PRONOVA

SOLUÇÕES
INTELIGENTES

MANUAL DE INSTRUÇÕES

PROTOKEN PRO

Versão 1.1

Pronova Consultoria em Tecnologia da Informação Ltda.

Todos os produtos da Pronova Soluções Inteligentes (PRONOVA) incluindo, sem limitar-se a, cópias de avaliação, disquetes, CD-ROMs, hardware, software e documentação, e todos os futuros pedidos, estão sujeitos aos termos desta Licença. Se você não está de acordo com os termos aqui expostos, por favor, proceda a devolução do pacote completo e dentro do prazo de quinze dias úteis e reembolsaremos o custo do produto, exceto o frete e os encargos administrativos. Ao utilizar o produto você declara conhecer e aceitar os termos e condições do presente, que se formalizará em um contrato de Licença entre você e a PRONOVA, que também terá alcance às revendas ou aos representantes da PRONOVA, com o alcance aqui convencionado.

1. **Uso Permitido** – Você pode fundir, relacionar e/ou fazer link do Software com outros programas com o único propósito de proteger esses programas de acordo com o uso descrito no Guia do Desenvolvedor que está junto com o produto, ou que pode ser encontrado no site web da PRONOVA (www.pronova.com.br). Você pode realizar cópias do Software com o fim de utilizá-las como cópias de segurança ou backup.

2. **Uso proibido** – O Software ou o hardware fornecido pela PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desassemblada, descompilada, revisada, melhorada e modificada de qualquer forma, exceto como especificamente se permite no presente. Você não pode praticar engenharia reversa ao Software ou qualquer parte do produto, ou tentar descobrir o código fonte do Software. Você não pode usar o meio ótico ou magnético incluído com o produto com o propósito de transferir ou guardar dados que não fazem parte original de Produto, ou uma melhora ou atualização de Produto fornecida pela PRONOVA.

3. **Garantia** – A PRONOVA garante que os Produtos e os meios de armazenamento de Software são substancialmente livres de defeitos de fabricação ou materiais. Esta garantia terá validez por um período de tempo de doze (12) meses desde a entrega de produto por parte da PRONOVA.

4. **Fim da garantia** – No caso de que ocorra qualquer fato que produza o fim da garantia, a única obrigação por parte da PRONOVA é efetuar ou reparar a descrição da PRONOVA, qualquer produto sem que isto possa gerar algum encargo para você.

Para tanto, a PRONOVA (distribuidor oficial) ou revendas autorizadas, não serão responsáveis em nenhum caso por nenhum dano, prejuízo, gasto, ou conceito sobre a garantia expressamente reconhecida no presente. Em conseqüência a responsabilidade total faz de você ou qualquer terceiro por qualquer causa, tanto contratual como extracontratual, incluindo dolo, culpa ou negligência, não excederá, em nenhum caso, do preço que você pagou pelo Produto que tenha causado um dano, ou que tenha sido objeto de, ou indiretamente relacionado com, a causa do dano.

Em nenhum caso a PRONOVA será responsável por nenhum dano causado por culpa ou negligência sua ou de terceiros, nem por nenhuma perda de dados, ganhos ou economias, ou por outros danos casuais ou casualidades, mesmo se a PRONOVA tiver avisado da possibilidade de ocorrência ao dano. Qualquer produto que você entregará à PRONOVA com a finalidade de troca em cumprimento desta garantia, passará a ser propriedade da PRONOVA.

5. **Limitação da Garantia** – A presente garantia não cobre e nem cobrirá defeitos provocados por uso inadequado ou conservação do produto. A garantia também se perderá se for verificado que o produto foi, de qualquer modo, aberto, forçado, desarmado ou que tenha sido feito qualquer um dos Usos Proibidos detalhados no presente.

Para invocar a garantia, é necessário se comunicar por escrito com a PRONOVA, durante o período de garantia, previsto da presente garantia e a nota fiscal de compra do produto. A PRONOVA terá direito de avaliar o produto em até 15 dias, ou por um prazo maior desde que o defeito seja importante. Qualquer produto que você devolver à PRONOVA (Distribuidor Autorizado) deverá ser enviado com frete e seguro pré-pago.

Exceto as condições expostas, a PRONOVA não outorga outra garantia do produto do que as expressamente detalhadas no presente. Para tanto não poderá se entender que exista extensão ou maior alcance da mesma, tanto expressa com implícita, incluindo, podem sem limitar-se a possibilidade do uso do produto para um propósito em particular.

6. **Término da Garantia** – Esta licença será considerada automaticamente terminada em qualquer caso em que você não cumprir total ou parcialmente os termos deste contrato.

Atestado de Conformidade EC

O Token USB Protoken PRO obedece ao principal requerimento de proteção da Diretiva EMC (Diretiva 89/336/EEC relativa à compatibilidade eletromagnética) baseada em um teste voluntário.

Este certificado se refere somente a um exemplo particular do produto e a documentação técnica deste fornecida para teste e certificação. Os resultados detalhados e todos os padrões usados, bem como o modo de operação estão listados em:

Após a preparação da documentação técnica necessária, bem como a declaração de conformidade CE a marca exibida acima pode ser fixado no equipamento como estipulado no Artigo 10.1 da Diretiva. Outras diretivas relevantes devem ser observadas.

Relatório Teste No.	ACS-E07104
Testes Realizados	EN55022, EN55024, IEC61000-3-2, IEC61000-3-3, IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8 e IEC61000-4-11.

Certificado de Aprovação FCC

O Token USB Protoken PRO está em conformidade com a Parte15, Sub-parte B, Classe B 2006 (ANSI: C63,4: 2003) das Regras e Regulamentações FCC para Equipamentos de Tecnologia da Informação. Relatório número ACS-F07052

Este equipamento está baseado nos padrões USB.

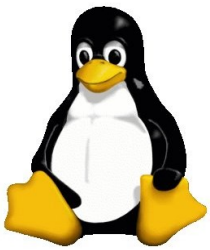
WEEE (Waste Electrical and Electronic - Descarte de Equipamentos Elétricos e Eletrônicos)

A Diretiva Européia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É sua responsabilidade eliminar este e qualquer outro equipamento elétrico e eletrônico através dos postos de recolhimento designados pelas autoridades governamentais ou locais. A eliminação e reciclagem correta ajudarão a prevenir as conseqüências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o sei equipamento antigo, entre em contato com as autoridades locais, serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Programa Logo Microsoft Windows

O ProToken PRO e o Cartão Inteligente Pronova foram aprovados nos testes Windows HCT, realizados nos Laboratórios de Provas de Hardware Windows (WHQL), os quais determinam que os produtos atendem a todos os requisitos do Programa de Logos do Windows.

O ProToken PRO e o Cartão Inteligente Pronova já possuem driver assinado para o sistema operacional Windows 7 (32bits e 64bits).



O ProToken PRO e o Cartão Inteligente Pronova possuem instalador gráficos para as distribuições Debian e Ubuntu.

Índice

1. Glossário

Assinatura Digital: Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê os seguintes serviços de segurança: autenticação da origem, integridade de dados e não repudiação do signatário.

Atribuição de chaves (key establishment): Processo que possibilita atribuir uma chave simétrica para uso criptográfico aos participantes legítimos de uma sessão de comunicação. A atribuição de chaves pode ser realizada por meio de duas técnicas: "Negociação de Chaves" ou "Transferência de Chaves".

Autoridade Certificadora (AC): Entidade idônea autorizada a emitir, renovar e cancelar certificados digitais. É responsável pela administração das chaves públicas.

Autoridade de Registro (AR): É uma entidade operacionalmente vinculada à determinada Autoridade Certificadora Habilitada, responsáveis pela confirmação da identidade dos solicitantes dos certificados e-CPF e e-CNPJ.

Certificado Digital: Documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública.

Chave criptográfica: Código ou parâmetro usado em conjunto com um algoritmo criptográfico, determinando as seguintes operações:

- Transformação de dados em texto claro para um formato cifrado e vice-versa;
- Assinatura digital computada a partir de dados;
- Verificação de uma assinatura digital computada a partir de dados;
- Geração de um código de autenticação computado a partir de dados; ou
- Um acordo para troca de um segredo compartilhado.

Chave Criptográfica em texto claro: representa uma chave criptográfica não cifrada.

Chave secreta: Chave criptográfica, usada com um algoritmo criptográfico de chave secreta, que está unicamente associada a uma ou mais entidades e não deveria tornar-se pública.

Código de Autenticação: corresponde a um verificador de integridade criptográfico que é comumente referenciado como MAC (Message Authentication Code).

Co-assinatura: A co-assinatura (ou sign) é aquela gerada independente das outras assinaturas.

Contra-assinatura: A contra-assinatura (ou countersign) é aquela realizada sobre uma assinatura já existente. Na especificação PKCS#7, a contra-assinatura é adicionada na forma de um atributo não autenticado (countersignature attribute) no bloco de informações (signerInfo) relacionado a assinatura já existente.

Elemento de Dado: Corresponde a um item de informação para o qual são definidos um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4].

Entidade usuária externa: Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido.

FIPS (Federal Information Processing Standards): correspondem a padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS, quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade, e não há padrões ou soluções industriais aceitáveis.

Firmware: Programas e componentes de dados de um módulo que estão armazenados em

hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) e não podem ser dinamicamente escritos ou modificados durante a execução.

Fronteira criptográfica (cryptographic boundary): A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.

Hardware: Parte ou equipamento físico usado para processar programas e dados.

ICP-Brasil: conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Identificador de Registro: Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4].

Integridade: propriedade que determina que dados não devem ser modificados ou apagados de uma maneira não autorizada e indetectável.

Interface: representa um ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos módulos criptográficos.

