




GUIA DE DESBLOQUEIO DO CERTIFICADO DIGITAL

Antes de iniciar o procedimento, temos alguns lembretes para você.

O PIN é a senha de acesso do certificado digital e a PUK é a senha de desbloqueio. Ambas são de uso pessoal e intransferível e cadastradas por você durante a emissão do Certificado Digital. Ressaltamos que, antes do bloqueio dessas senhas, é possível realizar três tentativas de acesso para senhas PIN e PUK.

Para evitar esse contratempo, entregamos um guia de “instalação e recomendações”, que contém campo para preencher a data de validade do certificado e anotar as senhas de gerenciamento/revogação, PIN e PUK.

**AASP**

**CERTIFICADO
DIGITAL**

Guia de instalação

Para utilizar o seu certificado digital, é necessário instalar os arquivos referentes à mídia adquirida (token ou cartão + leitora). O manual e os arquivos de instalação estão disponíveis no site da AASP (www.aasp.org.br), no item Suporte Profissional/Certificação Digital/Suporte e Download. Em caso de dúvidas, acesse o site da AASP e clique no item Certificação Digital/Perguntas Frequentes.

Recomendações

- Não molhe, não dobre nem exponha seu cartão/token a agentes químicos corrosivos. Armazene suas senhas de forma segura.
- A senha de gerenciamento/revogação é utilizada para cancelar o certificado digital em caso de perda, roubo ou extravio do cartão/token e é criada pelo usuário no momento da emissão do certificado digital.
- O PIN (Personal Information Number) é um código composto de números, de letras ou da combinação de ambos, sendo proibidos caracteres especiais (como @#%*) com mínimo de quatro e máximo de oito caracteres, e será utilizado no dia a dia (acesso ao site da Receita Federal, assinatura de documentos, e-mails, etc.). Se houver três tentativas incorretas de digitação da senha PIN, ela será bloqueada.
- A PUK (PIN Unlock Key) segue as mesmas regras do PIN, porém será utilizada somente quando o PIN estiver bloqueado. Caso a PUK seja esquecida e o cartão esteja bloqueado, deve-se revogar o certificado digital (pela internet, caso o titular se lembre da senha de gerenciamento/revogação, ou pessoalmente, na AR) e solicitar um novo, repetindo o processo, inclusive o pagamento das taxas.

Certificado válido até

Pessoa física Pessoa jurídica

Anote suas senhas e guarde-as em local seguro.

Senha de gerenciamento/revogação:

PIN (4 a 8 caracteres):

PUK (4 a 8 caracteres):

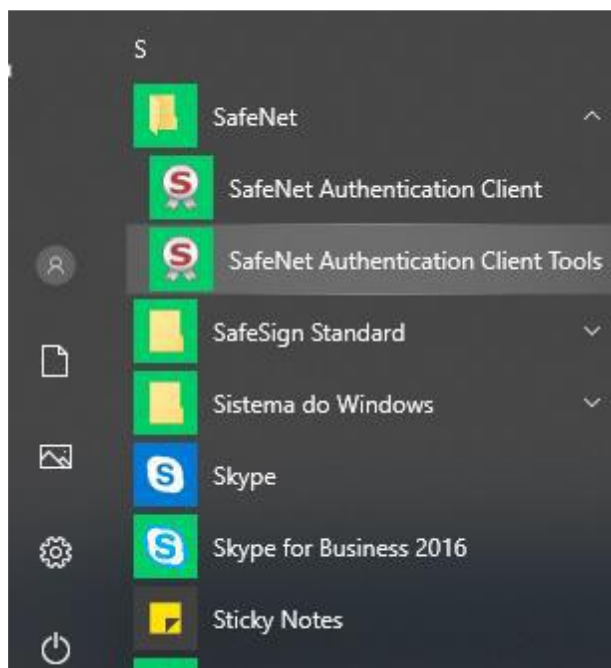
* Horário de atendimento - Posto AR AASP
Dias úteis, das 8h30 às 16h30 - Sábados, das 8h30 às 11h30
Capital e região metropolitana de São Paulo: (11) 3291 9200, das 7h30 às 19h
Outras localidades: 0600 777 5656, das 7h30 às 19h

