PRONOVA

SOLUÇÕES
INTELIGENTES

Versão 2.57

Pronova Consultoria em Tecnologia da Informação Ltda. & Feitian Technologies Co., Ltd.

Todos os produtos da FEITIAN Technologies Co., Ltd. (FEITIAN) e 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 FEITIAN, que também terá alcance aos distribuidores, revendas ou representantes da FEITIAN, 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 FEITIAN (www.ftsafe.com) ou 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 FEITIAN/PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desasemblada, 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 FEITIAN ou pela PRONOVA.

3. **Garantia** – FEITIAN e PRONOVA garantem 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 FEITIAN ou 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 FEITIAN e da PRONOVA é efetuar ou reparar a descrição da FEITIAN e da PRONOVA, qualquer produto sem que isto possa gerar algum encargo para você.

Para tanto FEITIAN e 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 Feitian ou PRONOVA serão responsáveis 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 FEITIAN ou PRONOVA tiverem avisado da possibilidade de ocorrência ao dano. Qualquer produto que você entregará a FEITIAN ou a PRONOVA com a finalidade de troca em comprimento desta garantia, passará a ser propriedade da FEITIAN ou 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. FEITIAN e PRONOVA terão 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 a FEITIAN ou a PRONOVA (Distribuidor Autorizado) deverá ser enviado com frete e seguro pré-pago.

Exceto as condições expostas, FEITIAN e PRONOVA não ortogam outra garantia dos produtos do que as expressamente detalhadas no presente. Para tanto não poderá se estender 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 ePass2000 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:

Relatório Teste No.	RBJA04010201-1&2	
Testes Realizados	EN 55022:1998+A1:2000 Classe B	EN 55024:1998+A1:2001

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.

Certificado de Aprovação FCC

O Token USB ePass2000 está em conformidade com a Parte 15 Classe B das Regras FCC e Regulamentações para Equipamentos de Tecnologia da Informação. Relatório número RBJA04010201.

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

Este dispositivo foi aprovado 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.

Check Point OPSEC

O Token USB ePass2000 possui a certificação OPSEC (Open Platform for Security) da Check Point Software Technologies Ltd. (NASDAQ: CHKP), líder mundial em segurança através de Internet. Com a certificação OPSEC, o Token USB ePass2000 se integra de forma transparentemente com as soluções líderes da Check Point do mercado: VPN-1®, FireWall-1® e Next-Generation®.

Entrust Ready

Entrust® Ready

Os Tokens ePass são dispositivos criptográficos seguros e portáteis, ideais para Entrust/PKI e outras aplicações tais como: autenticação de dois fatores, codificação de e-mail, sites seguros (SSL), logon VPN e muito mais. Foi outorgado aos Tokens ePass o status Entrust Ready com as aplicações o Entrust Entelligence client e Entrust Authority Securtity Manager.