Interface CryptoAPI: Interface de operação de criptografia desenvolvida pela Microsoft. Esta interface oferece ao dispositivo independência ou implementação de encapsulamento de algoritmos criptográficos, permitindo aos desenvolvedores uma fácil utilização destes algoritmos em suas aplicações PKI, incluindo criptografia de dados, verificação de certificados e assinatura digital na plataforma Windows.

ITI: autarquia federal vinculada à Casa Civil da Presidência da República. O ITI é a Autoridade Certificadora Raiz - **AC Raiz** da Infra-Estrutura de Chaves Públicas Brasileira - **ICP-Brasil**. Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

Middleware: Software que é usado amarrar uma aplicação.

Módulo criptográfico (cryptographic module): Conjunto de hardware, software e/ou firmware que implementa funções ou processos criptográficos, abrangendo algoritmos criptográficos e de geração de chaves.

Módulo criptográfico de chip único (Single-chip Cryptographic Module): representa uma materialização física na qual um chip único de circuito integrado (Integrated Circuit Chip - ICC) poderia ser usado como dispositivo independente (standalone), ou poderia estar embutido/confinado dentro de um produto (material de área delimitada), que está ou não fisicamente protegido. Por exemplo, módulos criptográficos de chip único incluem os cartões inteligentes (Smart Cards).

Negociação de chaves (key agreement): Protocolo que possibilita atribuir uma chave simétrica aos participantes legítimos em função de valores secretos definidos por cada um dos participantes, de forma que nenhum dos participantes possa predeterminar o valor da chave. Neste método, a chave não é transferida, nem mesmo de forma cifrada. Exemplo clássico desta classe de protocolo é o algoritmo Diffie-Hellman.

Número de Identificação Pessoal (Personal Identification Number - PIN): um código alfanumérico ou senha usada para autenticar uma identidade.

Número de Registro: Número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4].

Oficial de segurança: uma entidade ou processo que age como tal, realizando funções criptográficas de iniciação ou gerenciamento.

Parâmetros críticos de segurança (PCS): Representam informações sensíveis e relacionadas a segurança, tais como, chaves criptográficas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja divulgação ou modificação podem comprometer a segurança de um módulo criptográfico.

PC/SC: especificação para integração de cartões inteligentes (smart card) em sistemas de computação

PKCS#11: padrão utilizado como interface para invocar operações criptográficas em hardware e é utilizado para prover suporte aos tokens.

Registro: Cadeia (string) de bytes que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].

Senha: uma cadeia de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar autorizações de acesso.

Software: Programas e componentes de dados usualmente armazenados em mídias que podem ser apagadas (disco rígido, por exemplo), os quais podem ser dinamicamente escritos e modificados durante a execução.

Token: Nome geral de todos os dispositivos criptográficos, tais como cartões inteligentes (smart cards), dispositivos que possuem senhas e funcionalidades de armazenamento de certificados etc.

Token USB: Dispositivo criptográfico com conector USB, portável e de fácil uso.

Transporte de chaves (key transport): Protocolo que possibilita que uma chave simétrica seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

Unidade de Dado: O menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].

Usuário: um indivíduo ou processo que age como tal com o intuito de obter acesso a um módulo criptográfico para executar serviços.

2. Lista de Acrônimos

AES Advanced Encryption Standard

APDU Application Protocol Data Unit

API Application Programming Interface

ATR Answer To Reset

CBC Cipher Block Chaining

CE Consumer electronics

CFCA China Financial Certificate Authority

CLK Clock

DES Data Encryption Standard

DF Dedicated File

EEPROM Electrically Erasable Programmable Read-Only Memory

EF Elementary File

FCC Federal Communications Commission

FIPS Federal Information Processing Standards

GND Ground

ICC Integrated Circuit Chip

ICP Infra-Estrutura de Chaves Públicas

ICP-Brasil Infra-Estrutura de Chaves Públicas Brasileira

IEC International Electrotechnical Commission

IKE Internet key exchange

IN Instrução Normativa

IPSec Internet Protocol Security

I/O Input/Output

ISO Internation Organization for Standardization

ITL Information Technology Laboratory

ITI Instituto Nacional de Tecnologia da Informação

IV Initialization Vector

JCE Java Cryptography Extension

LCR Lista de Certificados Revogados

LEA Laboratório de Ensaios e Auditoria

LSITEC Laboratório de Sistemas Integráveis Tecnológico

MAC Message Authentication Code

MAP Modular Arithmetic Processor

MF Master File

MSCAPI Microsoft Crypto API

NIST National Institute of Standards and Technology

OPSEC Operations security

PC Personal Computer

PCS Parâmetros Críticos de Segurança

PIN Personal Identification Number

PPS Protocol and Parameters Selection

PUK PIN Unlock Key

RFU Reserved for Future Use

RNG Random Number Generator

RSA Rivest Shamir and Adleman

RST Reset

SHA Secure Hash Algorithm

SO Sistema Operacional

SP Service Provider

SSL Secure Sockets Layer

TLV Tag Length Value

TSP Token Service Provider

TTL Time To Live

USB Universal Serial Bus

VPP Variable Supply Voltage

3. Sobre a Pronova Soluções Inteligentes

A Pronova Soluções Inteligentes é formada por uma equipe com mais de 15 anos de experiência no mercado de Segurança da Informação. Somos pioneiros neste setor, no qual sempre nos destacamos pela qualidade dos produtos que oferecemos aliada ao bom atendimento, formação de parcerias, lançamento de novas tecnologias, além de serviços de consultoria.

Ao longo deste período, lançamos e comercializamos no Brasil produtos desenvolvidos e utilizados em larga escala no mercado internacional. Atendemos as mais variadas necessidades de proteção, como armazenamento e transmissão segura de informações, monitoramento de conteúdo hostil, além de proteção de software contra pirataria, entre outros.

4. Instalação do ProToken PRO e/ou do Cartão Inteligente Pronova em máquinas Windows (XP/2000/2003/Vista/7)

Para instalar o software do Protoken PRO e/ou do Cartão Inteligente Pronova, basta inserir CD-ROM fornecido, aguardar a execução do Instalador e seguir as instruções abaixo detalhadas. Se você não possui o CD-ROM, entre em contato com a Pronova Soluções Inteligentes e solicite o instalador.

Nota: Se sua unidade de CD-ROM estiver com a função execução automática desabilitada, certamente será necessário executar de forma manual o arquivo *setup.exe*.

a) A primeira tela lhe dará a opção de escolher o idioma. Após selecionar o desejado, clique no botão "Next".

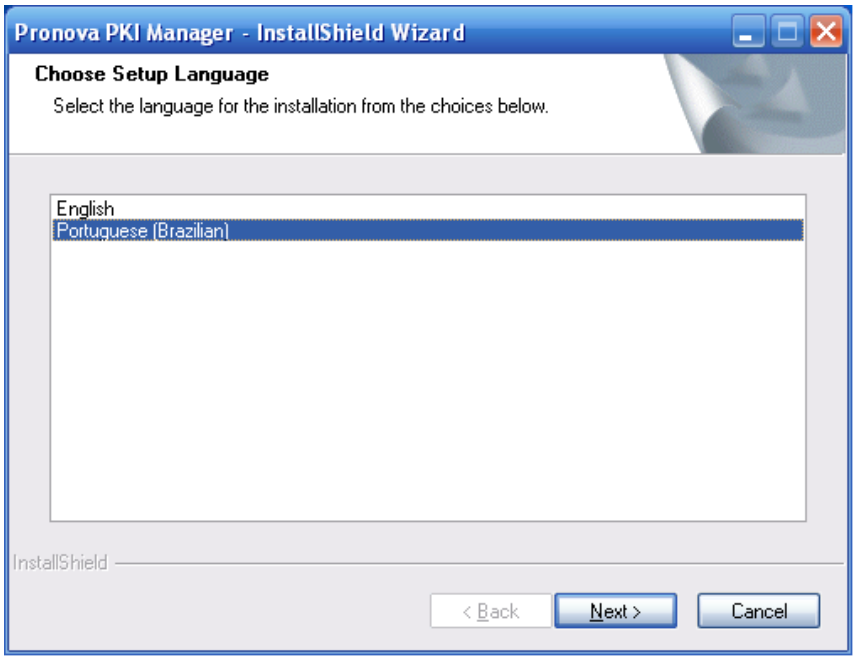


Figura 1 – Instalação: escolha do idioma

b) Em seguida, será carregado o Assistente de instalação do Gerenciador PKI Pronova. Para continuar, clique no botão "Avançar".

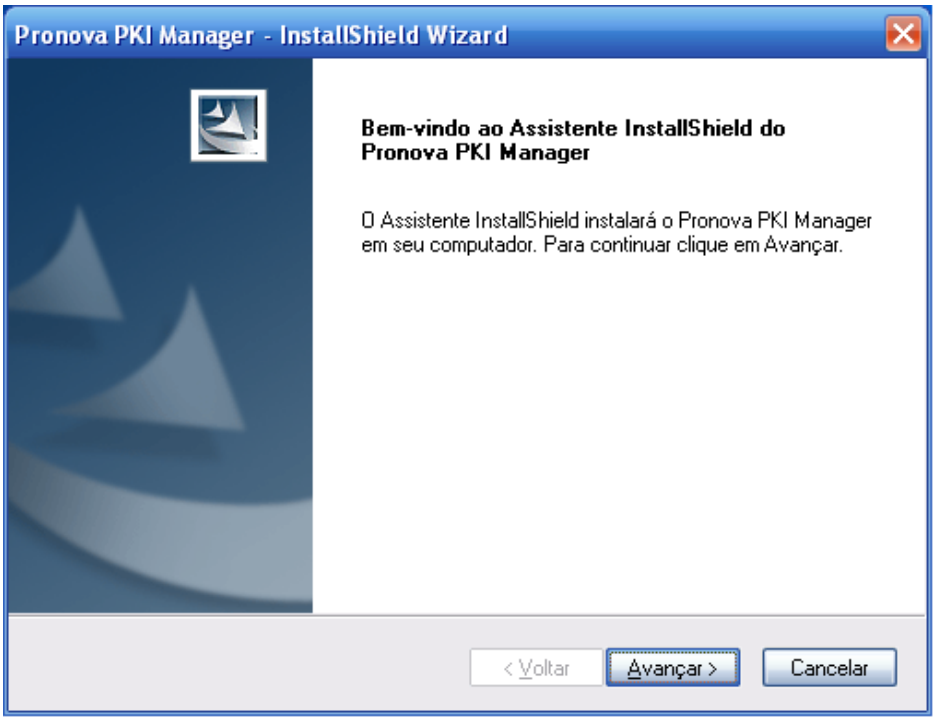


Figura 2 – Tela inicial do assistente de instalação

c) Para evitar a instalação de componentes desnecessários, selecione apenas a opção que corresponde somente aos equipamentos que você possui. Veja o quadro abaixo.