www.aasp.org.brF.CERT.DIG.06.03

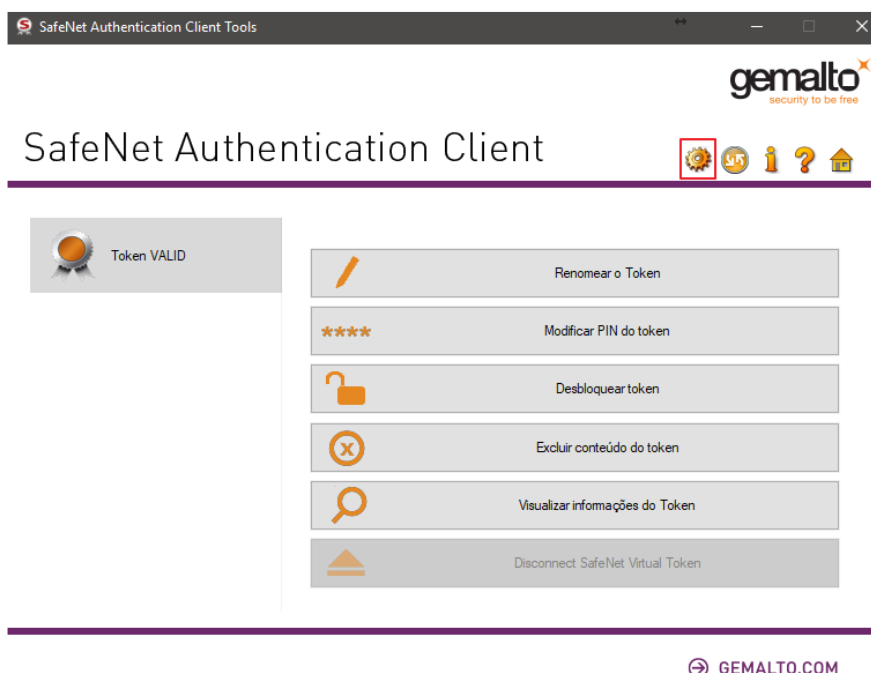
Para recuperar o acesso ao seu certificado digital, é preciso utilizar a senha PUK. Sem ela, não é possível desbloquear a senha PIN.

DESBLOQUEIO DO CERTIFICADO DIGITAL - SAFENET

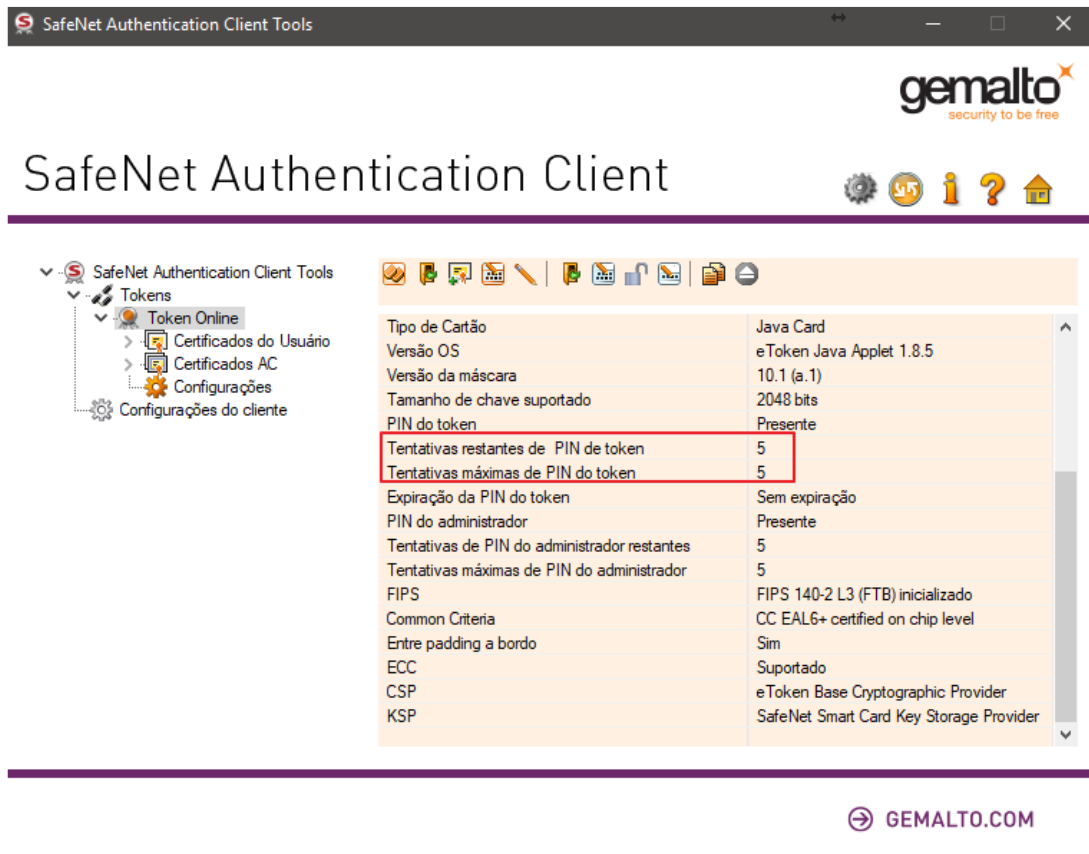
Após instalado, o gerenciador fica localizado em “Todos os aplicativos” do Windows. Localize e clique na pasta “SafeNet”, na sequência abra o aplicativo clicando na opção “SafeNet Authentication Client Tools”:



Ao selecionar a opção, o gerenciador de token está apto à utilização. No caso das mídias SAFENET, a digitação errada da senha PIN (5 vezes) ocasiona em bloqueio da mídia, necessitando digitar a senha PUK para desbloqueio. Ao abrir o Safenet, deve selecionar a opção “Vista avançada”:



Caso a senha esteja de fato bloqueada, será exibido ao cliente o número de tentativas restantes de “Senha do token” (Senha PIN), tal como o número restante para as tentativas de desbloqueio através da “Senha do administrador” (Senha PUK):



The screenshot shows the 'SafeNet Authentication Client Tools' window. The left sidebar is expanded to 'Tokens' > 'Token Online' > 'Configurações'. The main area displays a table of token configuration parameters. A red box highlights the 'Tentativas restantes de PIN de token' and 'Tentativas máximas de PIN de token' fields, both showing the value '5'.

Tipo de Cartão	Java Card
Versão OS	eToken Java Applet 1.8.5
Versão da máscara	10.1 (a.1)
Tamanho de chave suportado	2048 bits
PIN do token	Presente
Tentativas restantes de PIN de token	5
Tentativas máximas de PIN de token	5
Expiração da PIN do token	Sem expiração
PIN do administrador	Presente
Tentativas de PIN do administrador restantes	5
Tentativas máximas de PIN do administrador	5
FIPS	FIPS 140-2 L3 (FTB) inicializado
Common Criteria	CC EAL6+ certified on chip level
Entre padding a bordo	Sim
ECC	Suportado
CSP	eToken Base Cryptographic Provider
KSP	SafeNet Smart Card Key Storage Provider

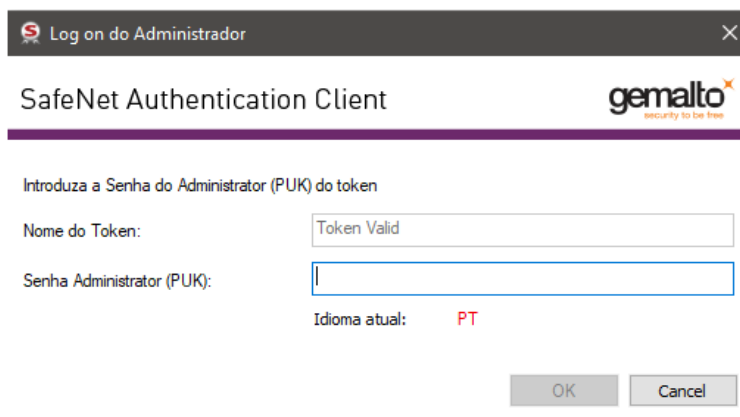
Para realizar o desbloqueio, o usuário deve selecionar a opção “Configurar a Senha do token”:



The screenshot shows the same 'SafeNet Authentication Client Tools' window. The left sidebar is expanded to 'Tokens' > 'Token Online' > 'Configurar a Senha do token'. The main area displays a table of token configuration parameters. A red box highlights the 'Configurar a Senha do token' icon in the top toolbar.

