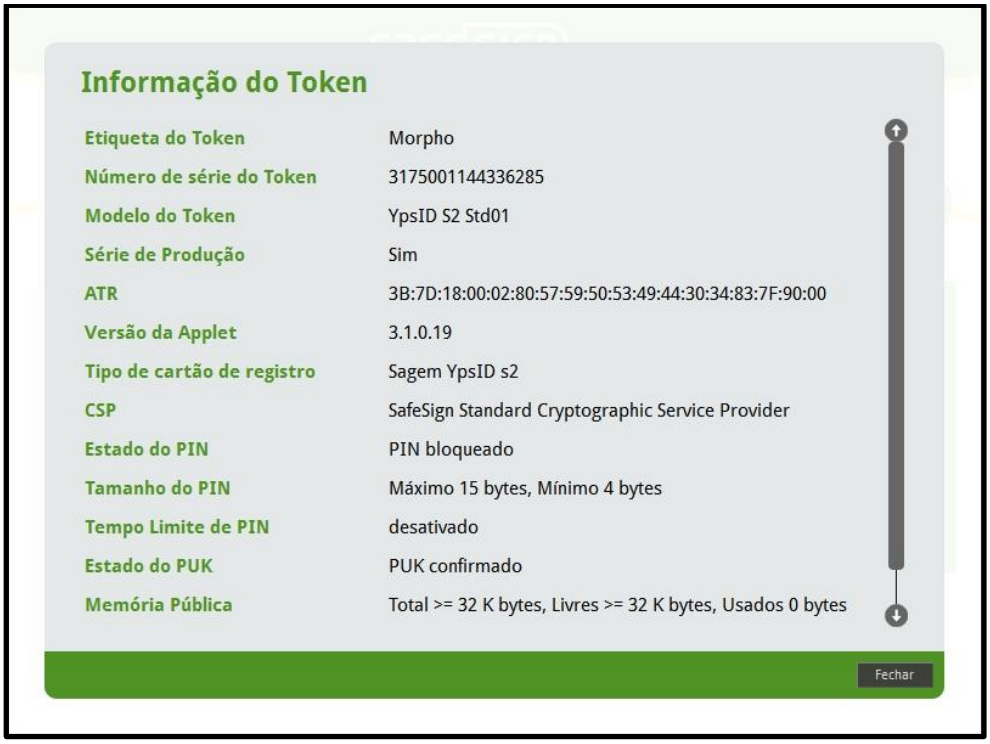

Figura 99: Utilitário de Token: Informação de Token

Figura 100 : Utilitário de Token: Informação de Token (continuação)

O Campo Informação de Token apresenta as seguintes informações:

Campo	Valor
Rótulo do Token	[rótulo do token]
	Mostra o rótulo do token atribuído pelo administrador ou pelo próprio usuário.
Número de série do Token	[número de série]
	Mostra o número de série do token (normalmente o número de série do chip).
Modelo do Token	[modelo do token]
	Mostra o modelo e versão do token.
Conclusão de série	[Sim / Não]
	Mostra se se trata de um token de teste ou de produção. Quando se trata de um token de teste, mostrará [Não], significando que poderá reinicializar o token; Quando se trata de um token de produção, mostrará [Sim], significando que pode apenas apagar os conteúdos do token.
ATR	[ATR]
	Answer To Reset (ATR) é uma mensagem apresentada por um smart card de contacto em conformidade com os standards ISO/IEC 7816.
Tipo de cartão de registo	[tipo de cartão de registo]
	Mostra o nome do cartão como este aparece na chave do Microsoft Cryptography[12].
CSP	[SafeSign Standard Cryptographic Service Provider]
	Mostra a configuração do CSP do token.
Versão da Applet	[Versão da Applet]
	A versão da applet que está dentro do token.
Mensagem Segura ativa	[Sim / Não]
	Informa se a comunicação com o cartão ou token USB ocorre de forma encriptada
Contador de Reciclagem	[Contador de Reciclagem]
	Número máximo de vezes que o PIN pode ser alterado. Também, o número de vezes já usado.
Estado do PIN	[Mensagem de estado do PIN]
	Mostra o estado do PIN: OK O PIN foi inserido incorretamente pelo menos uma vez Resta uma tentativa para inserir o PIN correto

[12] A chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards.

	BLOQUEADO
Tamanho do PIN	[máximo x caracteres / mínimo x caracteres]
	Mostra o número máximo e mínimo de caracteres exigido para o tamanho do PIN.
PIN Timeout	[desativo / -]
	Mostra o status das definições de tempo limite da autenticação do PIN, que está desativado por defeito. Quando o tempo limite do PIN timeout é ativado, é pedido que se autentique (novamente)com o token, i.e. surgirá uma caixa de diálogo do PIN SafeSign. Por exemplo, ao utilizar o Outlook para enviar emails assinados ou ao utilizar o Adobe Reader para assinar um documento, ser-lhe-á pedido para inserir novamente o seu PIN quando o tempo limite tiver sido ultrapassado desde a última vez que se autenticou no token.
Última alteração do PIN	[Última vez em dias]
	É possível definir um limite de validade do PIN. Quando definido, será notificado de que o seu PIN é inválido ou tornar-se-á inválido dentre de um número de dias, e será pedido que o altere. Contudo, não é mandatório que altere o PIN para um novo valor (pode inserir o mesmo PIN e não é exigida conformidade com nenhuma política de PIN). Quer esteja ativado ou não, a caixa de diálogo *Informação do Token* do Utilitário de Token incluirá um item denominado 'Última alteração do PIN' e registará há quantos dias o PIN foi definido / alterado.
Estado do PUK	[mensagem de estado do PUK]
	Mostra o estado do PUK: • OK • O PUK foi inserido incorretamente pelo menos uma vez • Resta uma tentativa para inserir o PUK correto • BLOQUEADO
Memória Pública / Memória Privada	[Total x bytes / Livre x bytes / Ocupado x bytes]

	Mostra a quantidade total de bytes, a quantidade livre de bytes e a quantidade de bytes ocupada do total de bytes disponíveis na memória pública no token (após inicialização).

Nota

Note que a memória privada não é o local onde as chaves privadas são armazenadas. Em concordância com o padrão PKCS#15, as chaves privadas estão localizadas num diretório, enquanto que a memória privada é usada para armazenar objetos seguros, por exemplo.

Isso explica o porquê da quantidade de espaço privado não diminuir quando é inserido um token que contém chaves privadas.

3.10 Mostrar Objetos do Token

A opção Mostrar Objetos do Token permite uma visão mais técnica e detalhada dos conteúdos do token. Esta opção mostra todos os objetos (públicos) que estão no token. Selecione **Mostrar Objetos do Token** a partir do menu Token para abrir a lista de objetos PKCS#11:

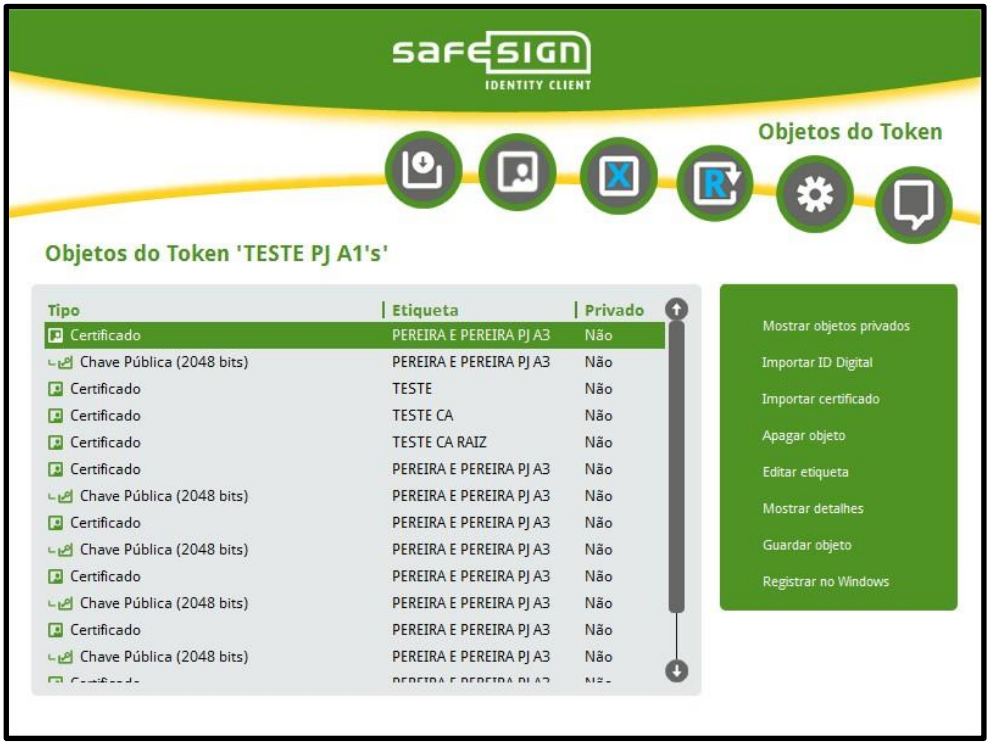

Figura 101: Objetos PKCS#11: Objetos do Token

Esta lista mostrará os objetos públicos do token.

Para ver todos os objetos / objetos privados no token, clique **Mostrar Objetos Privados**

Ao selecionar **Mostrar Objetos Privados**, ser-lhe-á pedido o PIN do token:

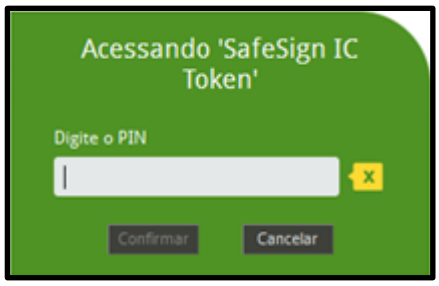

Figura 102: Objetos PKCS#11: Insira PIN

Insira o PIN correto para visualizar os objetos privados no token.

Ao digitar o PIN correto, os objetos privados no token também serão mostrados:

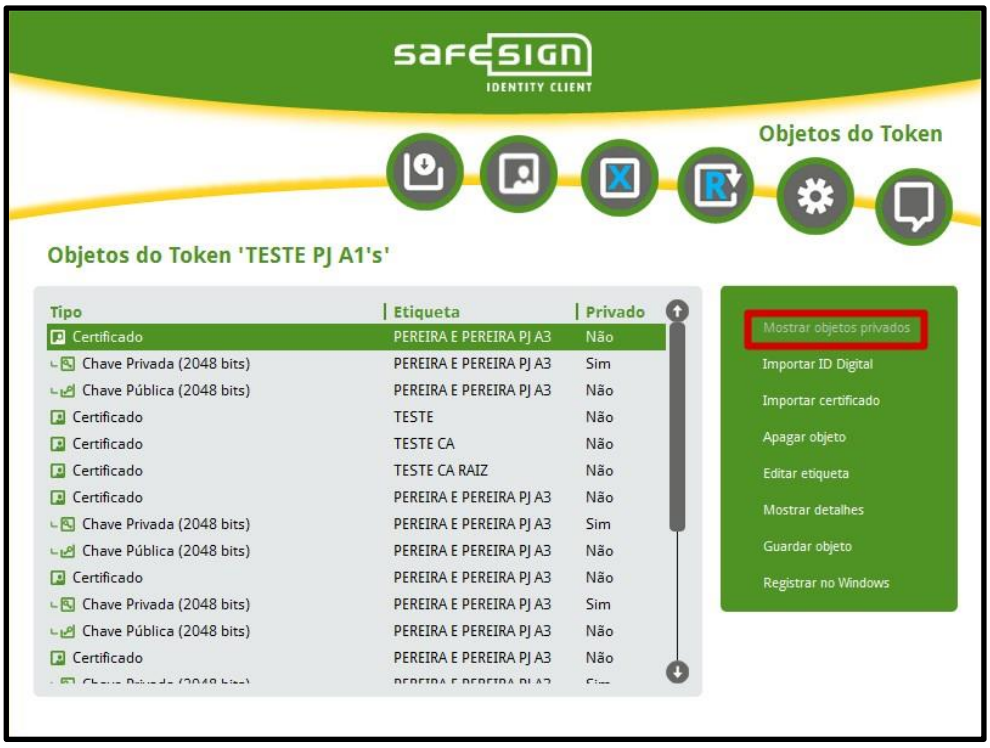

Figura 103: Objetos PKCS#11: Todos os objetos

É possível um número variado de operações no que diz respeito aos objetos no token, que são descritas nas próximas secções.

3.10.1 Ver Certificado

Permite visualizar o conteúdo do certificado.
Clique em **Ver Certificado** para visualizar os conteúdos do certificado:

Figura 104: Ver Certificado: Informação do Certificado

3.10.2 Salvar Objeto

Permite salvar certificados no formato *.cer, bem como objetos de dados no token.

Nota

Note que o botão "Gravar o Arquivo" na Figura 104 faz o mesmo para certificados.