Se você possui...	Escolha a opção:
o Protoken PRO, o Cartão Inteligente Pronova e o Leitor de Cartões Inteligentes Pronova*	Completo
apenas o Cartão Inteligente Pronova ou o Cartão Inteligente Pronova + Leitor de Cartões Inteligentes Pronova*	Componentes do Cartão Inteligente Pronova e do Leitor de Cartões Inteligentes Pronova*
apenas o de Leitor de Cartões Inteligentes Pronova*	Leitor de Cartões Inteligentes Pronova*
apenas o Protoken PRO	Protoken PRO

* O Leitor de Cartões Inteligentes Pronova possui o logo da Pronova em sua carcaça externa e, portanto, NÃO É o *Leitor ROCKEY200*. Em caso de dúvidas, entre em contato com a Pronova.

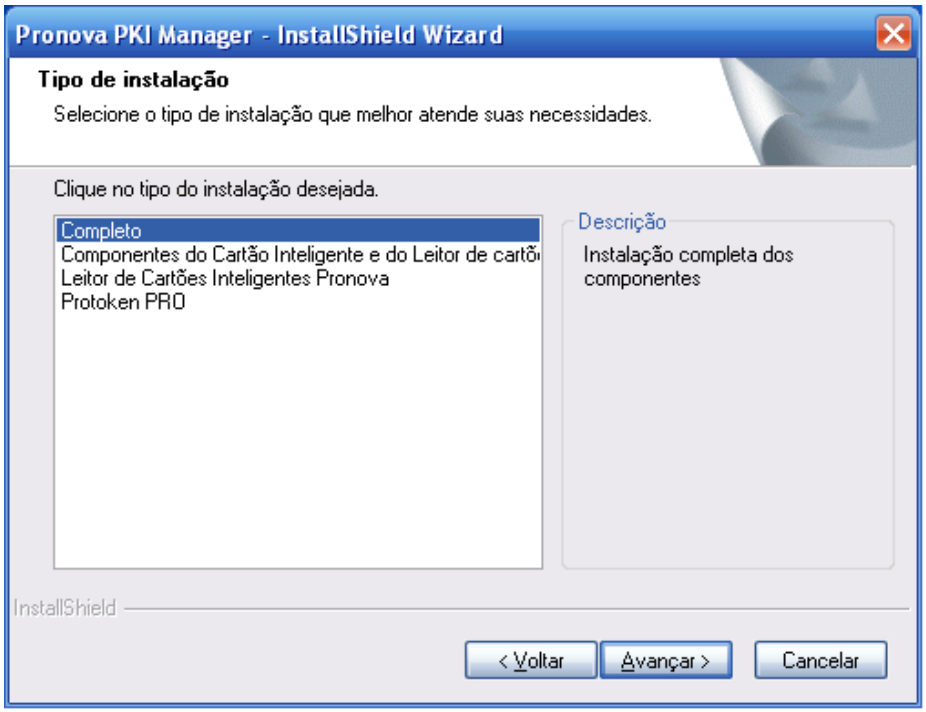


Figura 3 – Tipo de instalação

d) Se desejar alterar o diretório de instalação use o botão "Procurar" para definir um novo local. Do contrário, clique no botão "Avançar".

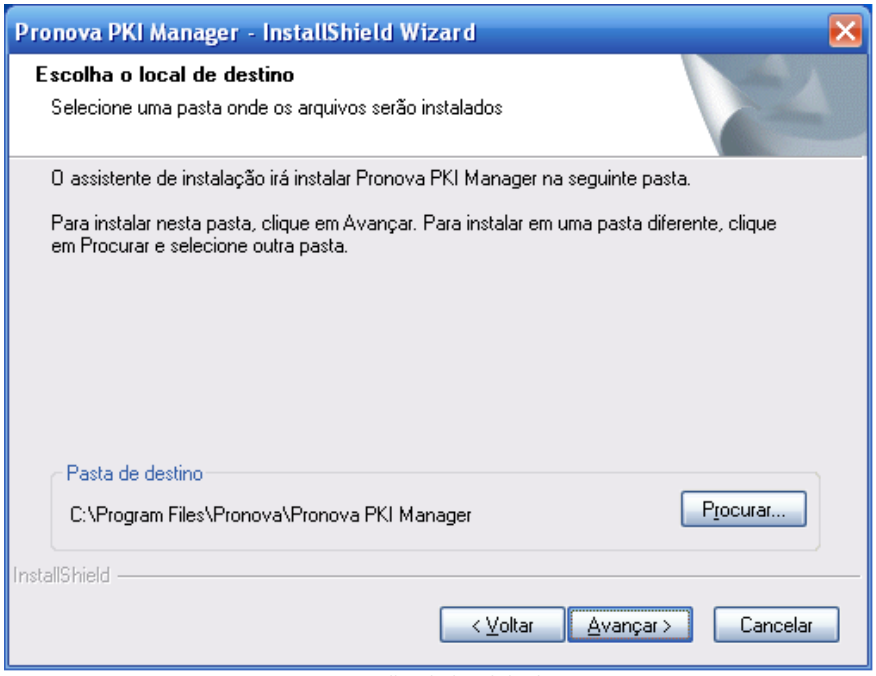


Figura 4 – Escolha do local de destino

e) Aguarde que o Assistente de instalação realize todas as operações necessárias.

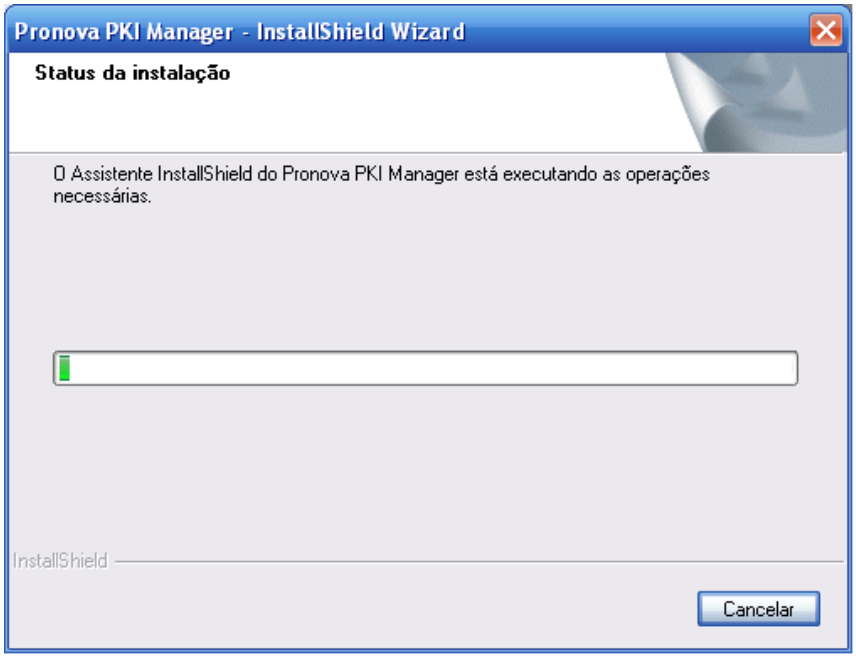


Figura 5 – Status da instalação

f) Assim que todas as operações de instalação necessárias forem realizadas, clique no botão "Concluir" e em seguida **reinicie o computador** para que as alterações tenham efeito.

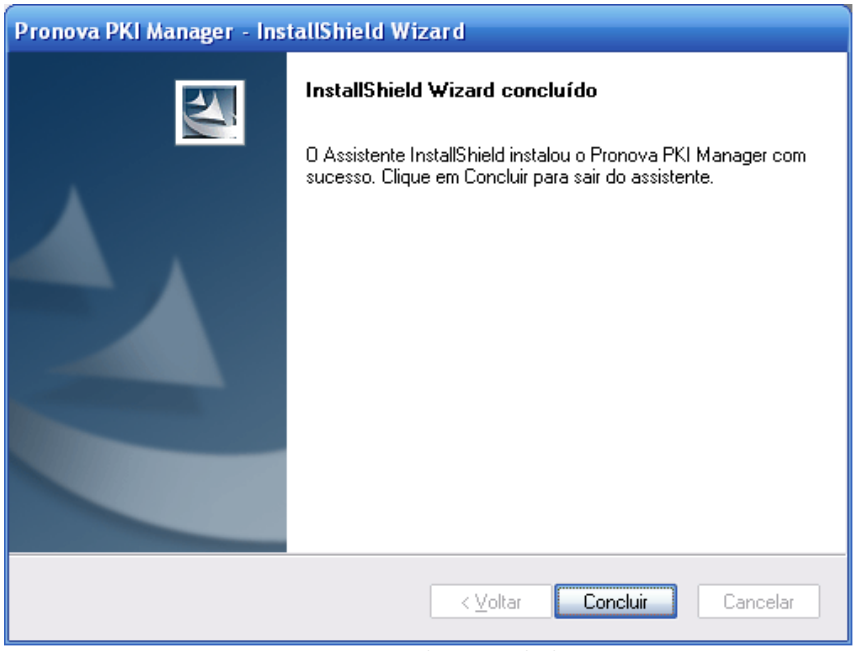


Figura 6 – Instalação concluída

5. Gerenciador PKI Pronova

Através do Gerenciador PKI Pronova é possível executar diversas operações com o Protoken PRO e com o Cartão Inteligente Pronova. Algumas dessas operações poderão ser executadas mediante a informação do PIN (Operações de Usuário) e outras mediante a informação do PUK (Operações de Administrador).