Nome do Token	Token Online
Categoria do Token	Hardware
Nome do leitor	AKS ifdh 0
Número de série	0x0281c1a7
Espaço livre no cartão de token (minimum estimated)	32767
Versão do Hardware	15.0
Versão do Firmware	15.0
ID do cartão	0281C1A7
Nome do produto	SafeNet eToken 5110 FIPS
Tipo de Cartão	Java Card
Versão OS	eToken Java Applet 1.8.5
Versão da máscara	10.1 (a.1)
Tamanho de chave suportado	2048 bits
PIN do token	Presente
Tentativas restantes de PIN de token	5
Tentativas máximas de PIN de token	5
Expiração da PIN do token	Sem expiração
PIN do administrador	Presente

Será solicitado ao usuário a introdução da Senha do administrador (PUK):



Log on do Administrador

SafeNet Authentication Client **gemalto**
security to be free

Introduza a Senha do Administrator (PUK) do token

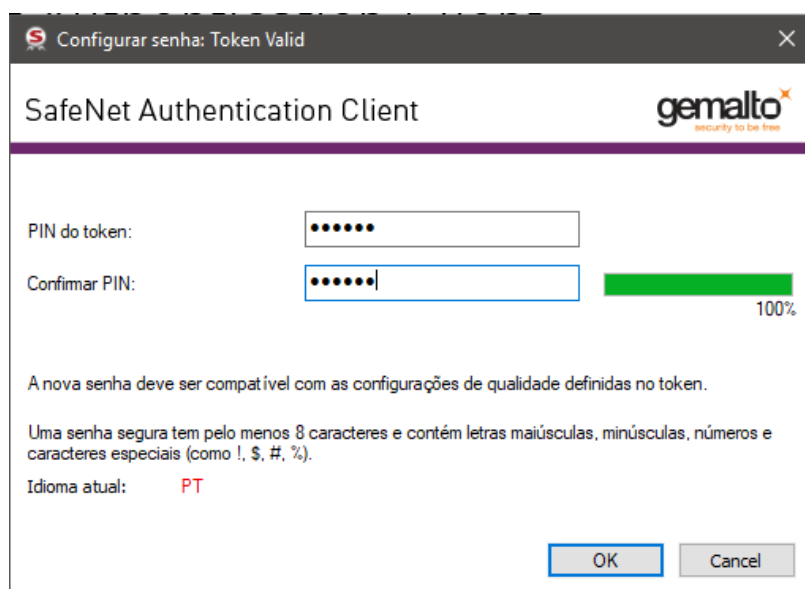
Nome do Token: Token Valid

Senha Administrator (PUK):

Idioma atual: PT

OK Cancel

Após inserir a senha e confirmar no botão “OK”, será solicitado ao usuário que digite e confirme a sua nova senha de utilização (Senha PIN):