Clique em **Salvar Objeto** para selecionar a localização onde pretende salvar o ficheiro:

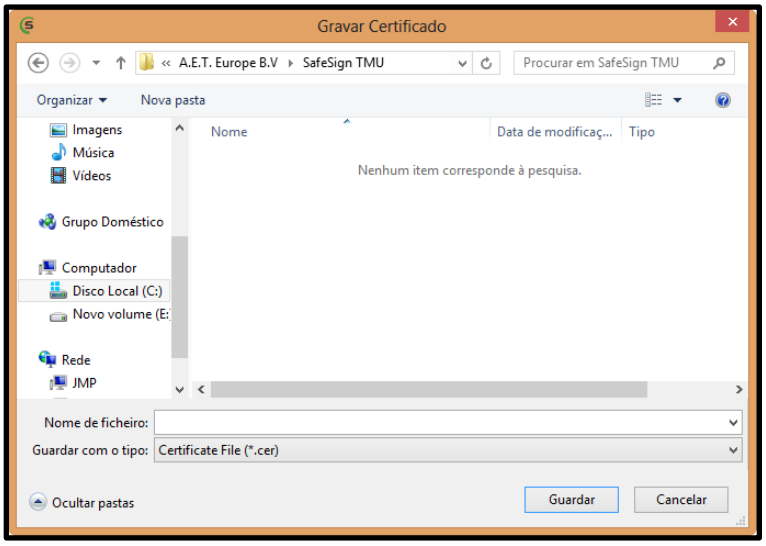

Figura 105: Salvar Objeto: Salvar certificado

Selecione a localização e clique **Guardar**

3.10.3 Importar ID Digital

O SafeSign IC permite-lhe importar um ID Digital para o seu token SafeSign Identity Client. Ao importar o ID Digital, as suas chaves e certificados serão guardados com segurança no seu token e podem ser utilizados para comunicações seguras.
Isto melhora visivelmente a segurança do seu ID Digital, agora protegido por uma autenticação de dois fatores: para aceder necessitará do token e saber o respetivo PIN.
A função Importar ID Digital pode ser usada para importar ficheiros de ID Digital armazenados no seu disco rígido ou dispositivos amovíveis (como um CD) no formato PKCS #12 ou PFX, desde que a função Transferir ID para o token (disponível em **Mostrar IDs Digitais Registadas**) possa ser utilizada para IDs Digitais presentes no Microsoft Personal Certificate Store.

Nota

O termo 'ID Digital ' refere-se à combinação de um certificado (incluindo uma chave pública) e uma chave privada (formato PKCS #12) normalmente protegida por uma password.

Esta ID Digital deverá estar armazenada como um ficheiro PKCS#12 (.p12) ou um ficheiro Personal Information Exchange (.pfx), que são ambos formatos que contêm a sua chave privada, num CD ou no seu disco rígido.

Um ficheiro neste formato pode ser obtido quer através da exportação de chaves e certificados do seu Firefox (.p12) ou do seu Microsoft Certificate Store (.pfx). Note que durante este processo ser-lhe-á pedido para inserir uma palavra chave para proteger o seu ficheiro. Esta palavra chave é necessária aquando da importação de uma ID Digital para o seu token SafeSign Identity Client.

Note que a aplicação usada (e a sua versão) determina a aparência do formato de uma ID Digital.

Quando o SafeSign Identity Client importa uma ID Digital, a chave pública não é armazenada no token, de forma a poupar espaço no token, uma vez que a chave pública não em que estar no token já que está embebida no certificado e utilizada apenas para operações de chave pública (e não tem que ser mantida secreta).

O usuário poderá a qualquer altura visualizar as IDs digitais disponíveis para si no menu IDs Digitais, que mostrará corretamente as IDs Digitas que podem ser usadas para operações criptográficas.

Para importar uma ID Digital, selecione o Token (Menu Token 3) para onde quer copiar a ID Digital, de seguida clique em **Mostrar Objetos do Token** > **Importar ID Digital**:

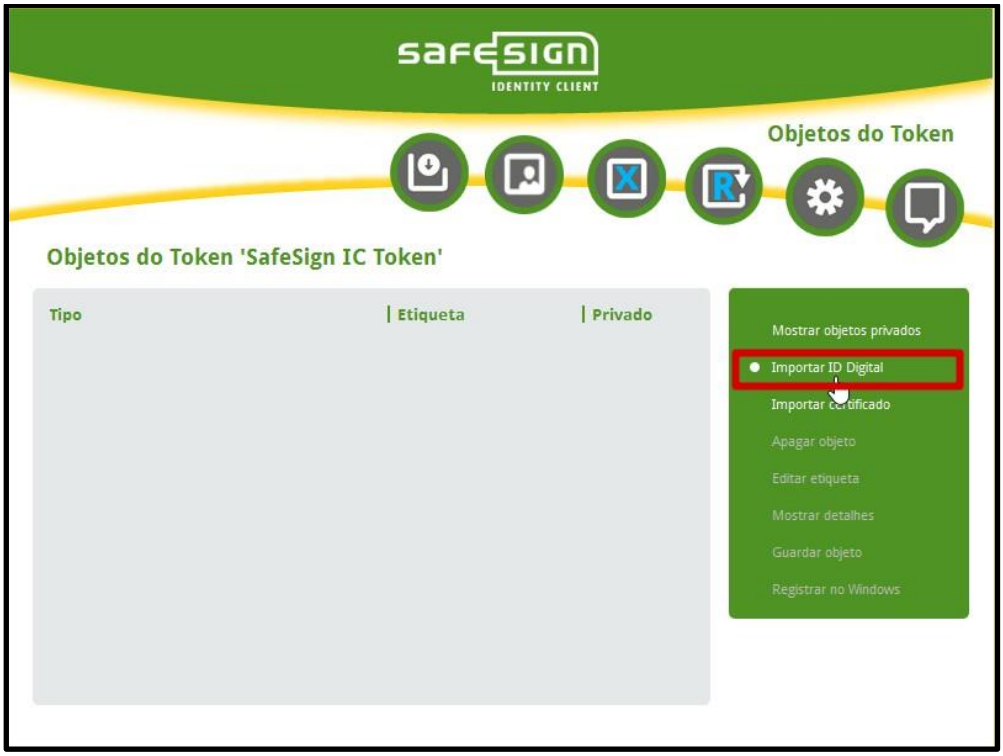

Figura 106: Utilitário de Token: Importar ID Digital

A seguinte caixa de diálogo surgirá:

Figura 107: Importar ID Digital

Primeiro, é necessário especificar a localização onde o ficheiro da ID Digital está armazenado. O ficheiro da ID Digital pode estar armazenado em qualquer lugar, quer seja num disco rígido quer seja num CD. Clique no símbolo para selecionar a localização:

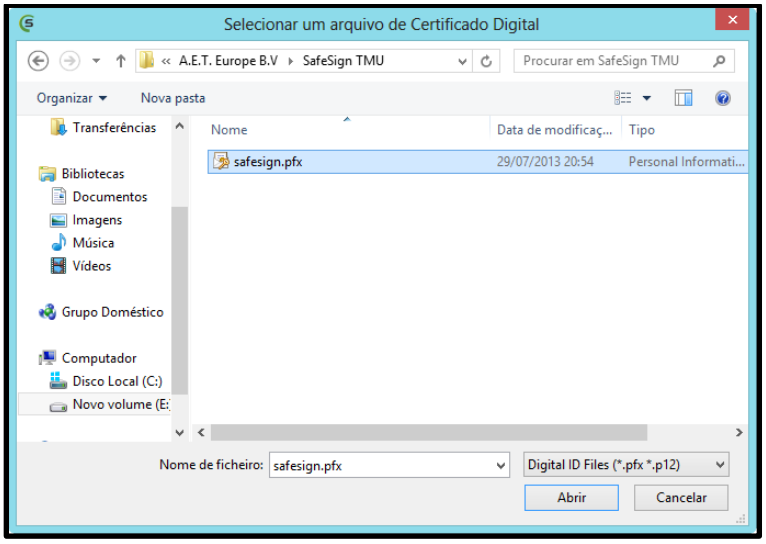

Figura 108: Importar ID Digital: Selecionar um ficheiro de ID Digital

No exemplo acima, o ficheiro está armazenado em: ***A.E.T. Europe B.V\SafeSign TMU***

Selecionar o ficheiro de ID Digital clicando sobre ele, e clicar de seguida no botão **Abir**

A caixa de diálogo Importar ID Digital seguinte mostrará o (caminho para o) ficheiro de ID Digital que acabou de selecionar:

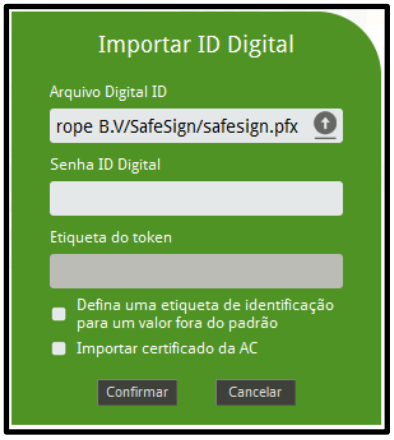

Figura 109: Importar ID Digital: Ficheiro de ID Digital Selecionado

O passo seguinte é inserir a password do ID Digital

Importar Certificados da AC

Ao importar uma ID Digital, pode escolher se pretende importar também os certificados da AC. Esta escolha irá assegurar máxima flexibilidade e interoperabilidade. Ao levar o seu token para outro computador (onde a cadeia de certificação confiável apropriada poderá não estar instalada), terá sempre os seus certificados consigo e poderá registá-los.

Por omissão, a opção **Importar certificado da AC** está selecionada.

Se não desejar importar os certificados da AC para o token, desseleccione a opção.

Definir a etiqueta do ID no token para um valor não predefinido

Ao importar uma ID Digital, será copiada a etiqueta da ID Digital tal como definida pela aplicação utilizada para obter a ID Digital. Se desejar definir a sua própria etiqueta para o certificado e chave privada, selecione **Defina uma etiqueta de identificação para um valor fora do padrão** e insira uma etiqueta na caixa **Etiqueta do token**.

Pode ver a etiqueta (alterada) na caixa de diálogo Mostrar objetos do token, definido para o certificado e chave privada.

Inserir a password para o ficheiro de ID Digital:

Figura 110: Importar ID Digital: Password de ID Digital inserida

Clique **OK** para importar a ID Digital

Password Errada

A password que lhe é pedida é a password que usou para proteger a ID Digital.

Se não inserir a password correta, será devolvida a seguinte caixa de diálogo:

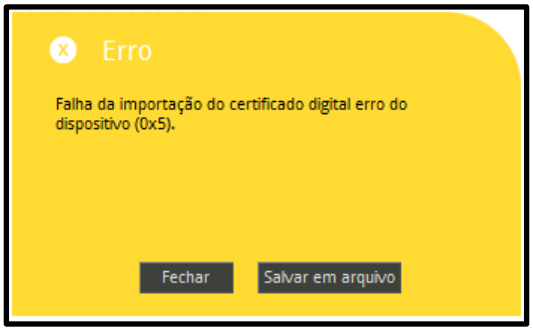

Figura 111: Erro: O ficheiro da ID Digital necessita de uma senha diferente

Clique Fechar para fechar a caixa de diálogo

Clique Salvar em Arquivo para guardar a mensagem de erro no computador

Terá que iniciar de novo o procedimento de importação de ID Digital clicando em **IDs Digitais > Importar ID Digital.**

Quando tiver clicado **OK** após inserir a password correta para o ficheiro de ID Digital, ser-lhe-á pedido que insira o PIN para o Token:

Figura 112: Importar ID Digital: Introduzir PIN

Insira o PIN correto e clique **OK**

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido13. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

Ao clicar **OK** após inserir o PIN correto, a ID Digital será importada:

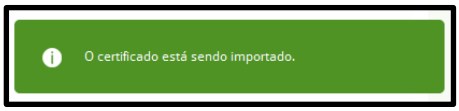

Figura 113: Importar ID Digital: Em trabalho

A sua **ID Digital** está a ser importada

Quando a ID Digital tiver sido importada com sucesso, surgirá a seguinte notificação:

[13] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

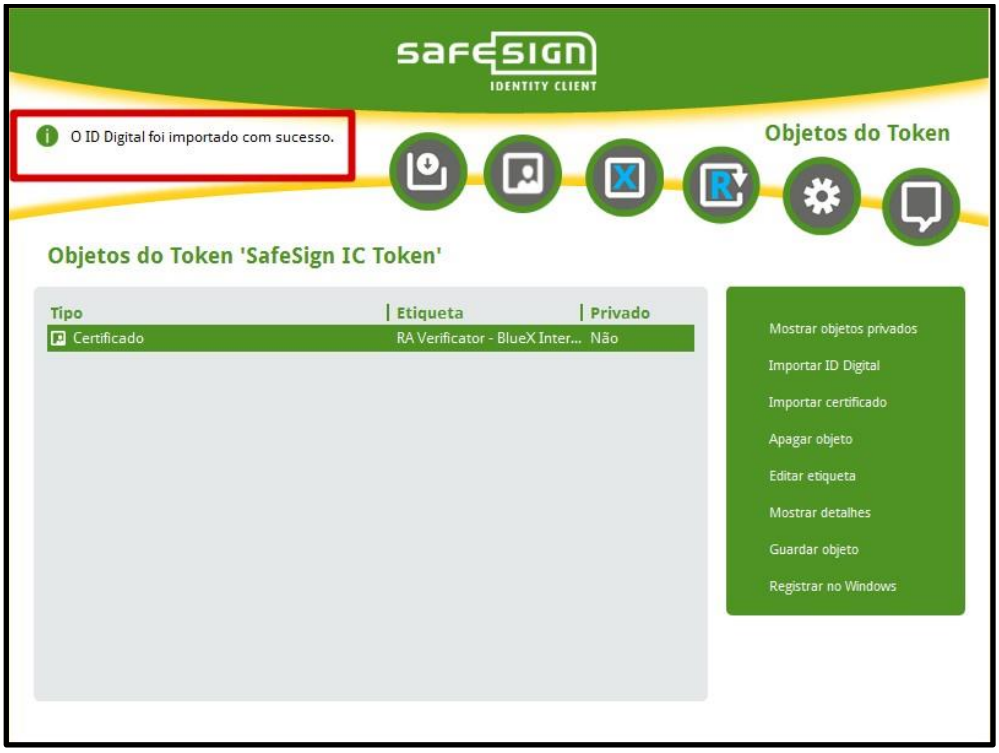

Figura 114: Importar ID Digital: A ID Digital foi importada com sucesso

Erro de Tamanho da Chave

Sempre que tentar importar uma ID Digital que não esteja de acordo com as restrições de comprimento da chave do token suportado, surgirá a seguinte caixa de diálogo:

Figura 115: Erro: Tamanho de chave menor que 768 bits ou maior do que 2048 bits

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

Token com Memória insuficiente

Quando o token estiver cheio, i.e. não tem memória suficiente para importar uma ID Digital, surge a seguinte caixa de diálogo:

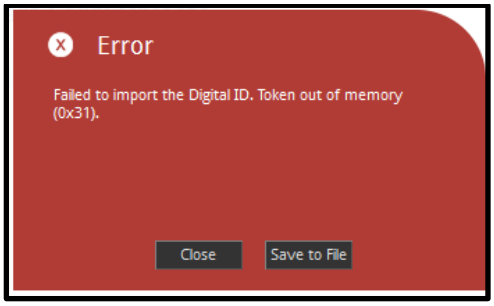

Figura 116: Erro: Token sem memória livre

Clique **Fechar** para fechar a caixa de diálogo.
Clique Salvar para Ficheiro para guardar a mensagem de erro no computador

Pode verificar na caixa de diálogo Informação de Token (**Token > Mostrar Informação de Token**) o espaço ainda disponível no Token. Note que o token pode conter partes do ficheiro de ID Digital importado (e.g. quando contém vários certificados).