Índice

1. Glossário 8
2. Lista de Acrônimos 11
3. Sobre a Pronova Soluções Inteligentes 14
4. Sobre a Feitian Technologies Inc., Ltd. 14
5. Sobre o Token USB ePass2000 14
5.1 Descrição Física Externa do ePass2000 14
5.9 O que é o PUK (PIN Unlock Key) 19
5.10 O que é o PIN do Usuário? 20
6. Instalando o software do Token USB ePass2000 20
6.1 Instalação nos sistemas Windows 2000, Windows XP, Windows Vista e Windows 2003 20
6.2 Instalação nos sistemas Windows 98SE e Windows ME 23
6.3 Instalação por linha de comando 24
6.4 Instalando o ePass2000 em máquinas com Linux 24
6.5 Instalando o ePass2000 em máquinas com Mac OS 25
6.6 Monitor de Certificados - Configurando o Tempo de Vida do PIN através 25
6.7 Monitor de Certificados - Alterando o PIN 26
6.8 Monitor de Certificados – Visualizando Detalhes do Certificado 27
6.9 Monitor de Certificados – Removendo um Certificado do Repositório do Windows . 27
6.10 Monitor de Certificados – Devolvendo um Certificado do Repositório do Windows 28
7. Gerenciador PKI do ePass2000 28
7.1 Gerenciador PKI – Login 29
7.1.2 Excluindo dados gravados no Token ePass2000 30
7.2 Gerenciador PKI – Alterar PIN 32
7.3 Gerenciador PKI – Renomear Token 34
7.4 Gerenciador PKI – Alterar PUK 36
7.5 Gerenciador PKI – Destravar PIN 37
7.6 Gerenciador PKI – Formatar Token 38
8. Suporte ao Mecanismo de chalenge/response (desafio/resposta) 40
11. Utilizando o Mozilla Firefox para alterar o PIN do ePass2000 45
12. Importando um certificado digital para o ePass2000 a partir de um arquivo 47
13. Configurando o Microsoft Outlook para usar um certificado armazenado no ePass2000 50
14. Configurando o Outlook Express para usar um certificado armazenado no ePass2000 52
15. Integrando o ePass2000 com o Mozilla Thunderbird 58
16. Configurando sua conta de e-mail no Mozilla Thunderbird para fazer uso do certificado digital armazenado no ePass2000 59
17. Adicionando a identidade digital do remetente ao catálogo de endereços do Windows 60
18. Enviando uma mensagem criptografada usando o Outlook Express 62
19. Adicionando uma identificação digital à sua lista de contatos do Microsoft Outlook 65
20. Enviar uma mensagem com uma assinatura digital para um destinatário da Internet usando o Microsoft Outlook 67
21. Enviar uma mensagem criptografada para um destinatário da Internet usando o Microsoft Outlook 67
22. Removendo o software do ePass2000 68
23. Perguntas e Respostas Comuns 68
24. Suporte Técnico 71
25. Contatos 71

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.

ePass2000: Dispositivo criptográfico portável integrado com smart card e porta USB, o qual foi desenvolvido pela Feitian. Uma das vantagens deste dispositivo sobre os cartões inteligentes é a portabilidade, bem como suporte a aplicações PKI.

ePassNG: Nova geração de produto (middleware framework) desenvolvido pela Feitian. Este novo middleware suporta todas as séries dos produtos ePass. Fácil de ser atualizado com novo suporte de hardware, bem como suporte a aplicações PKI.

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 idenpendência 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 firmaware 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.

TSP (Token Service Provider): Camada de hardware abstrata presente no framework ePassNG. Esta camada interfaces comuns de entrada e saída para todos os tipos de dispositivos. O design pode prover uma determinada expansão contra as diferenças de hardware.

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. Sobre a Feitian Technologies Inc., Ltd.

A Feitian Technologies Co., Ltd. iniciou suas operações em 1998 com o desenvolvimento do Sistema de Proteção de Software ROCKEY. Ao longo de suas atividades, a Feitian se tornou rapidamente o principal provedor de chaves de proteção de software na China e aumentou exponencialmente suas vendas no mercado mundial.

5. Sobre o Token USB ePass2000

O **ePass2000** é um dispositivo USB que foi desenvolvido para oferecer autenticação, verificação e serviços de criptografia de informações, além de suporte para criptografia de e-mails, assinatura digital e uso de SSL no Internet Explorer, Outlook, Outlook Express, Netscape Communicator ou qualquer outro software baseado em padrões Microsoft Crypto API ou PKCS#11. Como os demais produtos existentes no mercado, o ePass2000 é notavelmente versátil e o seu kit de desenvolvimento (SDK – Software Developer's Kit) pode ser usado para criar diversas outras aplicações.