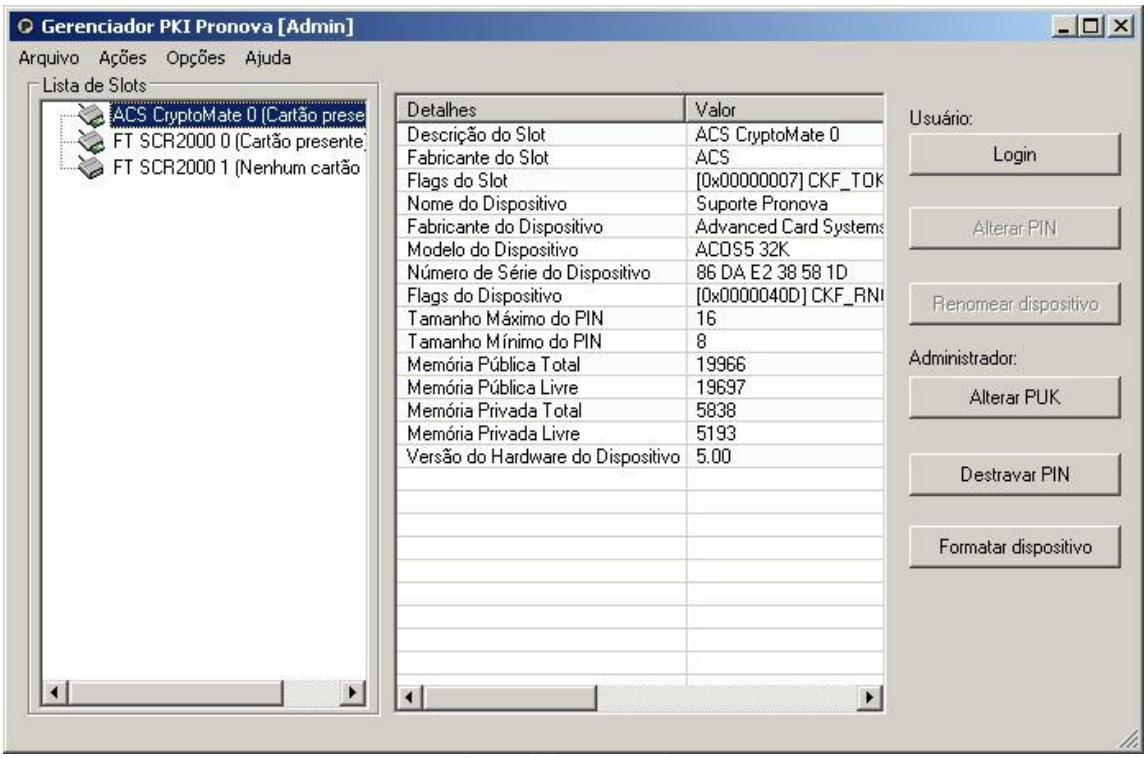


Figura 1 – Tela inicial do Gerenciador PKI Pronova

Na coluna à esquerda, em Lista de Slots, serão exibidos todos os dispositivos instalados no computador. Na Figura 1 acima, por exemplo, são mostrados os slots referentes ao Protoken PRO (ACS Cryptomate 0) e ao leitor de cartões inteligentes ROCKEY200 (FT SCR2000 0 e FT SCR2000 1). Quando um ou mais desses dispositivos estiverem conectados ao computador, a mensagem em seus slots correspondentes mudará de "Nenhum cartão presente" para "Cartão presente".

Ao selecionar um slot da lista, informações mais detalhadas serão exibidas na coluna à direita.

5.1 Operações de Usuário

Para que as operações destinadas ao usuário do dispositivo possam ser executadas, é necessário informar o PIN correto do dispositivo quando este for solicitado.

PIN (Personal Identification Number): Número de Identificação Pessoal. É a senha que será utilizada pelo usuário do dispositivo todas as vezes que for necessário ter acesso às informações pessoais que estão armazenadas no chip criptográfico. O valor de fábrica do PIN é 12345678 e, da mesma forma que o PUK, também existe um número máximo de acertos determinados para esta senha, que são 5 (cinco).

5.1.1 Login

Esta é a primeira operação a ser executada quando se deseja ter acesso às demais operações de usuário (Alterar PIN e Renomear dispositivo) e ao conteúdo do dispositivo.

Ao clicar neste botão, o PIN do usuário será solicitado:

Figura 2 – Login: digite o PIN

Se o PIN correto for informado, uma mensagem como o da figura abaixo será mostrada.

Figura 3 – Login: sucesso

Porém, se um PIN incorreto for informado, a seguinte mensagem será exibida, de acordo com o número de tentativas que ainda restarão para acerto do PIN.

Figura 4 – Login: falha

5.1.2 Alterar PIN

Após logar no dispositivo, é possível alterar o PIN atualmente definido para ele. Ao clicar no botão *Alterar PIN*, a seguinte janela será exibida:

Figura 5 – Alterar PIN: informar novo valor

Preencha os campos adequadamente e clique no botão *Alterar PIN*. Em caso de sucesso, a mensagem abaixo será exibida:

Figura 6 – Alterar PIN: sucesso

Caso contrário, uma mensagem de erro informará ao usuário o que estava errado.

5.1.3 Renomear dispositivo

Use esta operação para definir um novo nome para seu dispositivo.

A seguinte tela será exibida ao clicar no botão *Renomear dispositivo*:

Figura 7 – Renomear dispositivo: novo nome

Informe o novo nome que deseja atribuir ao seu dispositivo e clique no botão Alterar. Ao final, a mensagem abaixo será exibida:

Figura 8 – Renomear dispositivo: sucesso

Na tela principal do Gerenciador PKI Pronova, o novo nome será mostrado no campo "Nome do Dispositivo", conforme destacado na Figura 9.

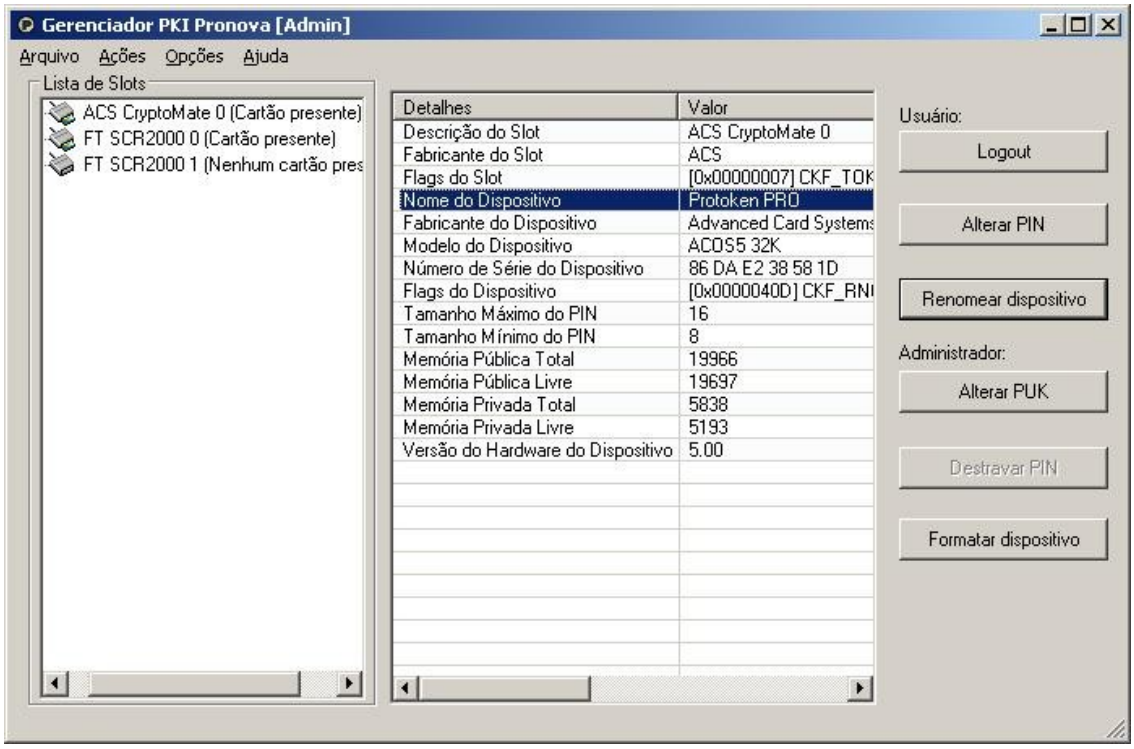


Figura 9 – Renomear dispositivo: resultado

5.1.4 Logout

Para encerrar o acesso às operações de usuário, clique no botão Logout. A seguinte mensagem será exibida:

Figura 10 – Logout

O logout do dispositivo também é feito de forma automática quando o mesmo é desconectado do computador.