Configurar senha: Token Valid

SafeNet Authentication Client **gemalto**
security to be free

PIN do token: ●●●●●●

Confirmar PIN: ●●●●●●

100%

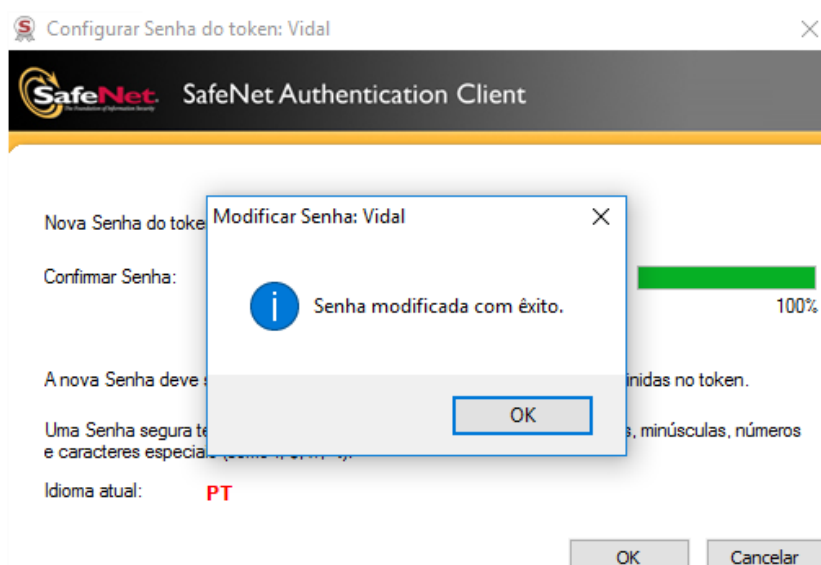
A nova senha deve ser compatível com as configurações de qualidade definidas no token.

Uma senha segura tem pelo menos 8 caracteres e contém letras maiúsculas, minúsculas, números e caracteres especiais (como !, \$, #, %).

Idioma atual: PT

OK Cancel

A confirmação da alteração da senha é exibida ao usuário:



Configurar Senha do token: Vidal

SafeNet SafeNet Authentication Client

Nova Senha do token: ●●●●●●

Confirmar Senha: ●●●●●●

100%

A nova Senha deve ser compatível com as configurações de qualidade definidas no token.

Uma Senha segura tem pelo menos 8 caracteres e contém letras maiúsculas, minúsculas, números e caracteres especiais (como !, \$, #, %).

Idioma atual: PT

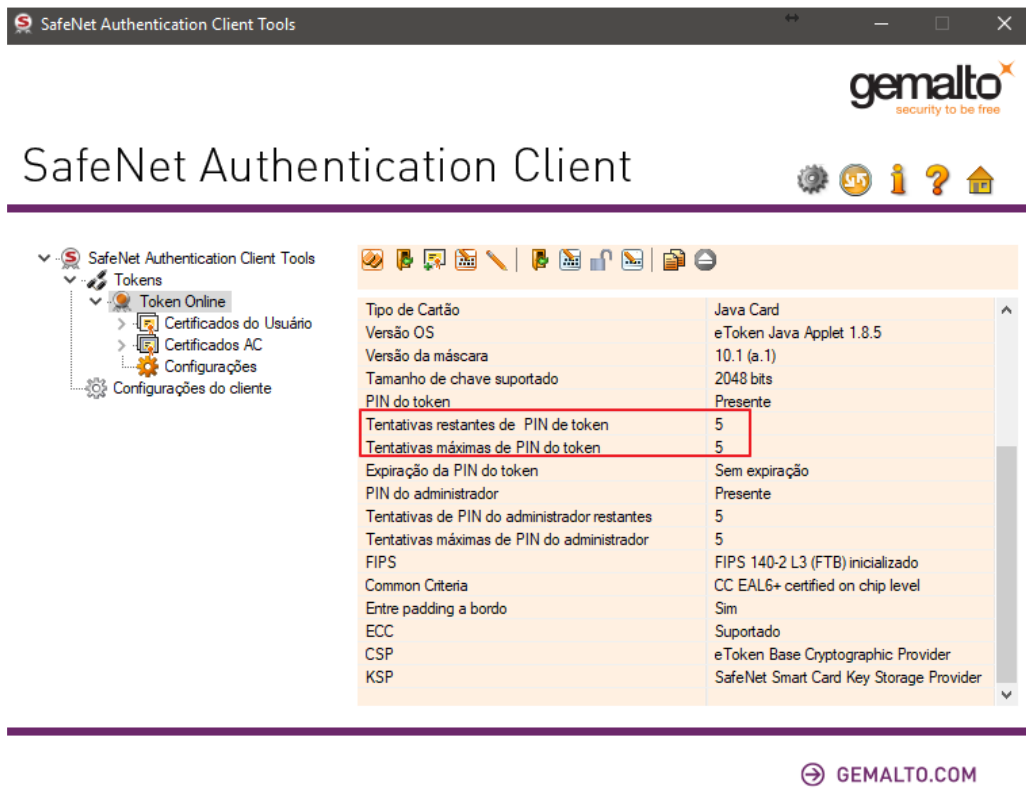
OK Cancel

Modificar Senha: Vidal

Senha modificada com êxito.