Depois de importar uma ID Digital, poderá verificar na caixa de diálogo de ID Digital (**IDs Digitais**) se a ID Digital foi importada corretamente:

Figura 117: Utilitário de Token: ID Digital Importada

3.10.4 Importar Certificado

O Utilitário de Administração de Token permite-lhe importar um certificado de Autoridade Certificadora (AC) para o seu token SafeSign Identity Client. Ao importar o ficheiro, o certificado da AC será guardado com segurança no seu token, melhorando significativamente a mobilidade e flexibilidade do seu token SafeSign Identity Client.

Ao usar o seu token SafeSign Identity Client noutro computador, em que o certificado da AC (root) não está instalado, o SafeSign Identity Client permitir-lhe-á instalar o certificado da AC, criando uma cadeia de certificação confiável para o seu ID Digital pessoal (o qual não seria seguro sem o certificado da AC que originou a sua instalação, como no caso em que o "*Windows não possui informação suficiente para verificar este certificado*" porque "*a origem deste certificado não foi encontrada*").

O utilitário suporta a importação de certificados armazenados em arquivos:

- Com extensões .pem, .cer, .crt ou .der;
- Codificados em formato DER ou PEM.

Nota

Os certificados da AC também podem ser importados durante a inicialização do token. Por favor consulte a seção 3.1.3

Para importar um certificado CA, selecione o Token para onde quer copiar o certificado, e de seguida clique **Mostrar Objetos do Token > Importar Certificado**:

Figura 118: Utilitário de Token: Importar Certificado

Ser-lhe-á pedido que especifique a localização em que o Certificado está armazenado:

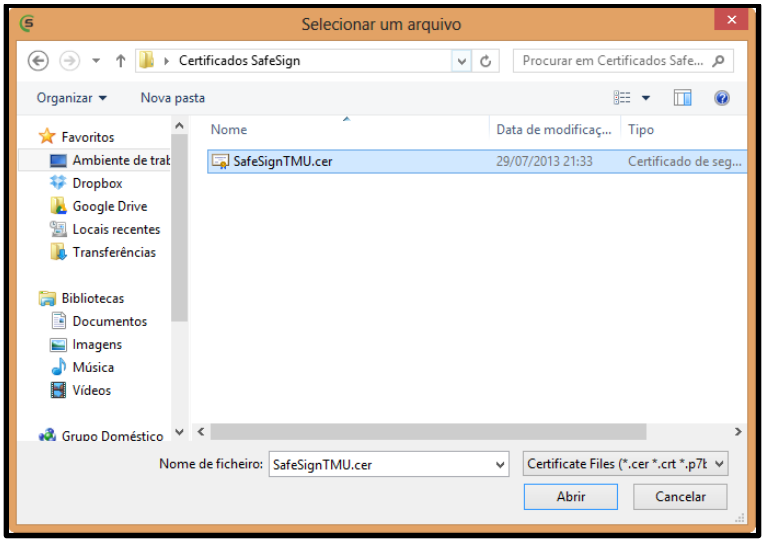

Figura 119: Importar Certificado: Nome do ficheiro

Especifique onde o certificado está armazenado. O Certificado pode ser armazenado em qualquer lugar, tanto num disco rígido como num dispositivo removível (como uma pen de memória USB).
No exemplo acima, o ficheiro estava armazenado em: ***\Desktop\Certificates SafeSign***
Selecione o ficheiro clicando sobre o mesmo, e de seguida clique **Abrir**

Após selecionar o certificado a importar, ser-lhe-á pedido que insira o PIN do seu Token SafeSign Identity Client:

Figura 120: Importar Certificado: Insira PIN

Insira o PIN e clique no botão **OK** para importar o ficheiro do certificado

Tamanho do PIN / PUK

O SafeSign Identity Client impõe um limite mínimo e máximo para o PIN / PUK. Se inserir um PIN / PUK com um tamanho inferior ao mínimo estabelecido ou superior ao máximo permitido, não será permitido clicar no botão OK nas instâncias em que o PIN / PUK é pedido14. Apenas quando inserir um PIN / PUK com o tamanho exigido é que este será aceite. Note que ambos os tamanhos mínimo e máximo do PIN / PUK podem ser ter sido configurados com valores diferentes (dos valores suportados por defeito pelo cartão) pelo administrador.

[14] Quando o tamanho máximo do PUK / PIN excede o comprimento máximo exigido, o botão **OK** ficará inativo.

Assim que o certificado tenha sido importado, será notificado:

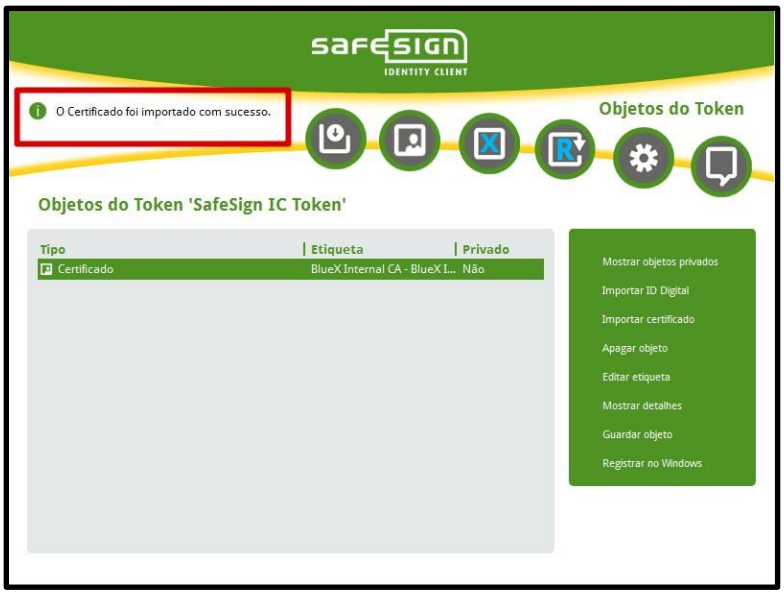

Figura 121: Utilitário de Token: Certificado importado com sucesso

3.10.5 Editar Rótulo

Poderá editar o rótulo de chaves e certificados públicos e privados (ex.: para poder identificar que chaves públicas, privadas e certificados formam par) ou poderá editar o rótulo das chaves públicas e privadas e dos certificados (e.g. para poder identificar que chaves públicas e privadas formam par com o certificado).

Nota

Ao pedir um par de chaves e certificado através do CSP, o par de chaves é gerado antes do certificado. O SafeSign Identity Client faz a correspondência do rótulo da chave privada e da chave pública com o rótulo do certificado de forma a distinguir que chaves públicas, privadas e certificados formam par.

Ao clicar **Editar Rótulo**, surge a seguinte caixa de diálogo:

Figura 122: Alterar Rótulo: nome

Insira o novo rótulo e clique OK para salvar.

Após digitar o PIN correto do token, o rótulo será alterado.

Nota

Terá que editar o rótulo de cada objeto separadamente.

3.10.6 Eliminar Objeto

Permite-lhe eliminar objetos do token, tanto chave(s) pública(s) e chave(s) privada(s), como certificado(s). Selecione um objeto e clique em **Eliminar Objeto**. Ser-lhe-á pedido que confirme a eliminação:

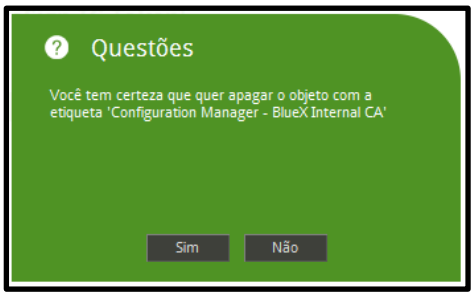

Figura 123: Eliminar Objeto: Tem a certeza

Clique no botão **Sim** se pretender eliminar o objeto.

Ser-lhe-á pedido o PIN do token:

Figura 124: Eliminar Objeto: Insira o PIN

Insira o PIN correto e clique **OK**, e o objeto será eliminado.

Nota

Se já tiver inserido o PIN na caixa de diálogo anterior (e.g. para visualizar objetos privados), não terá que inseri-lo novamente nesta etapa.

3.10.7 Registar Certificado no Windows

Nota

Esta funcionalidade apenas é exibida no sistema operativo Windows.

Permite-lhe registar manualmente no Windows um certificado. Normalmente quando se coloca um cartão na leitora o Windows regista automaticamente os certificados. Mas o serviço do Windows que automatiza este processo poderá estar inativo ou haver alguma limitação. Para estes casos existe a funcionalidade de registar o certificado no Windows.

Para registar um Certificado no Windows deverá aceder aos objetos do token, selecionar o certificado desejado (com chave privada associada), e selecionar a opção **Registar Certificado no Windows**.

Figura 125: Objetos do token : registar certificado no token

Depois de registar o certificado no Windows, uma mensagem de informação é mostrada ao utilizador:

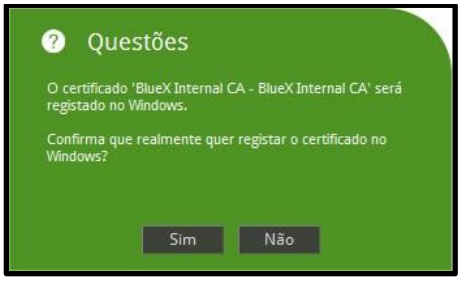

Figure 126: Objetos do token : confirmação do registo de certificado

Ao confirmar o certificado é registado com sucesso (Figura 127), no entanto pode ocorrer um erro se a chave privada não constar no token (Figure 128).

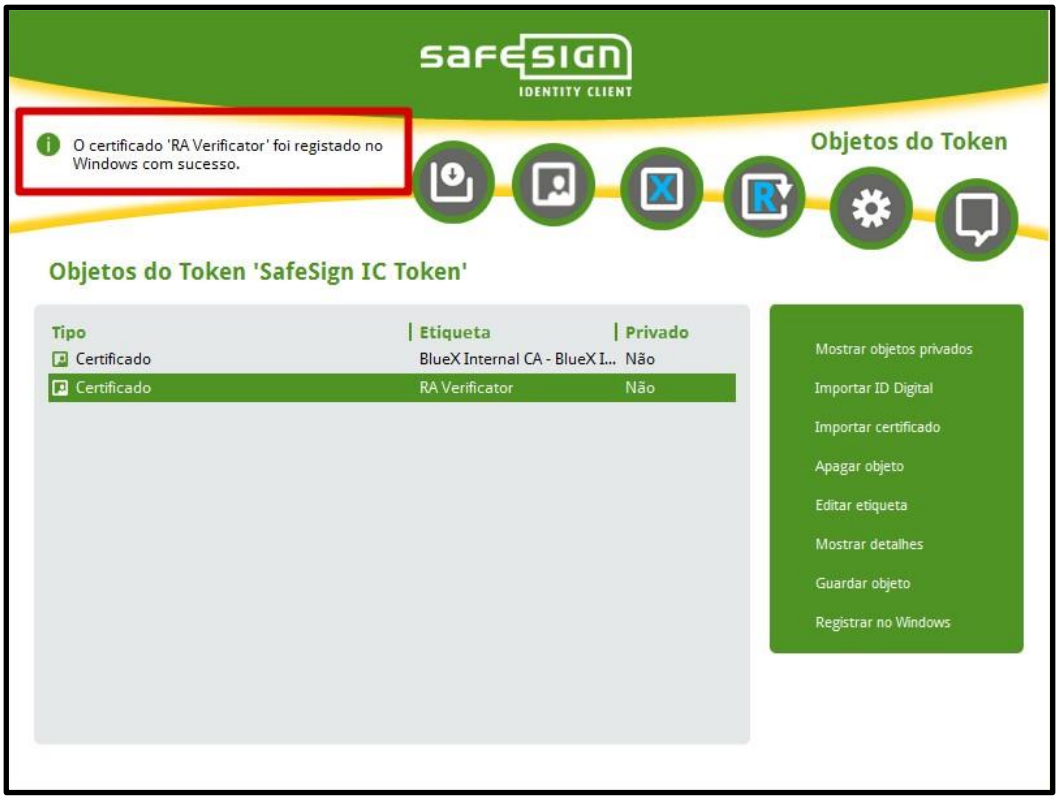

Figura 127: Registar Certificado : Certificado registado com sucesso

Figure 128: Registar Certificado : Chave privada não encontrada no token

3.11 Mostrar Certificados de Atributo do Token

Nota

Esta funcionalidade apenas é exibida no sistema operativo Windows.