5.2 Operações de Administrador

Para que as operações avançadas, destinadas ao administrador do dispositivo, possam ser executadas, é necessário informar o PUK correto do dispositivo quando este for solicitado. Não é necessário efetuar Login no dispositivo antes de executar as operações de administrador.

PUK (PIN Unlock Key): Chave de Desbloqueio do PIN. É a senha máster que permite recuperar o PIN e também formatar o setor PKI do Protoken PRO e do Cartão Inteligente Pronova. O valor de fábrica do PUK é 12345678 e, da mesma forma que o PIN, também existe um número máximo de acertos determinados para esta senha, que são 5 (cinco).

Tenha cuidado para não exceder as 5 (cinco) tentativas, pois se o PUK for travado, será necessário reinicializar o dispositivo com uma ferramenta chamada Formatador[1], que irá apagar todo o conteúdo armazenado no Protoken PRO ou no Cartão Inteligente Pronova.

Por questões de segurança e de privacidade, recomendamos que o PUK seja alterado assim que seja possível, ou seja, na primeira utilização. Depois que esta alteração for realizada, o PUK deverá ser guardado em um local seguro. Esta senha máster deve ter no mínimo 8 (oito) caracteres.

5.2.1 Alterar PUK

Ao clicar no botão *Alterar PUK*, a seguinte janela será exibida:

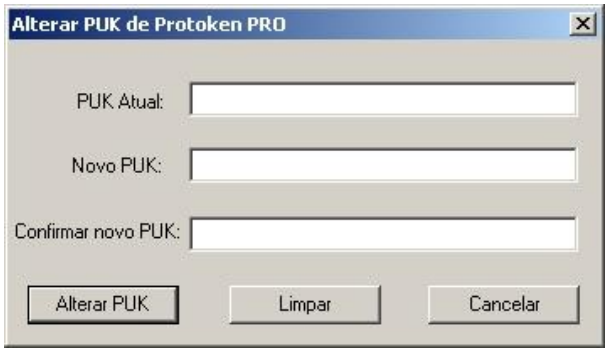


Figura 11 – Alterar PUK: informar novo valor

Preencha os campos adequadamente e clique no botão *Alterar PUK*. Em caso de sucesso, a mensagem abaixo será exibida:

Figura 12 – Alterar PUK: sucesso

Caso contrário, uma mensagem de erro informará ao usuário o que estava errado.

5.2.2 Destravar PIN

Quando o PIN de um dispositivo é perdido ou desconhecido o usuário fica sem acesso aos seus certificados nele armazenados e ainda não pode efetuar as operações Login/Logout, Alterar PIN e Renomear dispositivo. Nestes casos, a operação *Destravar PIN* deve ser utilizada, ainda que o número máximo de tentativas de acerto do PIN não tenha sido atingido.

A operação Destravar PIN permite que se defina um novo PIN para o dispositivo, mediante a informação do PUK. Ao final, o usuário recupera o acesso ao seu dispositivo e nenhum dado armazenado é perdido.

ATENÇÃO: Antes de iniciar este procedimento tenha absoluta certeza de que está de posse do PUK do dispositivo! Se ocorrer cinco tentativas de acesso com o PUK incorreto, o seu token/cartão inteligente será totalmente travado e será necessário reformatá-lo, perdendo assim todas as informações que estão armazenadas no equipamento.

Ao clicar no botão *Destravar PIN*, primeiramente a seguinte janela será exibida:

Figura 13 – Destravar PIN: novo PIN

Clicando depois no botão *Destravar*, o PUK do dispositivo será solicitado.

Figura 14 – Destravar PIN: PUK atual

Em caso de sucesso, a seguinte mensagem será exibida:

Figura 15 – Destravar PIN: sucesso

Do contrário, uma mensagem de erro informará ao usuário o que estava errado.

5.2.3 Formatar dispositivo

Sempre que você julgar necessário apagar todo o conteúdo (certificados e chaves criptográficas) do seu dispositivo, faça uso da operação "Formatar dispositivo" do Gerenciador PKI Pronova.

ATENÇÃO: Esta é uma ação irreversível e que vai apagar todas as informações, inclusive certificados digitais, que estiverem armazenadas no dispositivo. E não será possível recuperar estas informações.

Clique no botão *Formatar dispositivo* e informe o novo PIN e o novo nome (rótulo) para o dispositivo.

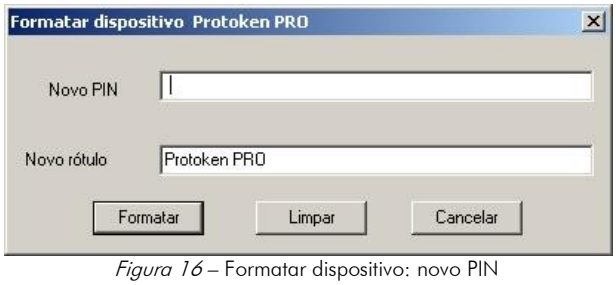


Figura 16 – Formatar dispositivo: novo PIN

Antes de iniciar o processo de formatação, o aplicativo pede que o usuário confirme se realmente deseja prosseguir.

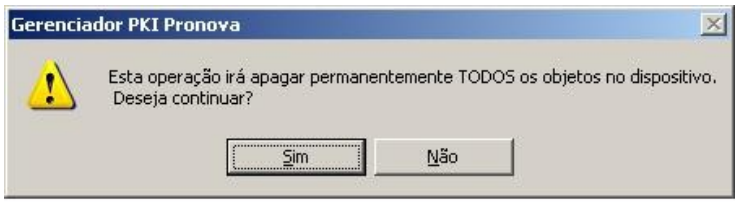


Figura 17 – Formatar dispositivo

Informe o PUK atual do dispositivo quando solicitado.

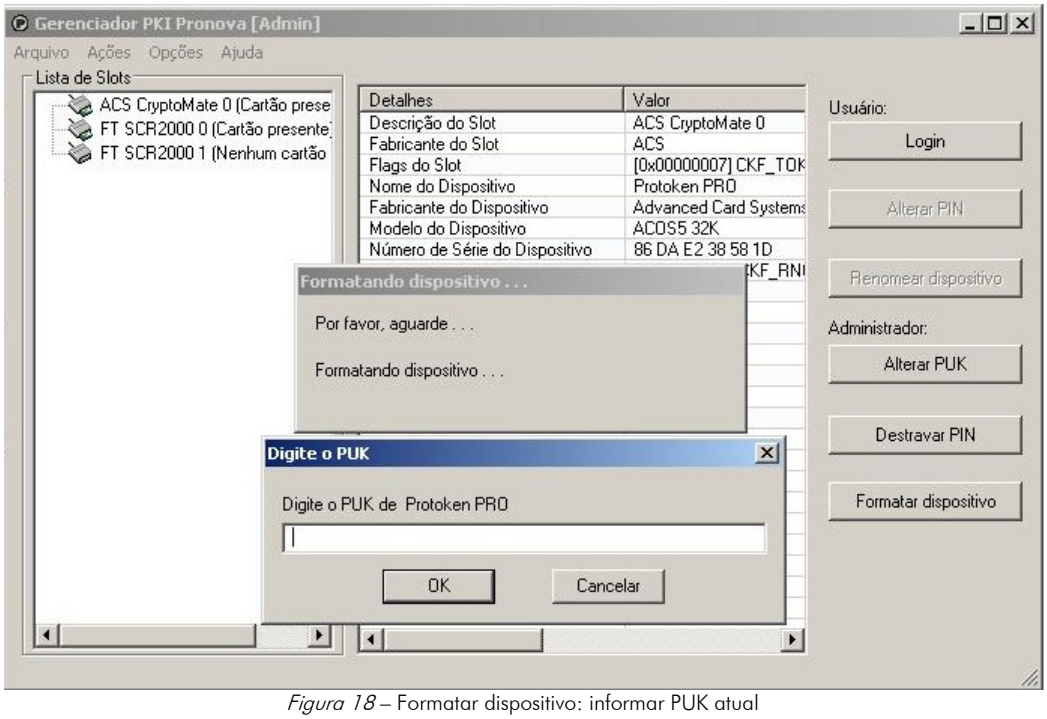


Figura 18 – Formatar dispositivo: informar PUK atual

Ao final de uma operação bem sucedida, a seguinte mensagem será exibida:

Figura 19 – Formatar dispositivo: sucesso

5.3 Menu

Além das operações disponibilizadas na tela principal do Gerenciador PKI Pronova, há também outras acessíveis pelo menu da aplicação.