OK

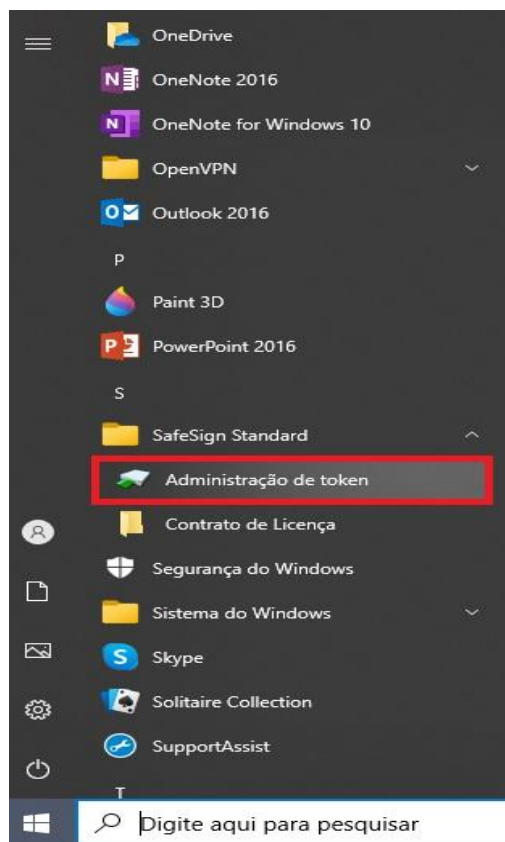
Podemos notar que após o desbloqueio, as tentativas restantes para utilização da senha PIN voltam ao padrão (5 tentativas):



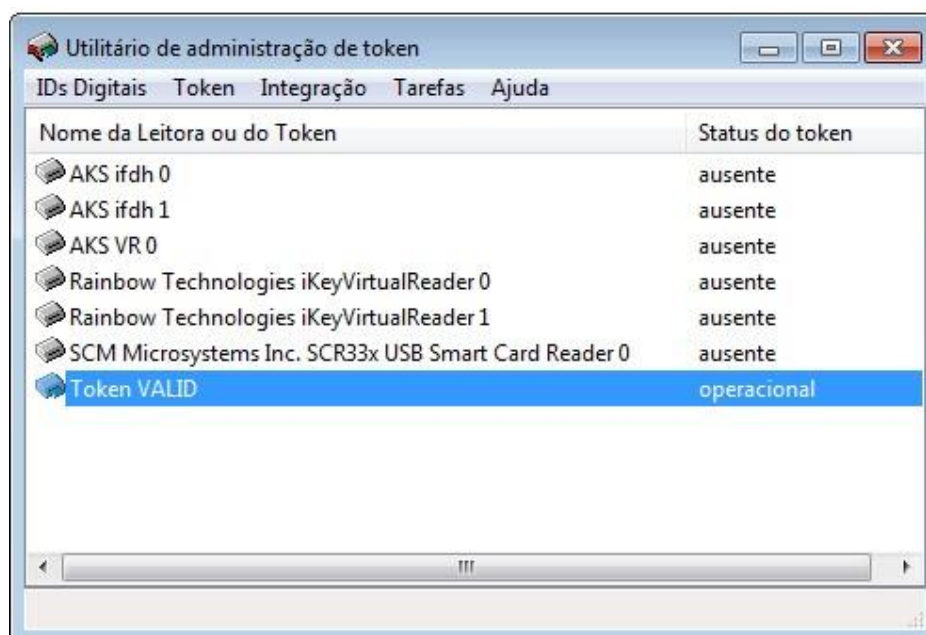
The screenshot displays the 'SafeNet Authentication Client Tools' application window. The title bar reads 'SafeNet Authentication Client Tools'. The Gemalto logo is in the top right corner with the tagline 'security to be free'. The main title is 'SafeNet Authentication Client'. Below the title is a navigation pane on the left with a tree view containing 'Tokens', 'Token Online', 'Certificados do Usuário', 'Certificados AC', 'Configurações', and 'Configurações do cliente'. The main area shows a configuration table for a 'Java Card' token. The table has two columns: the configuration parameter and its value. The values for 'Tentativas restantes de PIN de token' and 'Tentativas máximas de PIN de token' are both 5, and these two rows are highlighted with a red border. At the bottom right, there is a 'GEMALTO.COM' logo.