Nos sistemas operativos Mac OS X e Linux, se o token contiver certificados de atributo, estes apenas são exibidos na lista de objetos.

A opção **Mostrar Certificados de Atributo do Token** permite listar apenas os certificados de atributo que estão no token, ignorando os outros tipos de objetos (chaves públicas, certificados de identidade, etc.). Para ver os certificados de atributo existentes no token selecione **Mostrar Certificados de Atributo** a partir do menu **Token**, para abrir a lista:

Figura 129: Objetos PKCS#11: Lista Certificados de Atributo

É possível fazer a gestão dos certificados de atributo guardados no token, através da operações descritas nas próximas seções.

3.11.1 Importar Certificado de Atributo

A importação de um Certificado de Atributo é semelhante à importação de um Certificado de Identidade. Assim, para tal basta seguir os passos descritos na seção 3.10.4 (Importar Certificado).

3.11.2 Salvar Certificado de Atributo

Esta operação é similar a salvar um objeto, pelo que devem seguir-se os passos identificados na seção 3.10.2 (Salvar Objeto).

3.11.3 Mostrar Detalhes do Certificado de Atributo

Ao mostrar os detalhes do Certificado de Atributo, é possível verificar todos os atributos e outras informações incorporadas no mesmo, incluindo as extensões (definidas pela EEA que o emitiu).

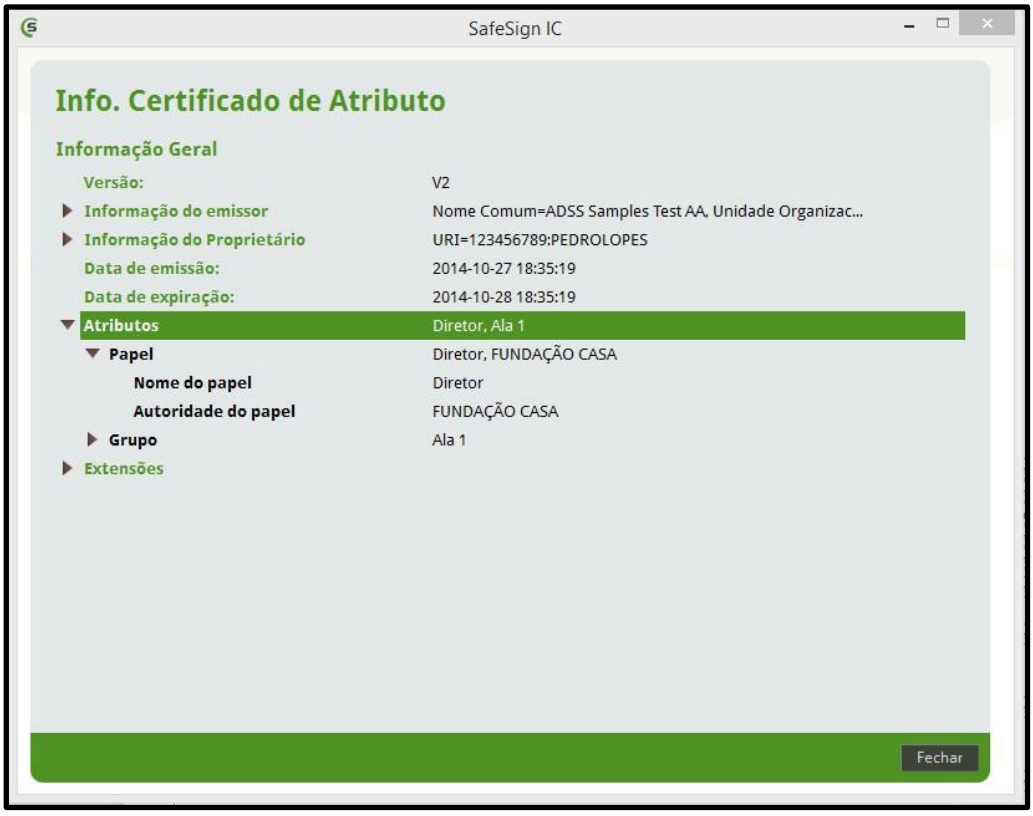

Figura 130: Ver Certificado de Atributo: Informação do Certificado

Nota

Atributos e extensões são definidos livremente pela EEA que emite o certificado de atributo.

Logo, poderão existir atributos e extensões que sejam incluídos num determinado Certificado de Atributo mas que não sejam exibidos nos detalhes, caso o SafeSign IC ainda não esteja preparado para interpretar os mesmos.

3.12 Exportar Conteúdo do Token

Esta função permite ao administrador exportar os conteúdos do token. Os Administradores podem enviar esta informação para o Suporte AET para análise se houver ocorrência de erros que possam estar relacionados com os conteúdos do token.

A exportação dos conteúdos do token identificará os Objetos PKCS#11 no token e os seus atributos.

Nota

Os objetos que estejam no token não serão de modo algum salvos ou colocados fora do cartão. Para exportar os conteúdos do Token, cliquem no menu Token e de seguida cliquem no item Exportar conteúdo do Token.

Ser-lhe-á pedida confirmação para continuar com a exportação:

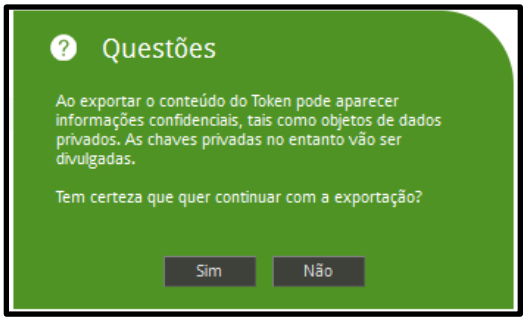

Figura 131: Exportar Conteúdos do Token: Pergunta

Clique **Sim** para continuar com a exportação

Ser-lhe-á pedido que escolha a localização e um nome para o ficheiro resultante:

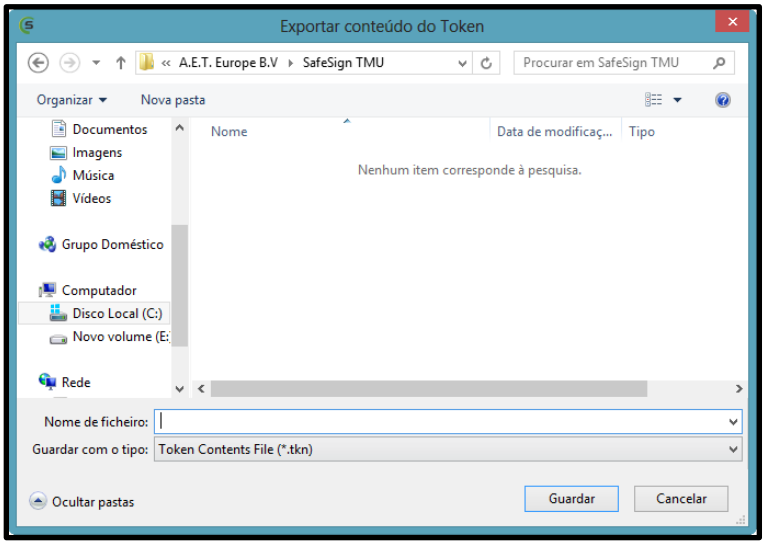

Figura 132: Exportar Conteúdos do Token: Salvar

Escolha a localização e um nome para o ficheiro e clique **Salvar**

Ser-lhe-á pedido que insira o PIN do token:

Figura 133: Exportar Conteúdos do Token: Introduza o PIN

Insira o PIN correto e clique no botão **OK**

Os conteúdos do Token serão escritos num ficheiro na localização especificada:

Figura 134: Exportar Conteúdos do Token: Despejando

Será notificado quando a limpeza tiver sido executada com sucesso:

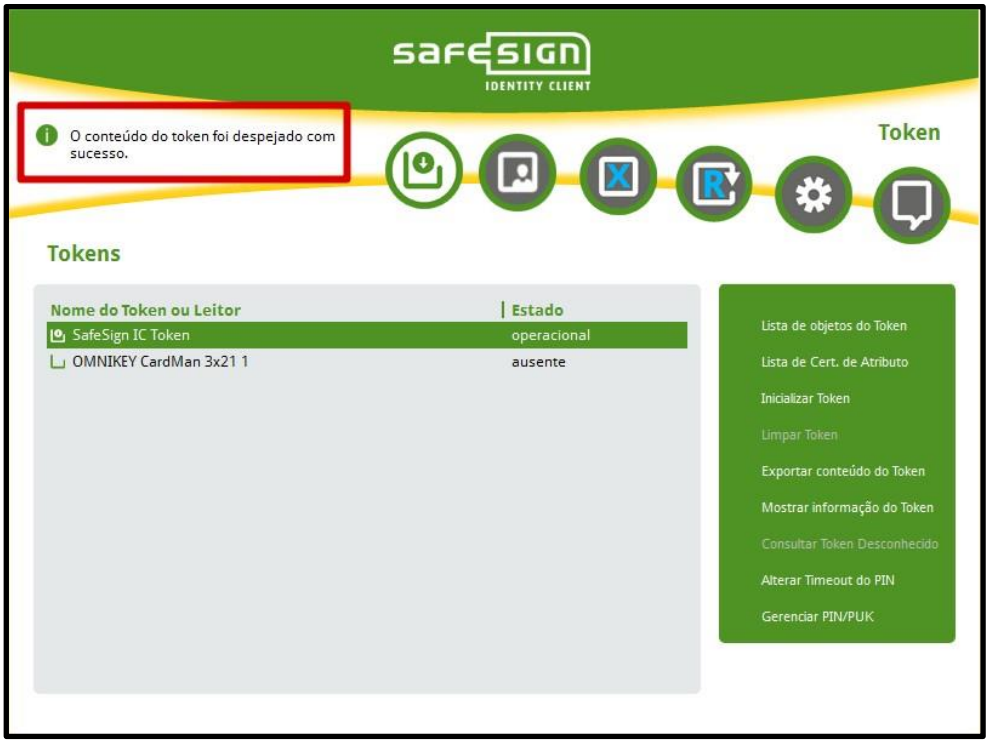

Figura 135: Exportar Conteúdos do Token: Exportado com sucesso

Pode agora visualizar os conteúdos do ficheiro na localização que escolheu.

3.13 Consultar Token desconhecido

Esta função foi inserida no Aplicativo SafeSign IC para ser possível acrescentar versões ainda não reconhecidas de tokens Java.

Se o token aparecer identificado como token desconhecido, isto pode significar[15] que os dados CPLC do token[16] não são conhecidos no SafeSign Identity Client. A função **Consultar Token desconhecido** permite-lhe fazer uma consulta nos dados CPLC do token e criar as entradas necessárias no registry para suportar o token.

Note que os dados CPLC só são utilizados para inicializar um token em branco com um jogo de chaves de teste, de modo a ter as definições corretas para instalar a applet durante a inicialização através do Utilitário de Token. Para tokens de produção que tenham a applet instalada (e um conjunto de chaves customizado), os dados CPLC não são usados.

Note que no caso do seu token não ser reconhecido, é recomendável verificar se existe uma nova versão do SafeSign Identity Client disponível (que possa reconhecer o seu token) e/ou contactar o seu fabricante acerca dos detalhes exatos do token.