5.3.1 Arquivo

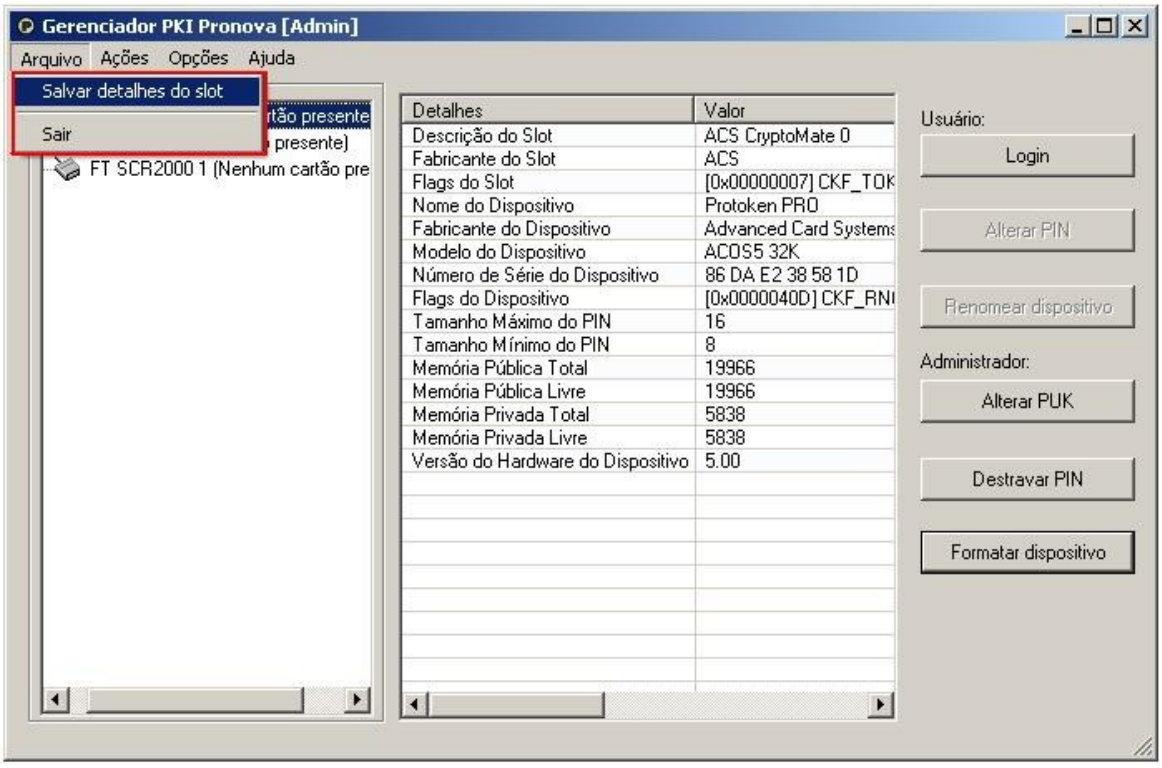


Figura 20 – Menu do Gerenciador PKI Pronova: Arquivo

Para salvar as informações exibidas no lado direito da tela do Gerenciador PKI Pronova, referentes a um slot selecionado, basta clicar na opção "Salvar detalhes do slot". Esses dados serão gravados em um arquivo texto que pode ser usado posteriormente, por exemplo, durante um atendimento, caso seja solicitado pela equipe de Suporte Técnico da Pronova.

Para fechar o Gerenciador PKI Pronova, clique na opção "Sair".

5.3.2 Ações

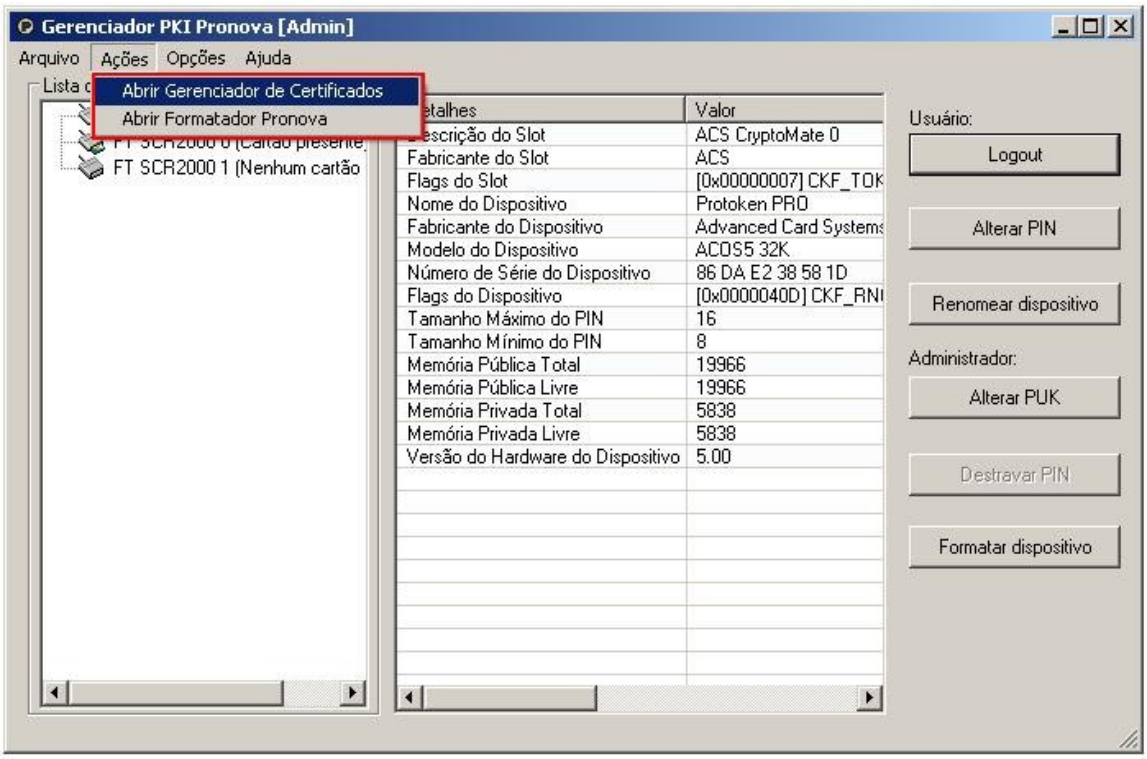


Figura 21 – Menu do Gerenciador PKI Pronova: Ações

a. Abrir Gerenciador de Certificados

O Gerenciador de Certificados só pode ser acessado após executar a operação "Login", na tela principal do Gerenciador PKI Pronova.

Com este gerenciador é possível: *ver* as informações sobre um certificado armazenado no Protoken PRO ou no Cartão Inteligente Pronova; *exportar* um certificado do dispositivo (somente a parte pública); *importar* um certificado para o dispositivo (a partir de um arquivo de formato .CER, .P12, .PFX, .P7B ou .P7C); *apagar* um objeto do dispositivo; *apagar todos os objetos* do dispositivo; e *atualizar* as informações que são vistas do conteúdo do dispositivo.

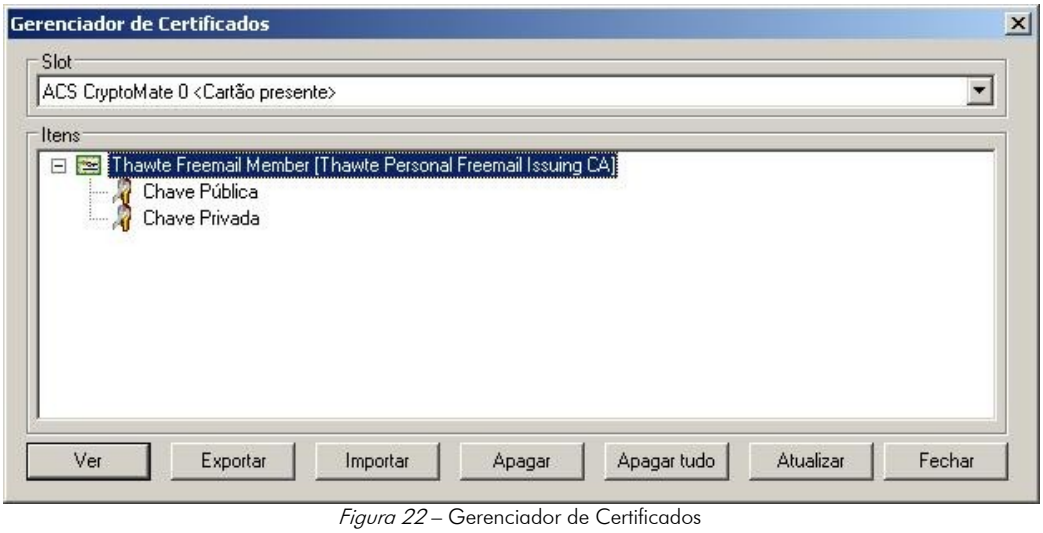


Figura 22 – Gerenciador de Certificados

Para sair do Gerenciador de Certificados, clique no botão "Fechar".

b. Abrir Formatador Pronova

Através do Formatador Pronova é possível formatar um Protoken PRO ou um Cartão Inteligente Pronova sem informar o PUK do dispositivo. Isto é útil quando ambos o PIN e o PUK de um dispositivo são perdidos.

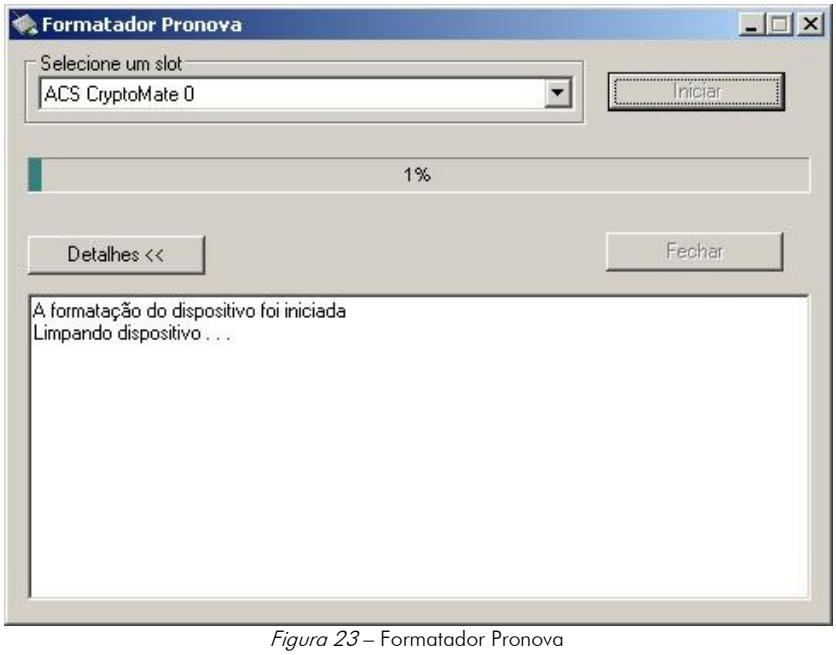


Figura 23 – Formatador Pronova

Ao formatar um dispositivo com o Formatador Pronova, TODAS AS INFORMAÇÕES GRAVADAS, INCLUSIVE CERTIFICADOS DIGITAIS, NO DISPOSITIVO SERÃO APAGADAS E NÃO PODERÃO SER RECUPERADAS, bem como serão restauradas as configurações de fábrica do Protoken PRO e do Cartão Inteligente Pronova, inclusive os valores do PIN e do PUK, que voltam a ser iguais a 12345678. O número máximo de tentativas de acerto do PIN e do PUK também é restaurado e volta a ser igual a 5.