O **ePass2000** é um token USB de autenticação aderente as normas do Comitê Gestor da ICP-Brasil que pode ser utilizado em Windows 98SE, 2000, ME, XP*, 2003, Mac OS 8/9/X e Linux. Da mesma forma que um cartão inteligente (smart card), pode executar poderosos cálculos de criptografia. As rotinas de criptografia executadas pelo ePass2000 que fazem uso das chaves privadas usam uma área de memória do tipo non-swappaple.

5.1 Descrição Física Externa do ePass2000

5.2 Sobre o chip criptográfico do ePass2000

O chip criptográfico do ePass2000 é um microcontrolador serial de acesso especialmente projetado para aplicações seguras e portáveis. O chip inclui também um MAP o qual está baseado em um processador de arquitetura de 1088bits. Ele processa multiplicação modular, squaring e cálculos adicionais de até 2176bits operands.

* Com exceção ao Windows XP Starter Edition, o qual, segundo a Microsoft Brasil, não possui o serviço cartão inteligente disponível para instalação.

O MAP (Modular Arithmetic Processor) e o acelerador DES foram projetados para acelerar os cálculos criptográficos usando algoritmos de chave pública e de chaves secretas. Este produto está baseado em uma CPU de 8bits e inclui chips de memórias: ROM Usuário, RAM Usuário e EEPROM Usuário com o estado da arte em recursos de segurança.

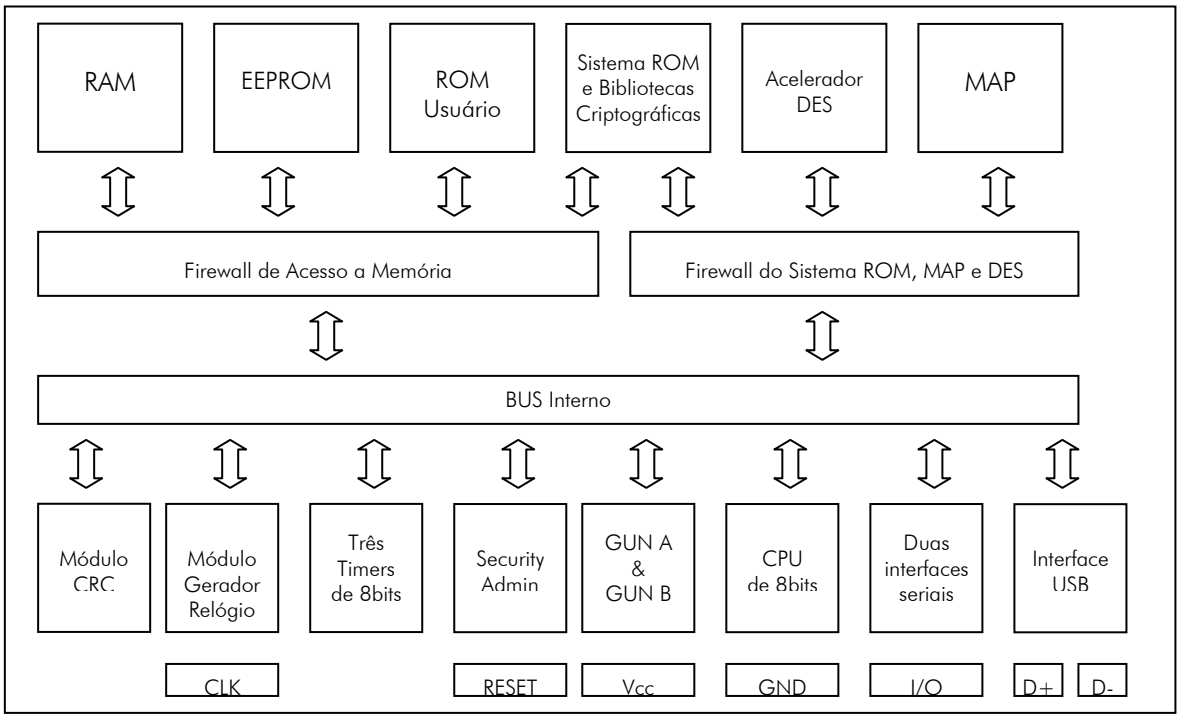
As memórias ROM, RAM e EEPROM podem ser configuradas com regras de acesso customizados. Acesso para qualquer área de memória para outra área está protegida por hardware firewalls. Regras de acesso são definidas pelo Usuário e podem ser selecionadas por opções de máscaras ou durante o ciclo de vida do produto.