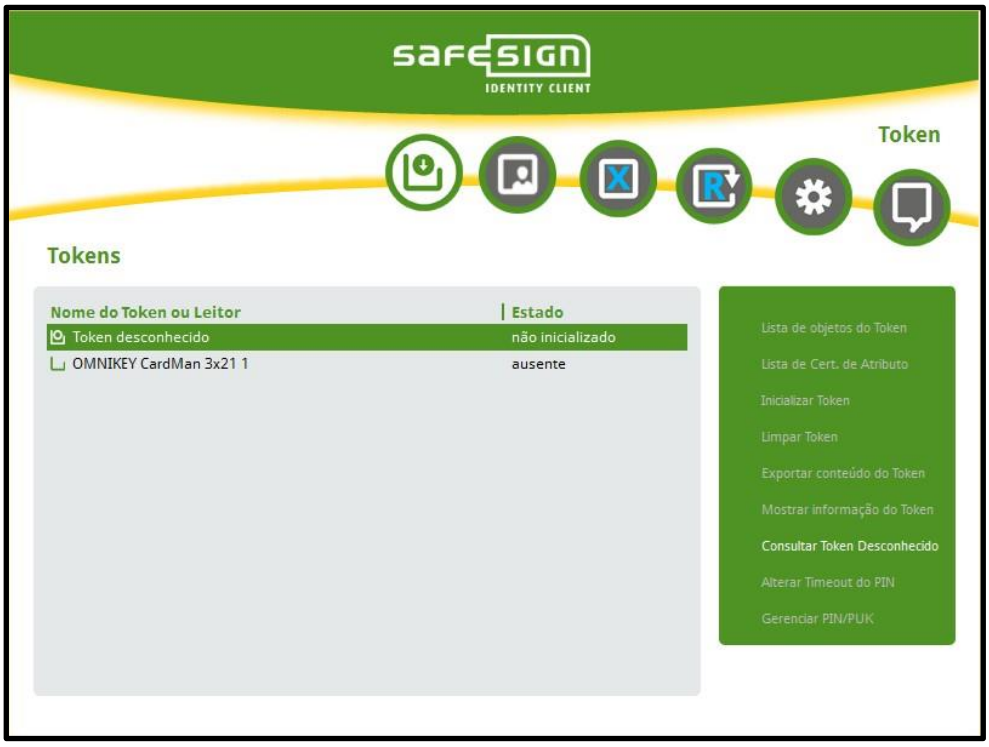

Figura 136: Utilitário de Token: Token Desconhecido

Quando o SafeSign Identity Client (ainda) não reconhece um token, o Aplicativo SafeSign IC mostrará a mensagem "*Token desconhecido – não inicializado*":

Selecione **Token > Consultar Token Desconhecido**

[15] Note que também pode ocorrer que um token em particular possa não ser suportado pelo SafeSign (ver lista de tokens suportados na Descrissão do Produto).

[16] De facto, usamos doze bytes extraídos dos dados CPLC, mas para este documento usaremos a expressão "dados CPLC".

Ao selecionar o item *Consultar Token Desconhecido* do menu **Token**, surge a seguinte caixa de diálogo:

Figura 137: Consultar Token Desconhecido: Java Card Desconhecido

Esta caixa de diálogo identifica a registry key para o Java card inserido.

Poderá copiar as definições do registry de um Java card reconhecido, se o cartão que está a utilizar é uma nova versão (ainda não reconhecida) de um Java card já suportado.

Use a caixa drop-down para selecionar o tipo de Java card correspondente ao seu token. A caixa drop-down não seleciona automaticamente o modelo de token que está a utilizar.

Selecione Copiar definições de registo de um Cartão Java conhecido e selecione o Java card conhecido

Pode agora aplicar as definições do registry ao cartão (ainda) desconhecido, ou pode salvar o ficheiro registry para o adicionar manualmente noutra altura, clicando com duplo clique sobre o mesmo [17].

3.13.1 Aplicar definições

Ao clicar em **Aplicar definições**, ser-lhe-á pedido para inserir o nome do novo cartão:

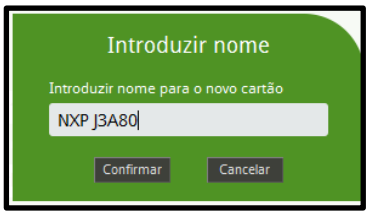

Figura 138: Aplicar definições: Insira o nome

Digite um nome para o novo cartão (ou mantenha o nome do Java card reconhecido) e clique **OK**

Ao clicar **OK**, será informado:

[17] Isto pode ser conveniente se um administrador precisar de atualizar a workstation dos utilizadores finais do SafeSign para suportar a nova versão de um Java card.

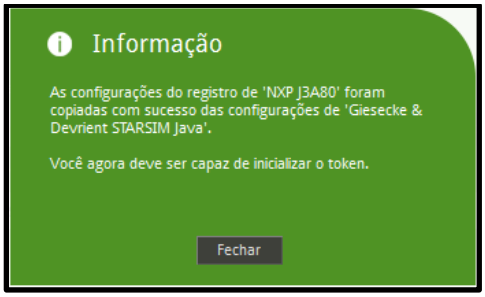

Figura 139: As definições do registo foram copiadas com sucesso

Clique **OK**, e de seguida clique em **Fechar**

O token pode agora ser inicializado, como descrito na seção 3.2:

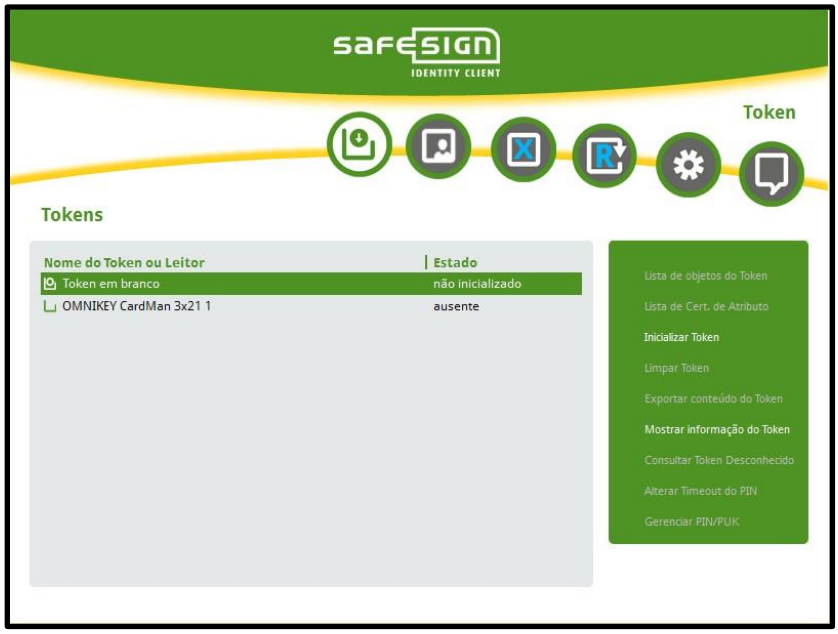

Figura 140: Utilitário de Token: Token em branco

3.13.2 Salvar arquivo de registo

Ao clicar em **Salvar arquivo de registo**, ser-lhe-á pedido para inserir o nome do novo cartão:

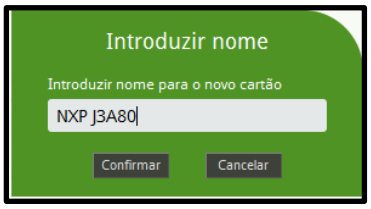

Figura 141: Salvar ficheiro de registo: Insira Nome

Digite um nome para o novo cartão (ou mantenha o nome do Java card reconhecido) e clique **OK.**

Poderá agora salvar o ficheiro de registo na localização desejada:

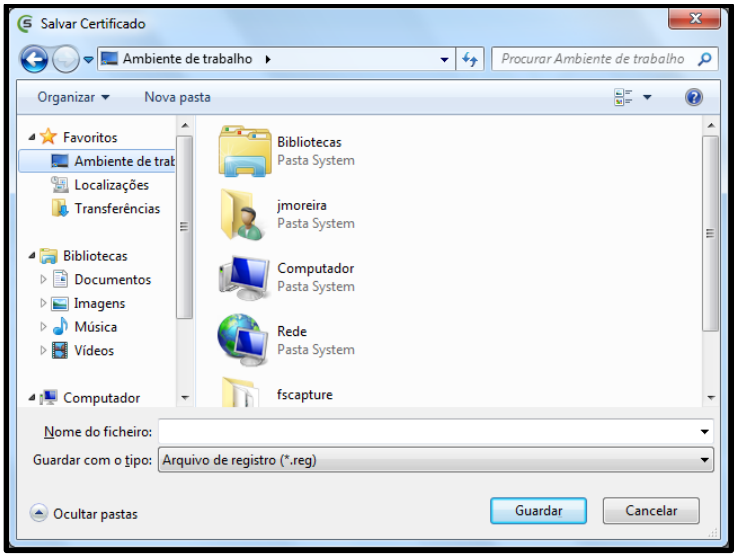

Figura 142: Salvar ficheiro de registo

Clique > **Salvar**

Quando o ficheiro de registo tiver sido salvo, surge uma notificação:

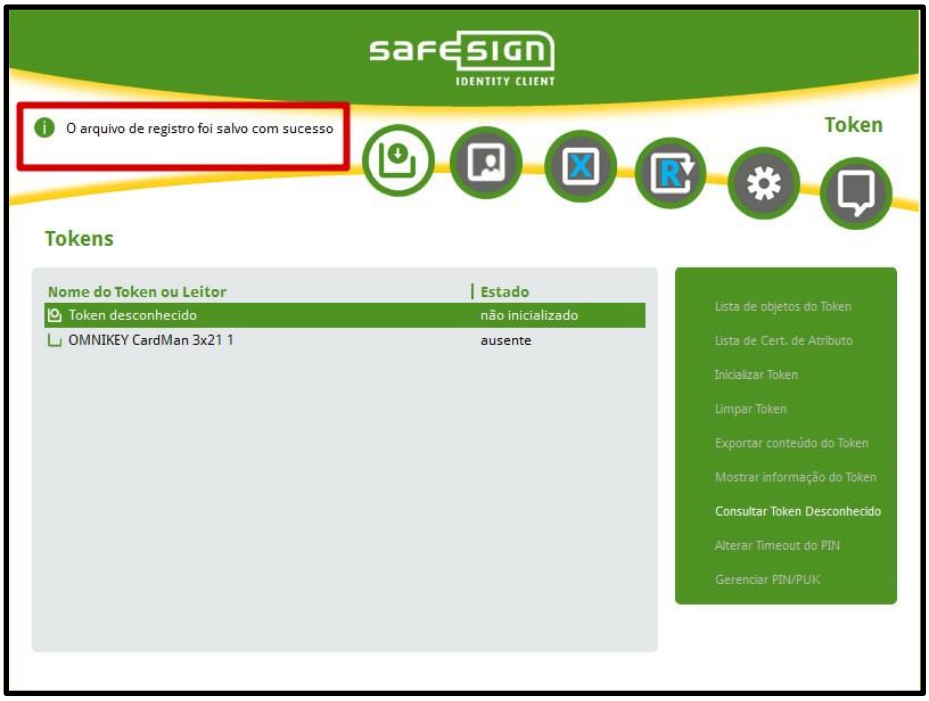

Figura 143: Salvar ficheiro de registo: O ficheiro de registo foi escrito com sucesso

Clique **OK**, e de seguida em **Fechar**

O ficheiro de registo está agora disponível na localização onde o salvou. Com duplo clique sobre o ficheiro, este será guardado no registry e será possível (agora) inicializar o token em branco:

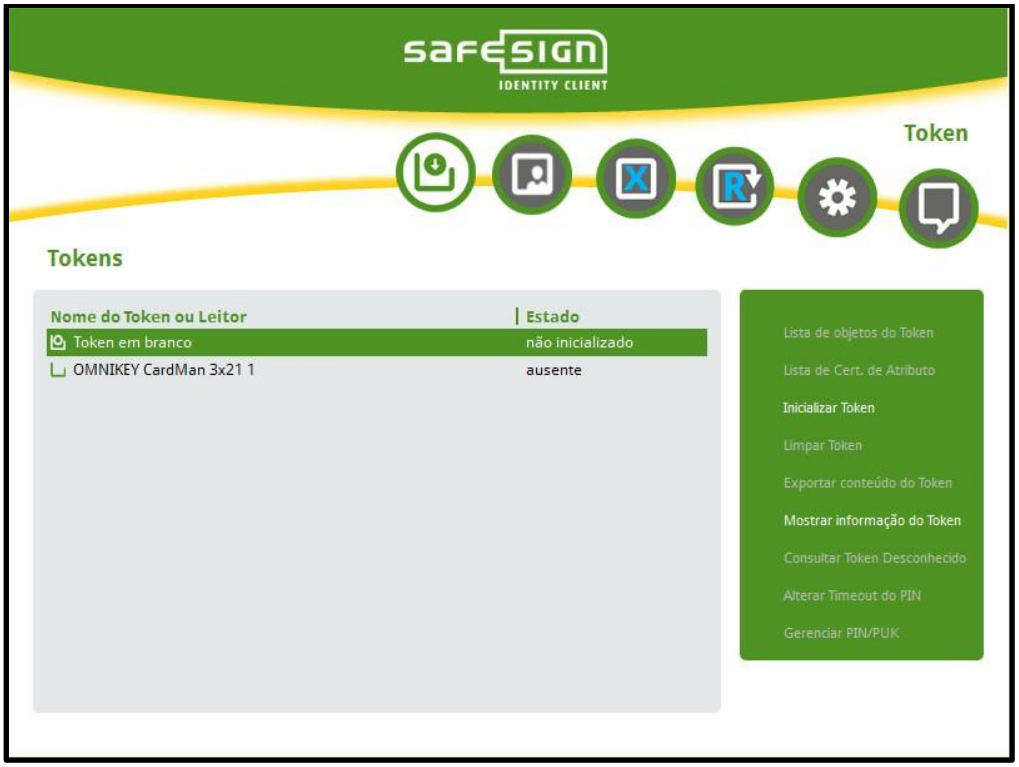

Figura 144: Aplicativo SafeSign IC: Token em branco

3.14 Alterar Timeout do PIN

É possível definir um tempo limite de PIN, mas apenas em cartões com a versão Java Card v2.2 +.

Por padrão, o tempo de espera do PIN está desativado, como na Figura seguinte.

Com a funcionalidade ativa, você será solicitado a colocar novamente o seu PIN após o tempo limite do PIN, ou seja, a janela para introduzir o PIN será exibida. Isto acontecerá para todas as aplicações que utilizem o seu token.