Tipo de Cartão	Java Card
Versão OS	eToken Java Applet 1.8.5
Versão da máscara	10.1 (a.1)
Tamanho de chave suportado	2048 bits
PIN do token	Presente
Tentativas restantes de PIN de token	5
Tentativas máximas de PIN de token	5
Expiração da PIN do token	Sem expiração
PIN do administrador	Presente
Tentativas de PIN do administrador restantes	5
Tentativas máximas de PIN do administrador	5
FIPS	FIPS 140-2 L3 (FTB) inicializado
Common Criteria	CC EAL6+ certified on chip level
Entre padding a bordo	Sim
ECC	Suportado
CSP	eToken Base Cryptographic Provider
KSP	SafeNet Smart Card Key Storage Provider

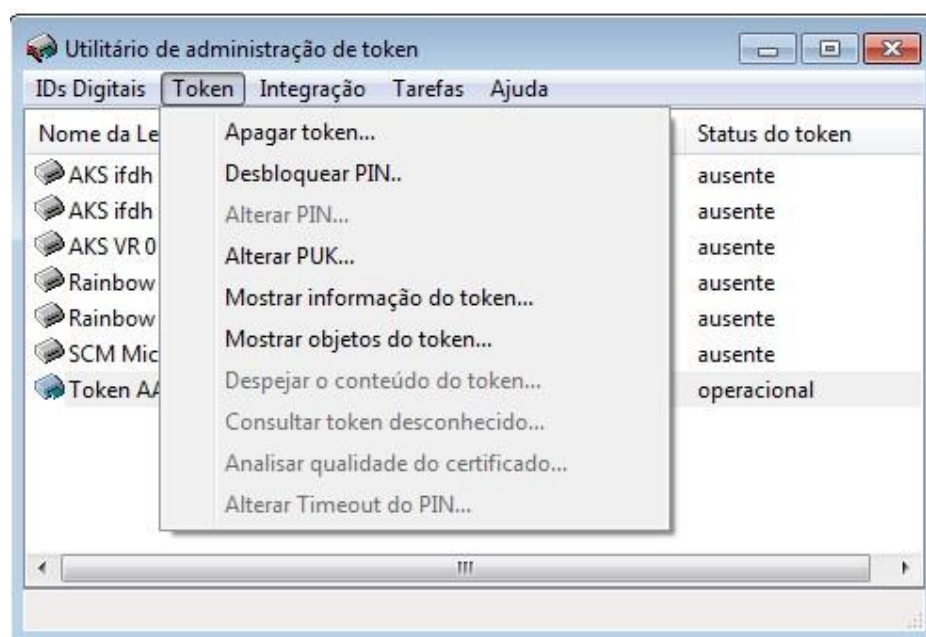