ATENÇÃO: SE VOCÊ JÁ POSSUI UM CERTIFICADO DIGITAL GRAVADO NÃO USE ESTA FERRAMENTA!

5.3.3 Opções

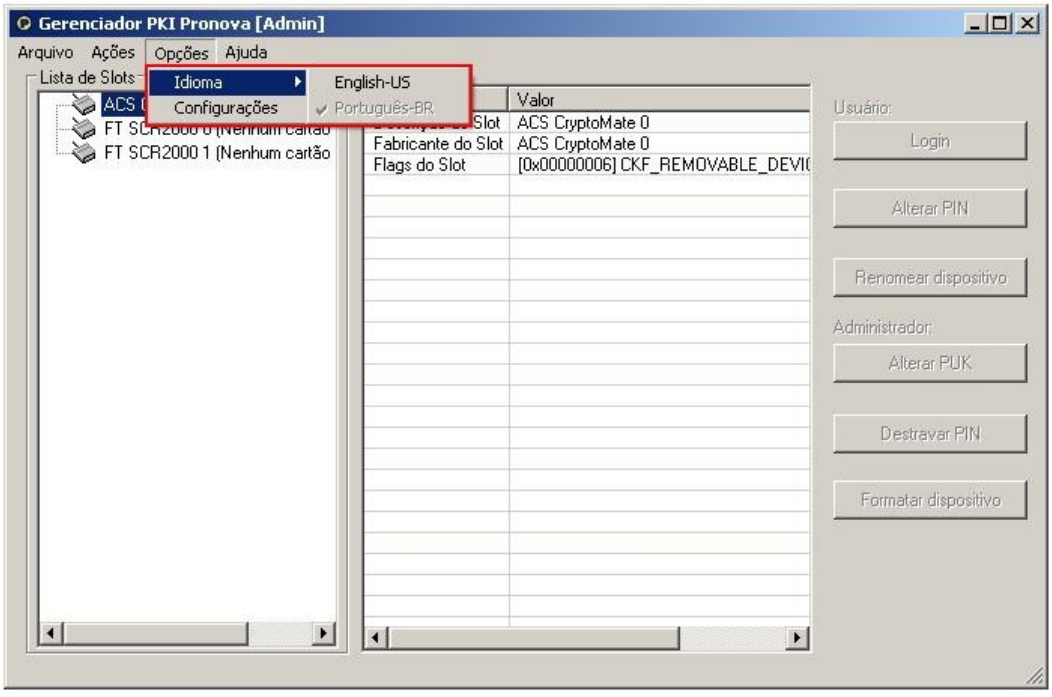


Figura 24 – Menu do Gerenciador PKI Pronova: Opções

No menu "Opções" é possível alterar o idioma do Gerenciador PKI Pronova para um dos dois disponíveis: Português-BR ou Inglês (English-US). Além disso, há uma série de outras opções avançadas que podem ser configuradas. Para isto, clique na opção "Configurações".

Na aba "Geral", na área "Tempo de vida do PIN", o usuário pode definir se deseja que seja feito logout do dispositivo somente quando o mesmo for desconectado do computador ou um certo tempo depois (em minutos) da última vez em que o PIN foi informado.

Figura 25 – Opções, Configurações: aba Geral

Ainda nessa aba, na área "Certificado", é possível definir que o certificado armazenado no dispositivo será instalado/removido no/do repositório do Windows sempre que o Protoken PRO ou o Cartão Inteligente Pronova for conectado/desconectado do computador.

Na aba "Suporte Técnico" o usuário pode habilitar a criação de logs (CSP e PKCS) em sua máquina. Esses logs registrarão todas as operações efetuadas com o dispositivo e podem ser de grande ajuda em caso de necessidade durante um atendimento de suporte pela equipe da Pronova. Assim como podem ser criados, esses arquivos de log também podem ser apagados através dessa aba.

Figura 26 – Opções, Configurações: aba Suporte Técnico

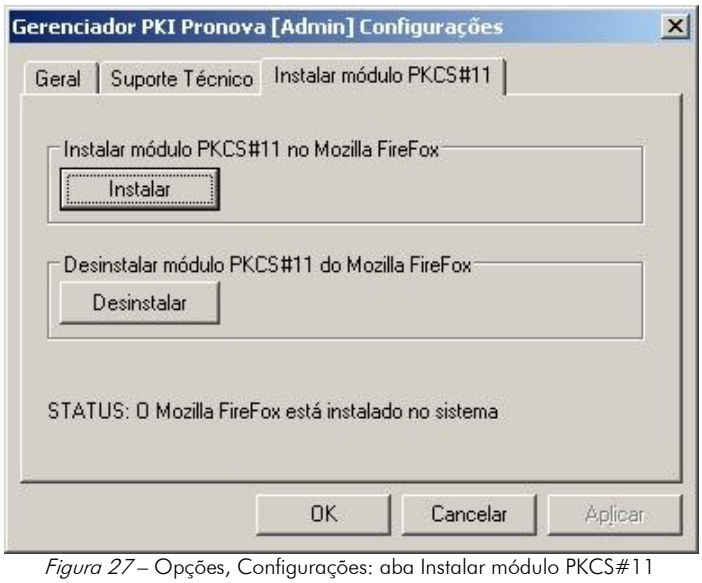


Figura 27 – Opções, Configurações: aba Instalar módulo PKCS#11

Caso o navegador Mozilla Firefox tenha sido instalado em seu computador após a instalação do software do Protoken PRO/Cartão Inteligente Pronova, é possível adicionar o módulo PKCS#11 do dispositivo nesse navegador. Esta ação é necessária para a utilização do certificado armazenado em seu dispositivo em sites acessados através do Firefox.

Para fazer a instalação, simplesmente clique no botão "Instalar" e siga as orientações que serão exibidas na tela. Caso algum dia precise desinstalar este módulo, basta clicar no botão "Desinstalar".

NOTA: Se o Mozilla Firefox já estiver instalado no sistema antes da instalação do software do Protoken PRO/Cartão Inteligente Pronova, a instalação desse módulo PKCS#11 será feita durante a instalação do software do dispositivo.

6. Aderência a Padrões

O Token USB e o Cartão Inteligente Pronova seguem os principais padrões de segurança hoje utilizados em soluções baseadas no uso de chaves públicas e privadas. No que tange ao suporte ao algoritmo SHA-2, estes hardwares suportam as seguintes variantes: SHA-256 e SHA-512. No CD-ROM de instalação são disponibilizadas duas aplicações para codificação do conteúdo de um arquivo usando os algoritmos 3DES, SHA-1, SHA-256 e SHA-512. No diretório SDK, desenvolvedores terão acesso ao Kit de Desenvolvimento que permite a integração com aplicações PKI através dos padrões Microsoft Crypto API ou PKCS#11.

7. Recursos Oferecidos

- → Geração no próprio dispositivo (on board) do par de chaves RSA 512, 1024 e 2048bits;
- → Suporte nativo para os algoritmos DES (ECB, CBC), 3DES (ECB, CBC), MAC, SHA-1, SHA-2 (SHA-256 e SHA-512) AES-128, RSA-512, RSA-1024 e RSA-2048;
- → Suporte padrão para aplicações Microsoft CAPI;
- → Compatível com Windows 2000 PC/SC;
- → Geração de números aleatórios em hardware;
- → Assinatura digital realizada em hardware;
- → Suporte para múltiplas aplicações PKI, inclusive ICP-Brasil;
- → Suporte para múltiplos armazenamentos de chaves;
- → Interface padrão USB tipo A 2.0 (compatível com 1.x);
- → Certificações: CE, FCC, IPX7 – IEC 529, Common Criteria EAL5+ (Chip Level)
- → Chassi de plástico resistente (tamper evident); resistente a água (IPX7 – IEC 529);
- → Capa protetora do conector USB;

8. Especificações Técnicas (EN.I.01.01 – MCT 3 – Volume II)

Sistemas Operacionais:	Windows 98SE, Windows 2000 (32 e 64bits), Windows ME, Windows XP (32 e 64bits), Windows 2003 (32 e 64bits), Windows 2008 (32 e 64bits), Windows 7 (32 e 64bits) e Linux (kernel 2.4 ou versão mais recente)
Certificações e Padrões:	PKCS#11 v2.11, MS CAPI, PC/SC, X.509 v3, SSL v3, IPSec/IKE, ISO 7816 1/2/3/4/8/9, FCC, CE, IPX7 – IEC 529, Common Criteria EAL5+ (Chip Level), RoHS e compatível com FIPS 140-2
Processador:	8 bits
Memória Disponível:	32 KB
Algoritmos On-Board:	DES (ECB, CBC), 3DES (ECB, CBC), MAC, SHA-1, SHA-2 (SHA-256 e SHA-512) AES-128, RSA-512, RSA-1024 e RSA-2048
Nível de Segurança do Chip:	Armazenamento de dados seguro e criptografado
Dimensões:	53.5 mm x 15.7mm x 7.8mm
Peso:	6g
Dissipação de Energia:	< 250 mW
Temperatura de Operação:	0 até 50°C
Temperatura de Armazenamento:	-40 até 85°C
Faixa de umidade:	0 até 100% - 0 até 100% sem condensação
Conector:	Universal Serial Bus, tipo A, 2.0 (compatível com 1.x)
Chassi:	Plástico reforçado, à prova de violação (tamper evident)
Retenção de Dados de memória:	10 anos
Capa protetora do conector USB	Sim
Número Serial	Sim