O valor de timeout para o PIN pode ser definido na aplicação através do menu **Token > Alterar timeout do PIN**.

Nota

O valor do timeout do PIN não pode ser definido como 0 (zero) segundos, visto que o PIN iria expirar imediatamente quando ele é inserido. Portanto, o valor mínimo do timeout do PIN é definido como 20 segundos.

A funcionalidade de timeout do PIN não funciona com leitoras PINPAD.

- Selecionar **Alterar timeout do PIN** no menu de **Token**:

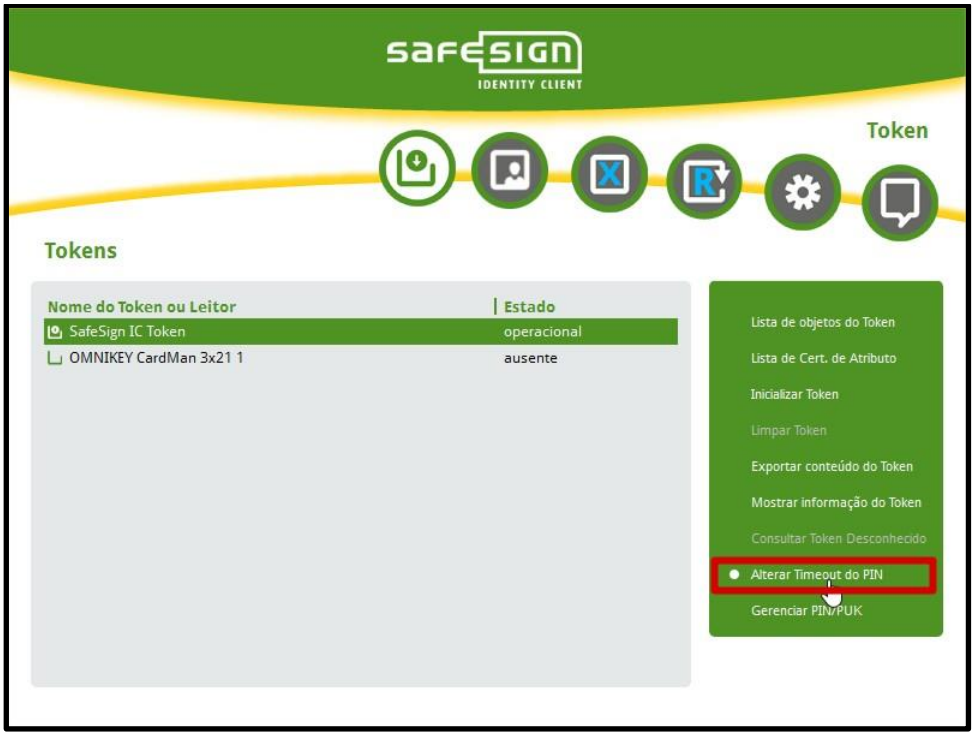

Figura 145: Token : Alterar timeout do PIN

Ao selecionar **Alterar timeout do PIN**, a janela da figura abaixo será mostrada:

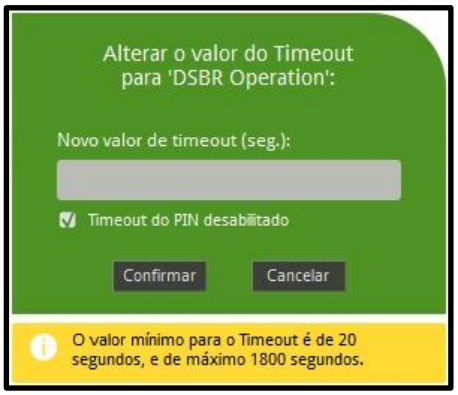

Figura 146: Alterar Timeout : Timeout do PIN desabilitado

Por defeito, o valor de timeout do PIN está desabilitado.

Desmarque a opção **Timeout do PIN desabilitado**, depois você será capaz de definir um novo valor para o timeout do PIN:

Figura 147: Alterar timeout : timeout do PIN ativo

Na caixa de texto introduzir um **valor entre 20 e os 1800** (no exemplo serão 200):

Figura 148: Alterar timeout : novo valor de timeout

- Clicar em **Confirmar**

O timeout do PIN será ativado:

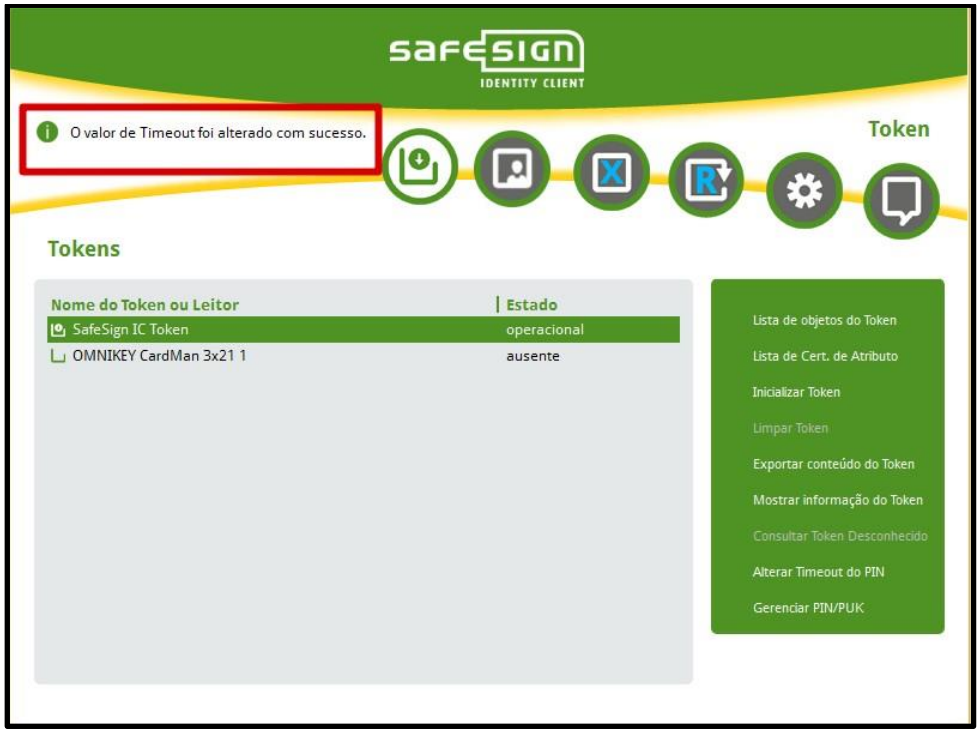

Figura 149: Alterar timeout : O valor do timeout foi alterado com sucesso

Quando o timeout do PIN está ativo, na janela de *Informação do Token* o campo de PIN timeout:

Figura 150: Alterar timeout : Informação do valor do timeout

4 Menu Auto Inscrição

A Auto Inscrição é um processo melhorado de obter[18] um certificado digital de forma mais cómoda. Todo o processo é realizado no computador através do aplicativo SafeSign IC, mediante comunicação com o sistema BlueX[19]. É necessário ter uma conexão à Internet estável para que seja possível comunicar com o BlueX.
O menu de **Auto Inscrição** do aplicativo SafeSign IC tem as seguintes seções:

4.1 Pré-Requisitos

Para iniciar um processo de obtenção de um certificado digital via BlueX serão necessários alguns requisitos:

1. ID e senha para levantar o certificado;
2. Cartão inteligente fornecido pela AR (no caso de levantamento de certificados de identidade do tipo A3 ou de certificados de atributo);
3. Uma leitora (no caso de levantamento de certificados de identidade do tipo A3);
4. Ligação à Internet.

4.2 Levantamento de um certificado de identidade do tipo A3

Um certificado do tipo A3 é obtido da mesma forma que um do tipo A1 mas oferece maior segurança porque o seu par de chaves é gerado, armazenado e utilizado dentro de um cartão inteligente ou token, permanecendo inviolável.

Para iniciar o processo clique no item de Auto Inscrição (ver Figura 151).

[18] O certificado pode ser armazenado em cartão inteligente, ou armazenado na store do Windows se este for o caso. Se for em Unix ou OSX é criado um ficheiro no formato PKCS#12.

[19] O BlueX é uma plataforma flexível de gestão de ARs e de ciclo de vida de IDs digitais especialmente desenvolvida para satisfazer requisitos extremamente variáveis e levar a cabo uma variedade de tarefas de modo competente e seguro.

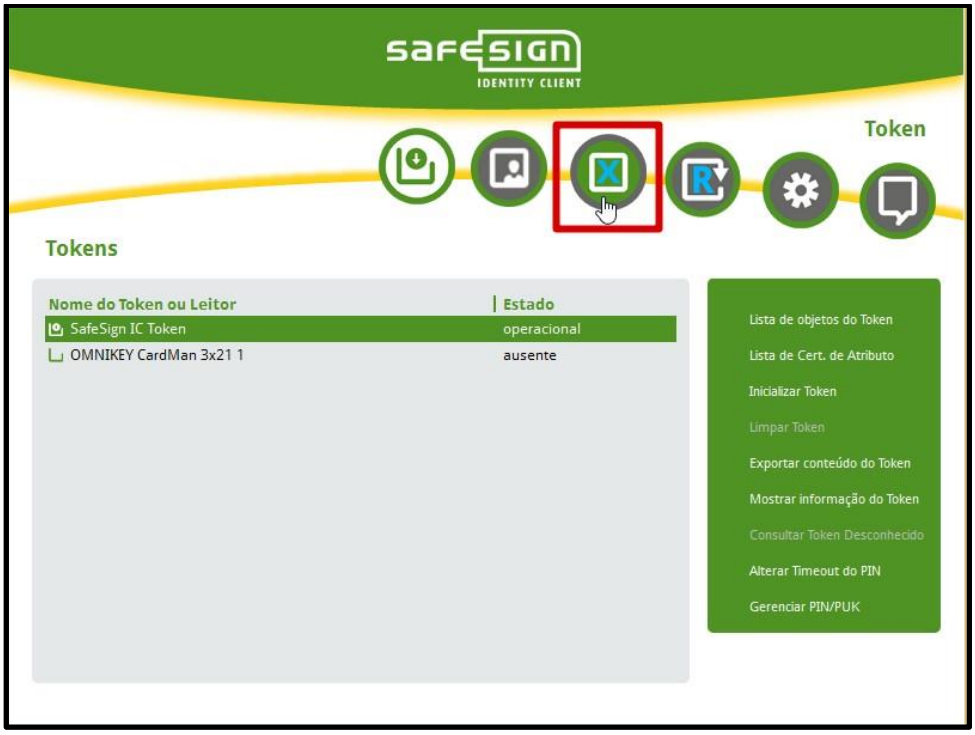

Figura 151: Menu de Auto Inscrição

Quando clicar no botão, será solicitado o ID do pedido como também a senha.

Figura 152: Ecrã de entrada de Auto Inscrição

- Quando os campos estiverem preenchidos clique no botão **Continuar**.
- Clique em **Cancelar** se pretender anular a recolha de certificado.

Depois de clicar em **Confirmar**, uma caixa de espera (Figura 153) será mostrada, indicando que está sendo estabelecida uma conexão à rede e posteriormente ao sistema BlueX.

Figura 153: Aplicativo SafeSign IC: Caixa de espera

Depois de um período de tempo de espera[20] , poderá ocorrer um erro ou serem-lhe mostrados os detalhes do certificado a ser gerado.

Um dos erros que pode acontecer, será o ID do pedido não estar registado, senha incorreta, ou mesmo inexistência de conexão à Internet.

Figura 154: Erros: Pedido não encontrado

Figura 155: Erros : Senha incorreta

Os dados do pedido serão mostrados caso os dados introduzidos estejam corretos. Na Figura 156, podem ver-se os dados de um pedido.

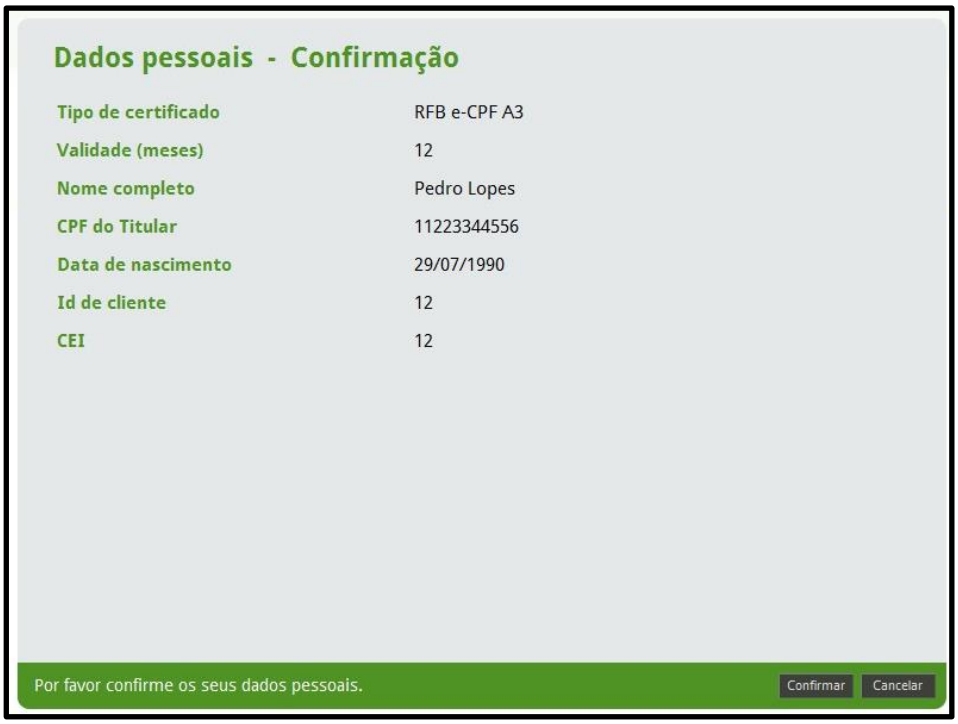

Figura 156: Auto Inscrição: Dados pessoais A3

- Ao clicar em **Confirmar** o processo prosseguirá
- Se clicar em **Cancelar** o processo será cancelado.