O chip inclui um acelerador DES o qual é acessado via biblioteca de software do sistema criptográfico. Assim como os demais chips criptográficos, as interfaces seriais são plenamente compatíveis com o padrão ISO7816 para todas as aplicações smart card disponíveis.

Em adição, chip inclui uma interface serial USB e duas interfaces (I/O) seriais ISO7816-3. Um bloco de cálculo CRC também está disponível e disponível para acesso direto pelo Usuário. Por fim, este produto é fabricado usando a mais confiável tecnologia CMOS EEPROM.

Por fim, o chip criptográfico do ePass2000 provê um método para sobrescrever com zeros binários os valores de todas as chaves simétricas, chaves assimétricas privadas e PCSs. Após a conclusão desta operação de sobrescrita, as chaves eliminadas não podem mais ser acessadas.

5.3 Diagrama do Chip Criptográfico



No ePass2000 as chaves privadas dos certificados digitais são armazenadas em uma área de memória própria que só pode ser acessada quando o usuário se autentica no ePass2000 com o seu PIN (Personal Identification Number). O middleware do ePass2000 irá associar automaticamente o par de chaves gerado ao certificado digital.

O ePass2000 utiliza os algoritmos simétricos de criptografia DES e 3-DES (k1, k2 e k3) implementados no próprio hardware e isto garante a segurança dos pares de chaves armazenados no ePass2000 durante a execução de cálculos de criptografia. Para maiores informações sobre a cifragem das chaves privadas no ePass2000, solicite a Pronova Soluções Inteligentes o documento "Hardware Description".

A seguir os principais recursos oferecidos pelo Token USB ePass2000

- → Geração no próprio dispositivo (on board) do par de chaves RSA 1024 bits;
- → Suporte nativo para os algoritmos RSA, MD5, SHA1, DES e 3DES;
- → Suporte aos padrões Microsoft CAPI e PKCS#11;
- → Suporte ao mecanismo de autenticação tipo challenge/response (desafio/resposta)
- → CSP (Cryptographic Services Provider) para Windows
- → Compatível com Windows 2000 PC/SC;
- → Middleware para Windows e Linux
- → 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 1.0 compatível com 2.0;
- → Certificações CE, FCC, Microsoft WHQL, CFCA, OPSEC e FIPS (para o chip criptográfico);
- → Chassi de plástico resistente (tamper evident); resistente a água;
- → Capa protetora do conector USB;
- → Gerenciamento através de um PIN e de um PUK;
- → Software de Gerenciamento do dispositivo em Português do Brasil.

5.4 Especificações Técnicas

Sistemas Operacionais:	Windows 98SE, 2000, ME, XP**, 2003, Vista, MacOS 8/9/X e Linux (kernel 2.4 ou mais recente)
Navegadores Suportados	Microsoft Internet Explorer 5.5 (e superiores), Netscape Navigator e Mozilla Firefox 1.5 e versões mais recentes.
Certificações e Padrões:	PKCS#11 v2.10, MS CAPI, PC/SC, X.509 v3, SSL v3, IPSec/IKE, ISO 7816 3-4, FCC, CE, CFCA, OPSEC e FIPS 140-2
Processador:	8 bits
Memória:	32 KB
Algoritmos On-Board:	RSA, DES, 3DES, DAS, MD5 e SHA-1
Nível de Segurança do Chip:	Armazenamento de dados seguro e criptografado
Dimensões:	50mm x 17mm x 7mm
Peso:	6g
Dissipação de Energia:	< 250 mW
Temperatura de Operação:	0 até 70°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, 1.0 compatível com 2.0
Chassi:	Plástico reforçado, à prova de violação (tamper evident)
Retenção de Dados de memória:	10 anos
Capa protetora do conector USB	Sim
Número Serial impresso no chassi	Sim
LED	Sim

** Com exceção a edição Starter Edition, o qual, segundo a Microsoft Brasil, não possui o serviço cartão inteligente disponível para instalação. A versão do driver está disponível para 32bits e 64bits.