DESBLOQUEIO DO CERTIFICADO DIGITAL - UTILITÁRIO DE ADMINISTRAÇÃO DE TOKEN



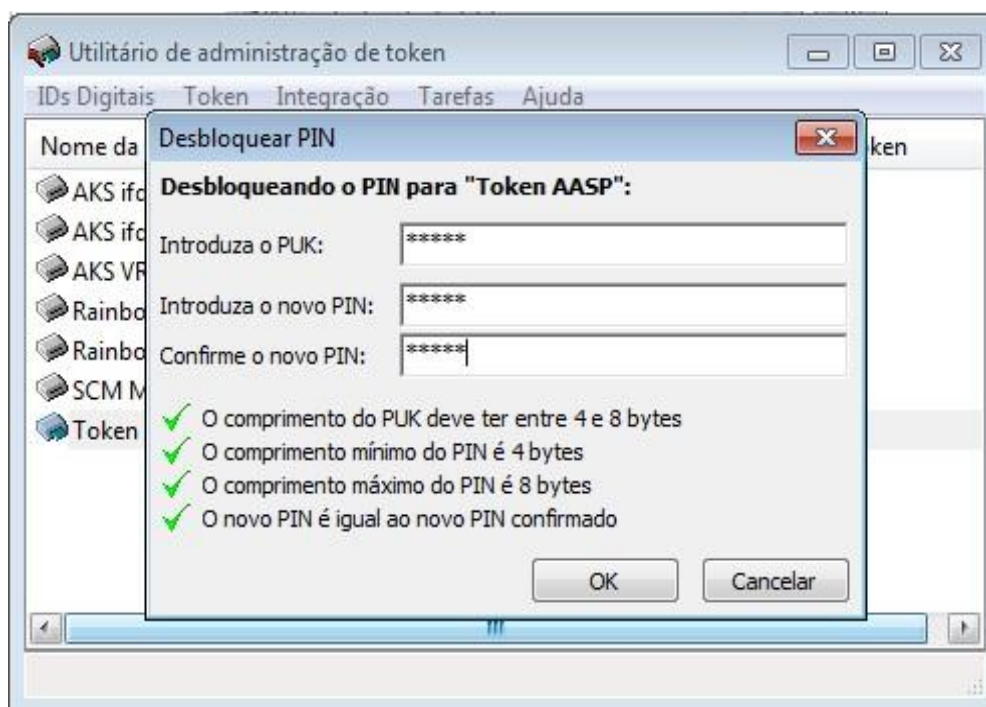
Comece abrindo o programa **Utilitário de Administração de Token**, que foi instalado junto com o seu certificado digital, verifique se o **“Token VALID”** tem o status **“operacional”**.



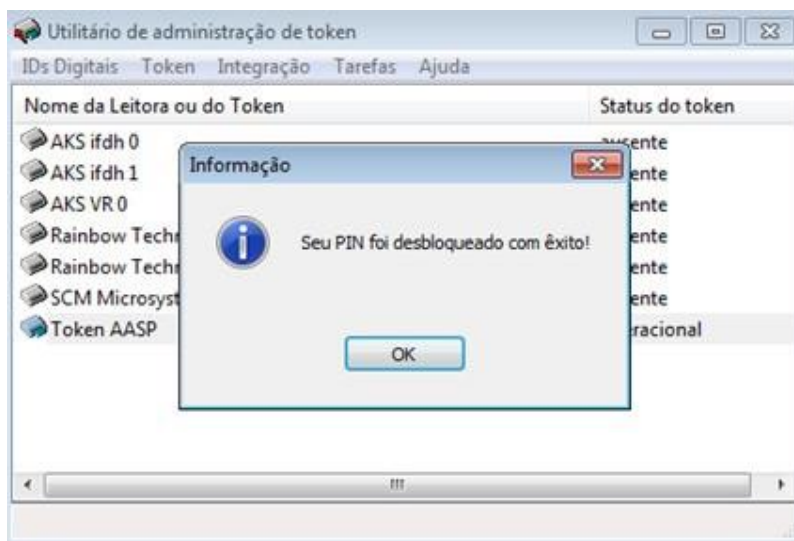
Em seguida, no campo “Token”, clique em “Desbloquear PIN”.



Digite sua senha PUK e, em seguida, sua nova senha PIN, confirme o novo PIN e clique em “OK”.



Aguarde a informação “**Seu PIN foi desbloqueado com êxito!**” e clique em “**OK**”.



Por fim, verifique a confirmação do desbloqueio e se o “estado” se encontra com o status “**Operacional**”.