[20] Dependente da largura de banda e da quantidade de informação de dados

Depois de clicar em **Confirmar**, irá ser verificado se o pedido foi validado pela AR[21]. Se o pedido ainda não foi validado a seguinte mensagem de erro será apresentada:

Figura 157: Erros : Pedido não validado

Caso o pedido já esteja validado o aplicativo SafeSign IC irá verificar se existe mais que um token conetado ao computador.

Nota

Se tem apenas um token conetado ao computador, a próxima janela não será apresentada.

Caso tenha mais que um token conetado ao computador, tem de selecionar aquele onde pretende que o certificado seja guardado, como indicado na Figura 158.

Figura 158: Auto Inscrição : Selecionar Token

- Depois de selecionar o token clique em **Continuar** e introduza o PIN correto

Nota

Para que este processo possa prosseguir o cartão que recebeu da AR terá que estar registado a um pedido. Caso contrário o seguinte erro é apresentado:

Figura 159 : Erros: Token inválido

[21] Autoridade de Registro

Se o cartão não estiver inicializado, a tela de inicialização é apresentada ao utilizador.

Figura 160: Auto Inscrição : Inicializar token

- Clique em **Confirmar** depois de preencher todos os campos

Para mais detalhes ver seção 3.2.1.

Se o token já estiver inicializado apenas tem que inserir o PIN correto e clicar em **Confirmar**.

Figura 161: Auto Inscrição : Inserir o PIN

Depois de inserir o PIN corretamente o par de chaves é gerado[22] no token (ver Figura 162).

Figura 162: Auto Inscrição : Gerar par de chaves

Quando o processo de gerar o par de chaves estiver conluído com sucesso a seguinte mensagem é apresentada.[23]

[22] Caso um par de chaves já tenha sido foi gerado no cartão inteligente, será reutilizado.

[23] A mensagem apenas será apresentada no Sistema Operativo Windows.

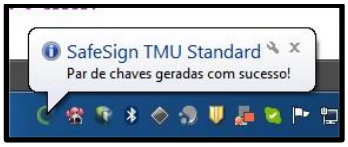

Figura 163: Gerar par de chaves : Mensagem de sucesso

Quando receber o email com a senha de levantamento do certificado, introduza a senha na seguinte tela:

Figura 164: Auto Inscrição : Senha para levantamento do certificado

- Depois de inserir a senha, clique em **Confirmar**
- Se pretender cancelar o processo e continuar mais tarde, clique em **Cancelar**

Ao confirmar, uma mensagem de espera será apresentada Figura 165.

Figura 165: Auto Inscrição : Mensagem de espera

Se a senha de levantamento não estiver correta (ver Figura 166) o processo termina.

Figura 166: Erro : Senha de personalização incorreta

Se a operação de levantamento do certificado foi bem-sucedida, é apresentada uma mensagem de sucesso na tela.

4.3 Levantamento de um certificado de identidade do tipo A1

O certificado digital do tipo A1 é emitido e armazenado em ficheiro num computador com sistema operacional Windows, Mac OS X e Linux. O levantamento de um certificado do tipo A1 difere de acordo com o sistema operativo.

O Windows detém um local (*certificate store*) próprio para armazenar os certificados e chaves. Em Mac OS X e Linux não existe esse conceito, pelo menos de forma suportada oficialmente pelo sistema operacional. Desse modo, nas seções seguintes são descritas as duas formas de levantamento de certificados de identidade do tipo A1, consoante o sistema operacional em causa.

4.3.1 Windows

Para iniciar o processo clique no item de Auto Inscrição (ver Figura 180).

Figura 167: Menu de Auto Inscrição

Quando clicar no botão, será pedido o ID do pedido como também a senha.

Figura 168: Ecrã de entrada de Auto Inscrição

- Quando os campos estiverem preenchidos clique no botão **Continuar**.
- Clique em **Cancelar** se pretender anular a recolha de certificado.

Depois de clicar em **Confirmar**, uma caixa de espera (Figura 182) será mostrada ao utilizador, indicando que está sendo estabelecida uma conexão à rede e posteriormente ao sistema BlueX.

Figura 169 : Aplicativo SafeSign IC: Caixa de espera

Depois de um período de tempo de espera[24], poderá ocorrer um erro ou serem-lhe mostrados os detalhes do pedido.

Um dos erros que pode acontecer, será o ID do pedido não estar registado, senha incorreta, ou mesmo inexistência de conexão à Internet.

Figura 170: Erros: Pedido não encontrado

Figura 171: Erros : Senha incorreta

Os dados do pedido serão mostrados caso os dados introduzidos estejam corretos. Na imagem seguinte, podem ver-se os dados de um pedido.

[24] Dependente da largura de banda e da quantidade de informação de dados

Figura 172: Auto Inscrição : Dados Pessoais A1

- Ao clicar em **Confirmar** o processo proseguirá
- Se clicar em **Cancelar** o processo começa do ínicio.

Depois de clicar em **Confirmar**, irá ser verificado se o pedido foi validado pela AR. Se o pedido ainda não foi validado a seguinte mensagem de erro será apresentada:

Figura 173: Erros : Pedido não validado

Quando receber o e-mail com a senha de levantamento do certificado, copie a senha para introduzir na seguinte tela:

Figura 174: Auto Inscrição : Senha para levantamento do certificado

- Depois de inserir a senha, clique em **Confirmar**
- Se pretender cancelar o processo e continuar mais tarde, clique em **Cancelar**

Ao confirmar, uma mensagem de espera será apresentada, similar à a Figura 188.

Figura 175: Auto Inscrição : Mensagem de espera

Se a senha de levantamento não estiver correta (ver a imagem seguinte) o processo termina.

Figura 176: Erro : Senha de personalização incorreta

Se a operação de levantamento do certificado foi bem sucedida, é apresentada uma mensagem de sucesso na tela, como se pode ver na imagem seguinte.

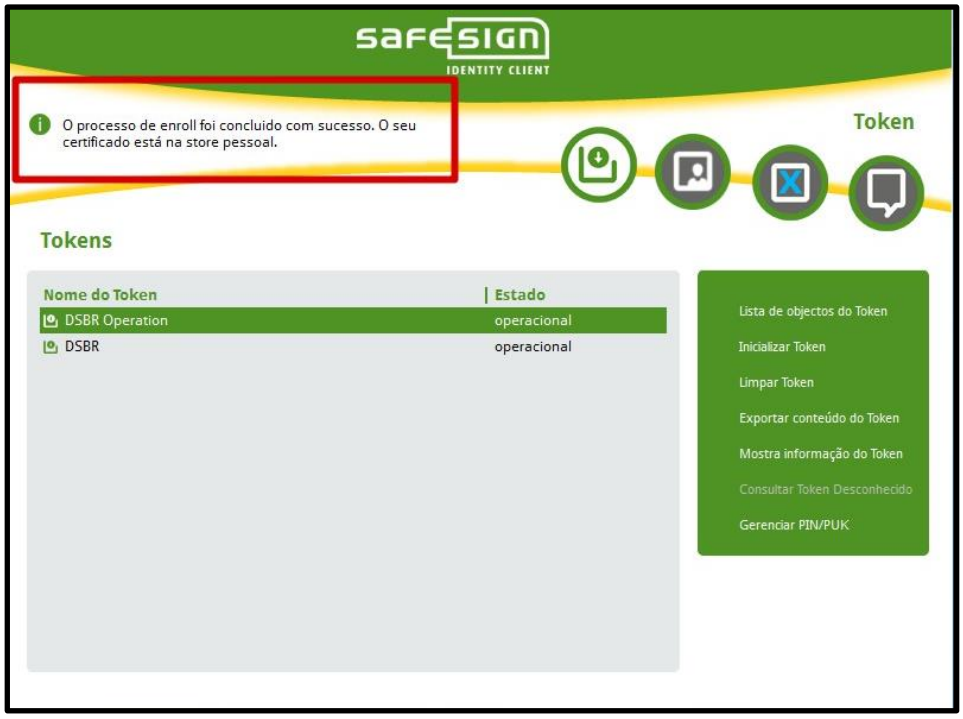

Figura 177: Auto Inscrição : Certificado levantado com sucesso - A1

O processo de levantamento do certificado foi realizado com sucesso, no entanto o usuário tem a opção de salvar o certificado em um arquivo .p12.

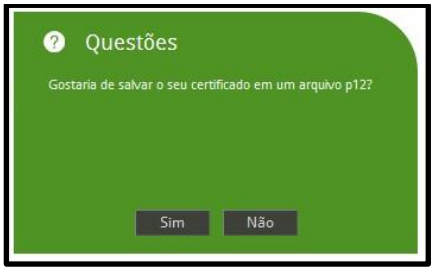

Figura 178: Auto Inscrição : Opção de salvar em arquivo

- Se pretender salvar o certificado em arquivo, clique em **Sim**
- Se não desejar salvar o arquivo, clique em **Não**

Ao clicar em **Sim**, é apresentada uma tela para definir a localização onde salvar o arquivo, como também a senha para proteger o arquivo.

Figura 179: Auto Inscrição : Selecionar a pasta de destino e a senha do arquivo

Nota

A senha que é solicitada é da escolha do usuário, não estando mencionada em nenhum lugar.

A senha do arquivo deve ter um mínimo de 4 carateres e um máximo de 8.

Ao **Confirmar**, o arquivo é armazenado no local que o usuário escolheu. A senha poderá ser necessária posteriormente, conserve-a num local seguro.

4.3.2 Mac OS X e Linux

Para iniciar o processo clique no item de Auto Inscrição (ver Figura 180).

Figura 180: Menu de Auto Inscrição

Quando clicar no botão, será pedido o ID do pedido como também a senha.

Figura 181: Ecrã de entrada de Auto Inscrição

- Quando os campos estiverem preenchidos clique no botão **Continuar**.
- Clique em **Cancelar** se pretender anular a recolha de certificado.

Depois de clicar em **Confirmar**, uma caixa de espera (Figura 181) será mostrada ao utilizador, indicando que está sendo estabelecida uma conexão à rede e posteriormente ao sistema BlueX.

Figura 182 : Aplicativo SafeSign IC: Caixa de espera

Depois de um período de tempo de espera[25], poderá ocorrer um erro ou serem-lhe mostrados os detalhes do pedido.

Um dos erros que pode acontecer, será o ID do pedido não estar registado, senha incorreta, ou mesmo inexistência de conexão à Internet.

Figura 183: Erros: Pedido não encontrado

Figura 184: Erros : Senha incorreta

Os dados do pedido serão mostrados caso os dados introduzidos estejam corretos. Na imagem seguinte, podem ver-se os dados de um pedido.

Figura 185: Auto Inscrição : Dados Pessoais A1

[25] Dependente da largura de banda e da quantidade de informação de dados

- Ao clicar em **Confirmar** o processo prosseguirá
- Se clicar em **Cancelar** o processo começa do início.

Depois de clicar em **Confirmar**, irá ser verificado se o pedido foi validado pela AR. Se o pedido ainda não foi validado a seguinte mensagem de erro será apresentada:

Figura 186: Erros : Pedido não validado

Se o pedido tiver sido validado e verificado pela AR, o processo irá seguir para a seguinte fase.

Quando receber o e-mail com a senha de levantamento do certificado, copie a senha para introduzir na seguinte tela:

Figura 187: Auto Inscrição : Senha para levantamento do certificado

- Depois de inserir a senha, clique em **Confirmar**
- Se pretender cancelar o processo e continuar mais tarde, clique em **Cancelar**

Ao confirmar, uma mensagem de espera será apresentada, similar à Figura 188.

Figura 188: Auto Inscrição : Mensagem de espera

Se a senha de levantamento não estiver correta (ver a imagem seguinte) o processo termina.

Figura 189: Erro : Senha de personalização incorreta

Se a operação de levantamento do certificado foi bem sucedida, é apresentada uma tela para definir a localização onde salvar o arquivo, como também a senha para proteger o arquivo.p12.

Nota

A senha que é solicitada é da escolha do usuário, não estando mencionada em nenhum lugar.

Figura 190: Janela de introdução da senha do arquivo .p12

- Depois de inserir a senha, clique em **Confirmar**
- Se clicar em **Cancelar,** o certificado não é levantado.

Nota

A senha que é solicitada é da escolha do usuário, não estando mencionada em nenhum lugar.

A senha do arquivo deve ter um mínimo de 4 carateres e um máximo de 8.

Ao **Confirmar**, o arquivo é armazenado no local que o usuário escolheu. A senha poderá ser necessária posteriormente, conserve-a num local seguro.
Depois de confirmar a senha, é apresentada uma mensagem de sucesso na tela como pode ver na imagem seguinte.