5.5 Requisitos mínimos do sistema:

Para que seja possível fazer uso do ePass2000, verifique se seu sistema possui os seguintes requisitos mínimos:

Sistema Operacional	Windows 98SE, ME, 2000, 2003, XP**, Vista**, MacOS 8/9/X ou Linux (kernel 2.4 ou mais recente).
Serviço Cartão Inteligente	O sistema operacional deverá oferecer suporte ao serviço cartão inteligente (smart card) para que seja possível a utilização do Token USB ePass2000.
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

5.6 Vantagens do Token USB ePass2000

- Conexão direta na porta USB sem interface intermediária para leitura;
- Altos Níveis de Segurança: a função criptográfica on board do dispositivo, baseada no algoritmo RSA, é muito mais segura que uma solução baseada em software. Toda informação sensível permanece armazenada na memória protegida do dispositivo. Todas as operações de assinatura e criptografia são realizadas dentro do dispositivo. A chave privada NUNCA deixa a memória segura do dispositivo, o que garante que ela não será copiada por um hacker, por exemplo. A avançada tecnologia de encapsulamento do chip também garante a segurança física dos dados armazenados no módulo criptográfico.
- Integração Transparente: são oferecidos dois padrões industriais reconhecidos: PKCS#11 e Microsoft Crypto API. O Token USB pode ser integrado com qualquer aplicação com qualquer um destes padrões. Além disso, este dispositivo é otimizado para trabalhar com soluções de software de terceiros. Em adição, o ePass2000 possui memória segura para armazenar simultaneamente certificados digitais, chaves privadas, senhas e outras credenciais pessoais, ou seja, suporte a múltiplas aplicações PKI.
- Exportação automática de certificados armazenados para o certificate store dos sistemas operacionais Windows 98SE, Windows ME, Windows 2000, Windows XP e versões mais recentes;
- Alta confiabilidade: o ePass2000 pode armazenar de forma segura credenciais por pelo menos 10 anos.