9. Requisitos mínimos

Verifique se seu sistema atende aos seguintes requisitos mínimos:

Sistema Operacional	Windows 98SE, ME, 2000, 2003, 2008, XP, Vista, 7 ou Linux (kernel 2.4 ou mais recente)
Espaço em disco	Pelo menos 10 MB
Porta USB	Pelo menos uma porta USB tipo A livre
Direitos	O usuário deverá ter privilégios de administrador para ter direito de instalar dispositivos no sistema operacional

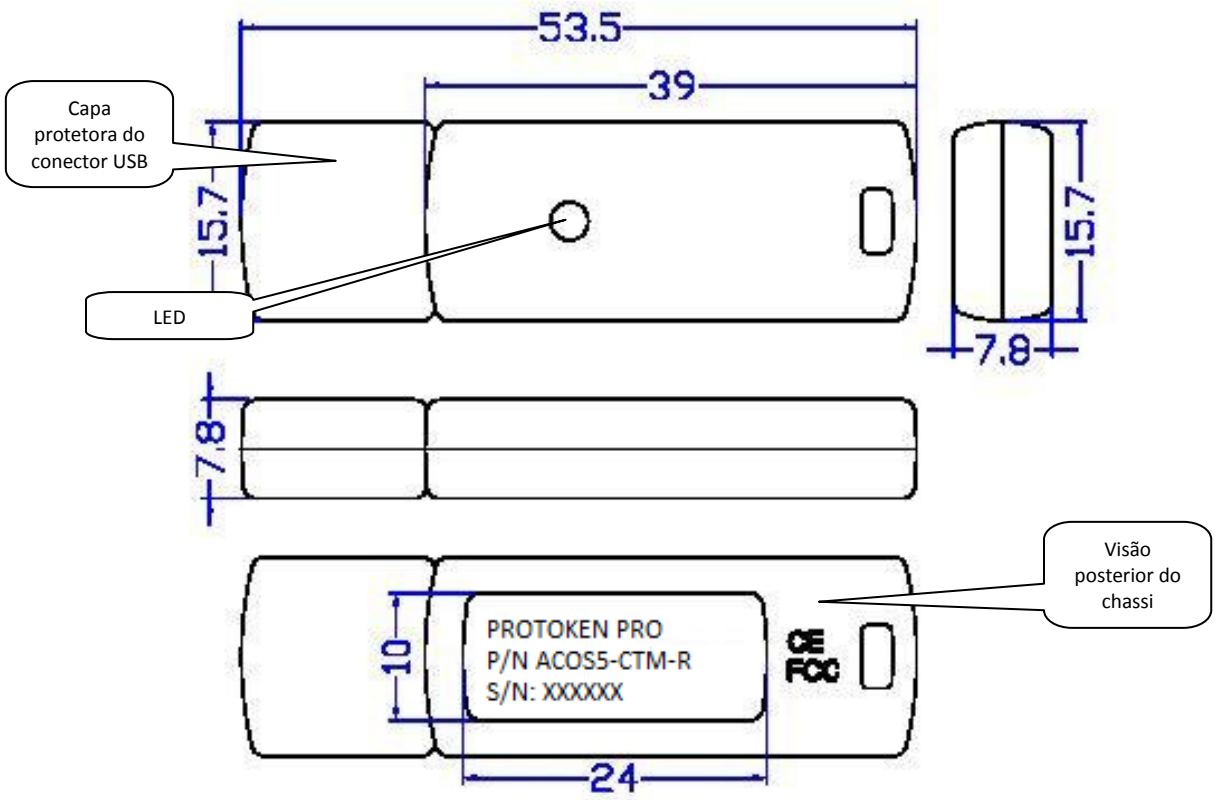
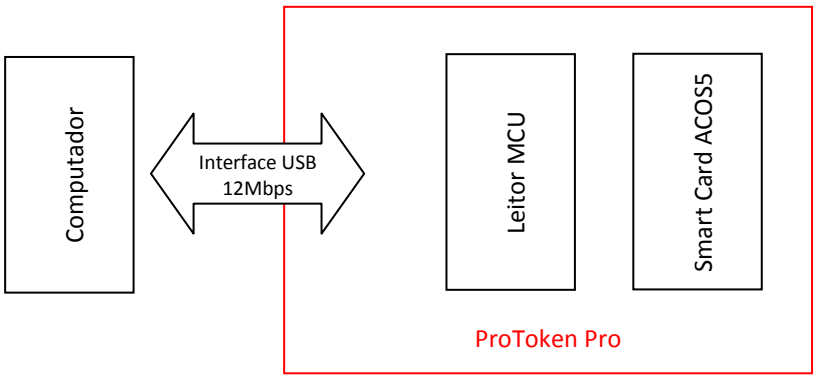


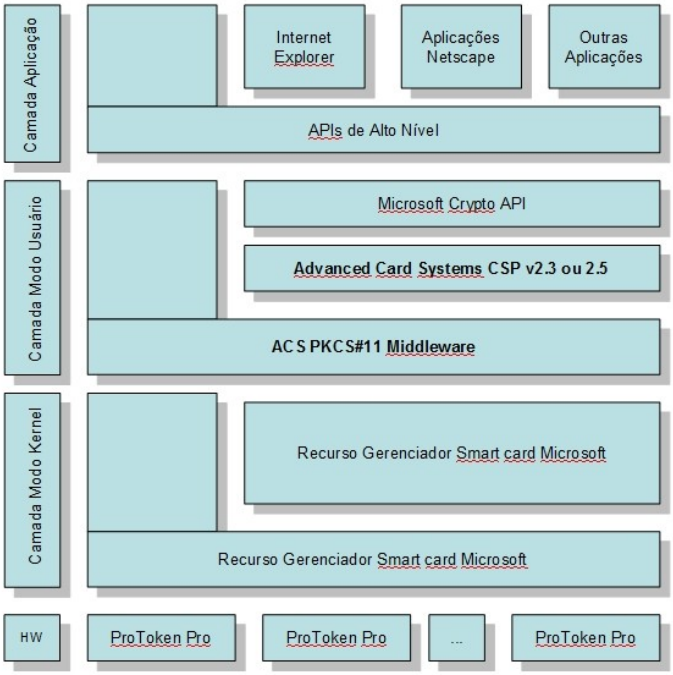
Figura acima é uma ilustração do chassi do ProToken Pro (REQUISITO I.2 – MCT – Volume II)



O Diagrama acima apresenta como está estruturada a PCB do ProToken Pro

10. Arquitetura (**REQUISITO I.1 do MCT 3 – Volume II)**

É oferecida uma API padrão PC/SC. Desenvolvedores podem fazer uso da função padrão Microsoft Win32 PC/SC para manipular o ProToken Pro ou o Smart Card Pronova.



A arquitetura do sistema consiste em quatro camadas a saber: Hardware, Kernel Driver, Interface do Usuário e Aplicação.

Camada Hardware	Consiste no circuito do dispositivo, programa firmware e conexão. Ele troca dados com o computador via protocolo de comunicação USB da porta USB
Camada Kernel Driver	Manipula a interação de dados entre o PC e a Camada de Hardware, e o acesso ao Token/Smart Card requer a camada de aplicação superior. É a interface do driver PC/SC padrão. As camadas de aplicação superiores podem acessar o dispositivo através do conjunto de funções padrão Win32 PC/SC
Camada Interface do Usuário	As interfaces nesta camada são a PKCS#11 API e a Microsoft Crypto API. Elas são suportadas por interfaces inferiores, compatíveis com as aplicações existentes e podem ser desenvolvidas novamente. Por exemplo, algumas aplicações requerem que os usuários assinem digitalmente o conteúdo que eles submetem pelo navegador com o dispositivo. Funções como esta requerem a camada de interface superior
Camada Aplicação	Programas na camada de aplicação incluem geralmente aplicações disponíveis. As interfaces fornecidas são baseadas nos padrões da indústria e são conhecidos da maioria dos desenvolvedores. Os desenvolvedores devem integrar suas aplicações com o dispositivo usando as interfaces fornecidas

11. Removendo o software do ProToken PRO e Cartão Inteligente Pronova

Para remover o software do ProToken PRO e do Cartão Inteligente Pronova, vá até o Painel de Controle "Adicionar ou Remover Programas", localize a opção "Pronova PKI Manager (Somente remover) e clique no botão "Alterar / Remover" e sigas as instruções do assistente.

12. Suporte Técnico

Se as informações contidas neste guia rápido não foram suficientes, não se preocupe, entre em contato conosco sempre que precisar. Nosso e-mail para suporte é suporte@pronova.com.br, o telefone para contato é (21) 2491-3688 e o nosso chat está em www.pronova.com.br.

13. Contatos

Pronova Soluções Inteligentes (Distribuidor Autorizado)

Endereço	Avenida das Américas 500, bloco 4 (entrada A), Sala 302. Barra da Tijuca. Rio de Janeiro – RJ. CEP 22.640-100. Brasil.
Telefones	+55-21-24913688
Fax	+55-21-24913688 (ramal 123)
E-mail	suporte@pronova.com.br ou sac@pronova.com.br
Sites	www.pronova.com.br - www.lojapronova.com.br - www.meucertificadodigital.com.br