Figura 191: Auto Inscrição : Certificado levantado com sucesso - A1

5 Menu Renovação

A Renovação é o processo no qual um usuário pode renovar o seu certificado digital de forma mais cómoda. Todo o processo é realizado no computador através do aplicativo SafeSign IC, mediante comunicação com o sistema BlueX[26]. É necessário ter uma conexão à Internet estável para que seja possível comunicar com o BlueX.
Este processo é semelhante com o processo de Auto Inscrição, no entanto tem ligeiras diferenças.

O menu de **Renovação** do aplicativo SafeSign IC tem as seguintes seções:

5.1 Pré-Requisitos

Para iniciar um processo de renovação de um certificado digital via BlueX serão necessários alguns requisitos:

1. ID e senha para renovar o certificado;
2. Cartão inteligente ou token fornecido pela AR (no caso de renovação de certificados de identidade do tipo A3 ou de certificados de atributo);
3. Uma leitora (no caso de renovação de certificados de identidade do tipo A3 em cartão inteligente);
4. Ligação à Internet.

5.2 Renovação de um certificado de identidade do tipo A3

A renovação de um certificado do tipo A3 é semelhante a um do tipo A1, no entanto oferece maior segurança porque o seu par de chaves é gerado, armazenado e utilizado dentro de um cartão inteligente ou token, permanecendo inviolável.

Para iniciar o processo clique no item de Renovação (ver Figura 192).

[26] O BlueX é uma plataforma flexível de gestão de ARs e de ciclo de vida de IDs digitais especialmente desenvolvida para satisfazer requisitos extremamente variáveis e levar a cabo uma variedade de tarefas de modo competente e seguro.

Figura 192: Menu de Renovação

Quando clicar no botão, será solicitado o ID do pedido como também a senha.

Figura 193: Ecrã de entrada de Renovação

- Quando os campos estiverem preenchidos clique no botão **Continuar**.
- Clique em **Cancelar** se pretender anular a recolha de certificado.

Depois de clicar em **Confirmar**, uma caixa de espera (Figura 194) será mostrada, indicando que está sendo estabelecida uma conexão à rede e posteriormente ao sistema BlueX.

Figura 194: Aplicativo SafeSign IC: Caixa de espera

Depois de um período de tempo de espera[27] , poderá ocorrer um erro ou serem-lhe mostrados os detalhes do certificado a ser gerado.

Um dos erros que pode acontecer, será o ID do pedido não estar registado, senha incorreta, ou mesmo inexistência de conexão à Internet.

Figura 195: Erros: Pedido não encontrado

Figura 196: Erros : Senha incorreta

É necessário escolher a leitora que contém o certificado de identidade a ser renovado.

Nota

Se tem apenas um token conetado ao computador, a próxima janela não será apresentada.

Caso tenha mais que uma leitora conetada no computador, terá que selecionar aquele onde tem armazenado o certificado a renovar, como indicado na Figura 197.

Figura 197: Renovação : Selecionar token

- Depois de selecionar a leitora clique em **Continuar** e introduza o PIN correto
- Se clicar em **Cancelar** o processo termina

Depois de introduzir o PIN corretamente, terá que escolher o certificado de identidade (com par de chaves associado) a renovar. É apresentada uma listagem de certificados que estão armazenados na leitora previamente selecionada (Ver Figura 198).

[27] Dependente da largura de banda e da quantidade de informação de dados

Figura 198: Selecionar o certificado a renovar

- Depois de selecionar a ID Digital clique em **Confirmar** para prosseguir o processo
- Se clicar em **Cancelar** o processo termina

O processo de renovação permite que a senha de gerenciamento seja alterada, no qual o usuário tem obrigatoriamente definir uma senha [28](Ver Figura 199).

Figura 199: Alteração da senha de gerenciamento

Depois de **Confirmar** e definir a senha (Ver Figura 200), o termo de renovação com os dados que o usuário terá que assinar é apresentado, como na Figura 201.

[28] A senha de gerenciamento terá que ter pelo menos 6 carateres.

Figura 200: Definir a senha de levantamento

Figura 201: Renovação A3 : Termo de Renovação

- Se concordar com os dados apresentados, clique em **Assinar**
- Se clicar em **Cancelar** o processo termina

Nota

Para que este processo possa prosseguir, o certificado de identidade selecionado previamente, terá que estar registado para renovação no sistema BlueX da sua AC:

Figura 202 : Erros: Certificado de identidade errado

Os dados da assinatura são enviados para que sejam validados. Se estes estiverem corretos, o processo de levantamento do novo certificado é automaticamente iniciado. Se todo o processo de levantamento ocorrer com sucesso o novo certificado em conjunto com o par de chaves, como também os certificados de AC, estarão no cartão inteligente ou token selecionado.

5.3 Renovação de um certificado de identidade do tipo A1

O certificado digital do tipo A1 é emitido e armazenado em ficheiro num computador com sistema operacional Windows, Mac OS X e Linux. A renovação de um certificado do tipo A1 difere de acordo com o sistema operativo.

O Windows detém um local próprio (*certificate store*) para armazenar os certificados e chaves. Em Mac OS X e Linux não existe esse conceito, pelo menos de forma suportada oficialmente pelo sistema operacional. Desse modo, nas seções seguintes são descritas as duas formas de renovação de certificados de identidade do tipo A1, consoante o sistema operacional em causa.

Para iniciar o processo clique no item de Renovação (ver Figura 192).

Quando clicar no botão, será solicitado o ID do pedido como também a senha (Ver Figura 203).

Figura 203: Ecrã de entrada de Renovação

- Quando os campos estiverem preenchidos clique no botão **Confirmar**.
- Clique em **Cancelar** se pretender anular a renovação do certificado.

Depois de clicar em **Confirmar**, uma caixa de espera (Figura 204) será mostrada, indicando que está sendo estabelecida uma conexão à rede e posteriormente ao sistema BlueX.

Figura 204: Aplicativo SafeSign IC: Caixa de espera

Depois de um período de tempo de espera[29] , poderá ocorrer um erro ou serem-lhe mostrados os detalhes do certificado a ser gerado.

Um dos erros que pode acontecer, será o ID do pedido não estar registado, senha incorreta, ou mesmo inexistência de conexão à Internet.

[29] Dependente da largura de banda e da quantidade de informação de dados

Figura 205: Erros: Pedido não encontrado

Figura 206: Erros : Senha incorreta

Os passos seguintes do processo têm diferenças dependentes do sistema operacional. Para ver em mais detalhe os próximos passos em Windows, ir para a Seção 5.3.1. Se estiver a utilizar Mac OsX ou Linux ver em mais detalhe na Seção 5.3.2.

5.3.1 Windows

Depois de inserir o ID do pedido e a senha corretamente, é pedido que escolha um certificado digital (armazenado na Personal Store) para que este seja renovado (Ver Figura 207).

Figura 207: Renovação A1 : Selecionar ID Digital

- Depois de selecionar um ID Digital, clique no botão **Confirmar**.
- Clique em **Cancelar** se pretender anular a renovação do certificado.

O processo de renovação permite que a senha de gerenciamento seja alterada, no qual o usuário tem que obrigatoriamente colocar uma senha [30](Ver Figura 208).

[30] A senha de gerenciamento terá que ter pelo menos 6 carateres.

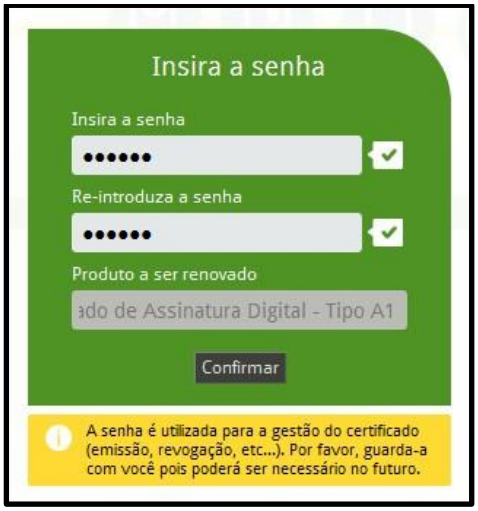

Figura 208: Alteração da senha de gerenciamento

Depois de **Confirmar** e definir a senha (Ver Figura 209), o termo de renovação com os dados que o usuário terá que assinar é apresentado como na Figura 210.

Figura 209: Definir a senha de levantamento

Figura 210: Renovação A3 : Termo de Renovação

- Se concordar com os dados apresentados, clique em **Assinar**
- Se clicar em **Cancelar** o processo termina

Depois do termo ser assinado e validado pela AR com sucesso, o processo de levantamento da ID Digital é concluído, salvando na Personal Store a ID Digital. No entanto, o usuário tem a opção de salvar o seu certificado em um arquivo .p12.

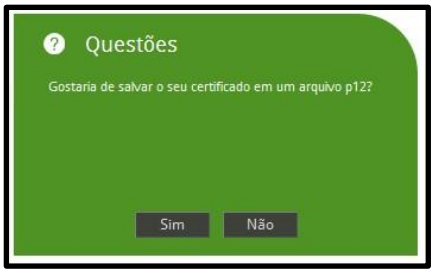

Figura 211: Auto Inscrição : Opção de salvar em arquivo

- Se pretender salvar o certificado em arquivo, clique em **Sim**
- Se não desejar salvar o arquivo, clique em **Não**

Ao clicar em **Sim**, é apresentada uma tela para definir a localização onde salvar o arquivo, como também a senha para proteger o arquivo.

Figura 212: Auto Inscrição : Selecionar a pasta de destino e a senha do arquivo

Ao **Confirmar**, o arquivo é armazenado no local que o usuário escolheu. A senha poderá ser necessária posteriormente, conserve-a num local seguro.

5.3.2 Mac OS X e Linux

O processo de renovação é diferente nos sistemas operativos Mac OSX e Linux pois é utilizado como meio de armazenamento dos certificados de identidade do tipo A1 um arquivo com extensão .p12.

Depois de inserir o ID do pedido e a senha corretamente, é pedido que localize (no sistema de ficheiros) o certificado digital a ser renovado em formato de arquivo .p12, como também a sua senha.

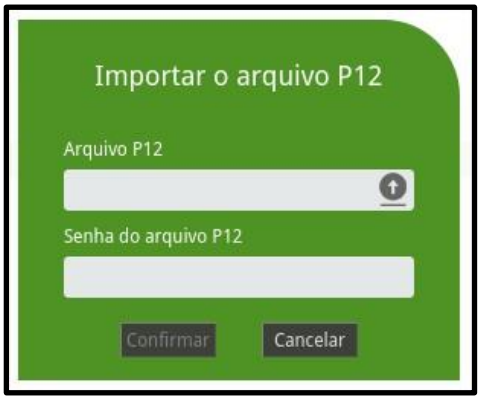

Figura 213: Renovação A1 : Importação do arquivo .p12

O processo de renovação permite que a senha de gerenciamento seja alterada, no qual, o usuário tem que obrigatoriamente colocar uma senha [31](Ver Figura 214).

Figura 214: Alteração da senha de gerenciamento

Depois de **Confirmar** e definir a senha (Ver Figura 209), o termo de renovação com os dados que o usuário terá que assinar é apresentado como na Figura 216.

[31] A senha de gerenciamento terá que ter pelo menos 6 carateres.

Figura 215: Definir a senha de levantamento

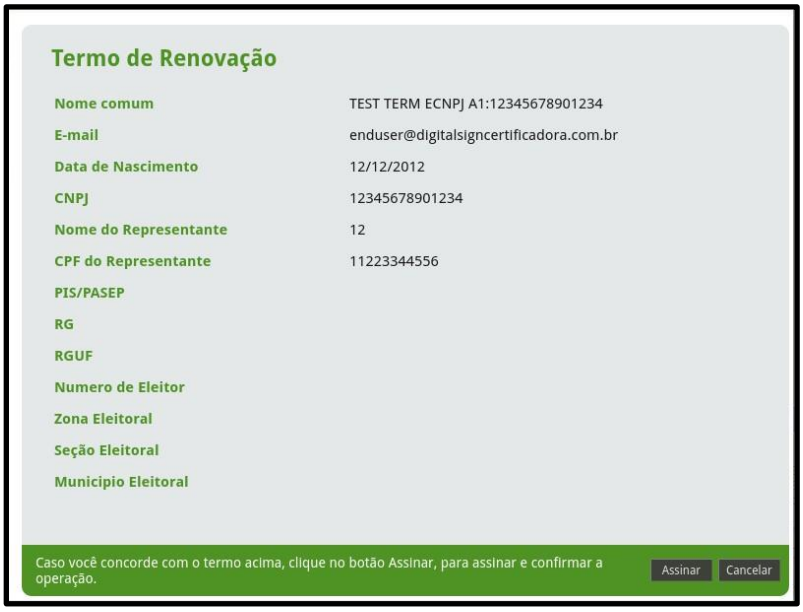

Figura 216: Renovação A3 : Termo de Renovação

- Se concordar com os dados apresentados, clique em **Assinar**
- Se clicar em **Cancelar** o processo termina

Depois do termo ser assinado e validado pela AR com sucesso, é apresentada uma tela para definir a localização onde salvar o arquivo, como também a senha para proteger o arquivo.

Figura 217: Selecionar o local de destino do arquivo .p12

- Depois de escolher a pasta de destino clique em **Confirmar**
- Se clicar em **Cancelar** o processo termina e a ID Digital não é renovada

Ao **Confirmar**, o arquivo é armazenado no local que o usuário escolheu. A senha poderá ser necessária posteriormente, conserve-a num local seguro. Posteriormente é apresentada uma mensagem de sucesso na tela (Ver Figura 191).