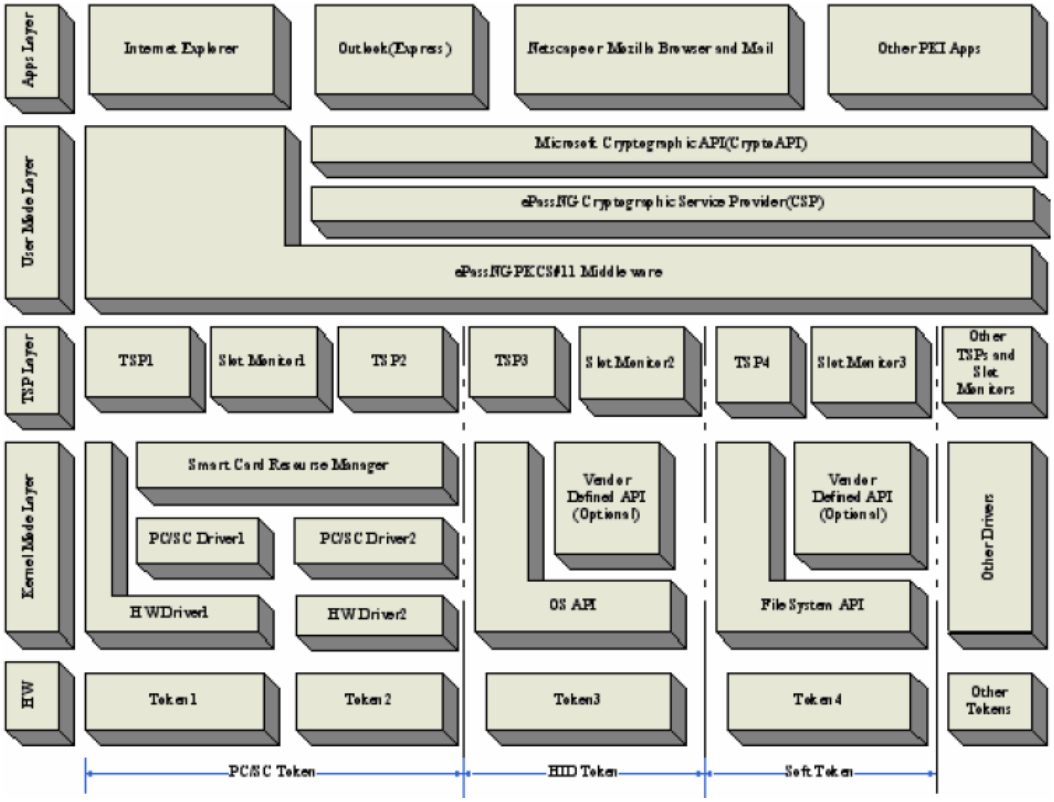
5.7 Recursos do Hardware

- Criptografia: o dispositivo suporta os seguintes algoritmos: RSA 1024 bits (assinatura e verificação), DES e 3DES; SHA-1 e MD5.
- Geração do par de chaves: o par de chaves RSA é gerado no próprio dispositivo e este processo não dura mais que 20 segundos.
- Gerador de números aleatórios: o dispositivo faz uso de um gerador de números aleatórios real para criar o par de chaves e o MAC (Message Authentication Code).
- Acesso multi-nível: existem 16 níveis de acesso do sistema de arquivos do ePass2000. O sistema de arquivos permite que usuários definam um ou mais privilégios de segurança para o gerenciamento de chave.

5.8 Arquitetura ePassNG

O framework ePassNG oferece interfaces de programação padrão PKCS$#11 e Microsoft Crypto API para a camada superior de aplicações PKI. ISVs podem desenvolver suas próprias aplicações PKI baseadas nestas interfaces. Além disso, as interfaces providas pelo framework ePassNG podem ser integradas de forma transparente com qualquer aplicação padrão PKI através de simples configuração.

A seguir uma breve descrição do framework ePassNG.



A arquitetura do sistema consiste em cinco camadas, a saber: Hardware, Núcleo do Driver, Abstrata do Hardware, Interface de Aplicação e Aplicação.

Camada Hardware: esta camada é a infra-estrutura de toda a arquitetura. Ela contém vários tokens incluindo seus circuitos de hardware, programas firmware e fios. Qualquer tipo de token em conformidade com o padrão PC/SC pode ser suportado por esta camada de hardware, como por exemplo, o ePass1000, o ePass2000_FT11, o ePass2000_FT12, o ePass3000, o ePass3000ND e vários outros leitores de smart card e combinações de smart cards e tokens USB de terceiros. Seu recurso comum é estar apto a ser controlado através do sistema de operação do Gerenciador de Recursos Smart Card. Tokens também podem ser dispositivos HID (Human Interface Device), como por exemplo, o ePassND (chave USB introduzida pela Feitian, a qual dispensa a instalação de driver. ND significa non-driver), flash memory USB e arquivos uniformes no disco rígido. Diferentes tipos de tokens ou múltiplos tokens do mesmo tipo podem trabalhar juntos.

Camada Núcleo do Driver: esta camada é responsável pelo gerenciamento das comunicações de dados e pedidos do acesso dos processos da camada TSP entre o computador cliente e a camada de Hardware. Para tokens do tipo PC/SC esta camada funciona como um driver de hardware, driver PC/SC e operação de sistema de Gerenciador de Recursos Smart Card. Para tokens do tipo HID, esta camada pode ser tratada como sistema de operação de drivers built-in.

Camada Abstrata do Hardware: esta camada prove a interface abstrata padrão para a camada Interface de Aplicação. Comunicações entre o computador e diferentes dispositivos (incluindo token) usam a mesma interface provida por esta camada. Este projeto oculta de forma eficaz a diferença entre hardwares. A implementação de software desta camada é chamada TSP (Token Service Provider).

Camada Interface de Aplicação: esta camada prove as implementações dos padrões das interfaces PKCS#11 e Microsoft Crypto API para a camada superior de aplicações PKI. Além disso, interface de aplicação PC/SC em conformidade com o padrão Microsoft ® PC/SC também é oferecida. Desenvolvedores podem escrever aplicações com seu conjunto familiar de funções PC/SC. Esta interface é independente da plataforma e pode ser aplicada em todas as plataformas compatíveis com ePassNG.

Camada Aplicação: esta camada oferece várias aplicações ePassNG e outras aplicações, pois ePassNG oferece diferentes tipos de padrões de interfaces de programação; ela é compatível com a maioria das aplicações existentes e além disso, desenvolvedores podem usar os conjuntos de interfaces familiares para projetarem suas próprias aplicações.

5.9 O que é o PUK (PIN Unlock Key)

NOTA: o valor do PUK do ePass2000 até 09/07/2006 era "rockey" (sem as aspas). A partir de 10/07/2007 com a introdução runtime versão 1.0.6.710, o valor de fábrica do PUK foi alterado para "12345678"(sem as aspas). Esta modificação foi realizada para atender aos requisitos II.11 e II.16 do Manual de Condutas Técnicas – Volume I - Detalhamento dos Requisitos Técnicos para Cartões Inteligentes (Smart Cards), Leitoras de Cartões Inteligentes e Tokens Criptográficos no âmbito da ICP-Brasil.

O PUK (PIN Unlock Key) é a senha máster que permite ao usuário recuperar o PIN do Usuário e, também formatar o setor PKI do ePass2000. O valor de fábrica é "12345678" (sem as aspas). Por questões de segurança, este PIN Unlock Key possui um número máximo de tentativas de acerto. *Tenha cuidado para não exceder as 5 (cinco) tentativas,* pois se o PUK for travado, será necessário reinicializar o ePass2000 com uma ferramenta chamada ePassNG Init[1], a qual irá apagar todo o conteúdo que estiver armazenado no seu ePass2000.

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.

[1] O instalador desta ferramenta se encontra no diretório FORMATADOR do CD-ROM de instalação!

5.10 O que é o PIN do Usuário?

NOTA: o valor do PIN do ePass2000 até 09/07/2006 era "1234" (sem as aspas). A partir de 10/07/2007 com a introdução runtime versão 1.0.6.710, o valor de fábrica do PIN foi alterado para "12345678"(sem as aspas). Esta modificação foi realizada para atender aos requisitos II.4 e II.16 do Manual de Condutas Técnicas – Volume I - Detalhamento dos Requisitos Técnicos para Cartões Inteligentes (Smart Cards), Leitoras de Cartões Inteligentes e Tokens Criptográficos no âmbito da ICP-Brasil.

O PIN do Usuário 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 do Usuário é "12345678" (sem as aspas) e da mesma forma que o PUK, também existe um número determinado de acertos desta senha, mas neste caso podem ser feitas até 5 (cinco) tentativas consecutivas de acerto desta senha. Ao contrário do PUK, você poderá destravar o PIN do Usuário (mais informações, consulte o tópico "Gerenciador PKI - Destravando o PIN").

Conforme normas estabelecidas pelo Comitê Gestor da ICP-Brasil, o PIN do ePass2000 poderá conter caracteres alfanuméricos, com suporte ao idioma Português do Brasil.

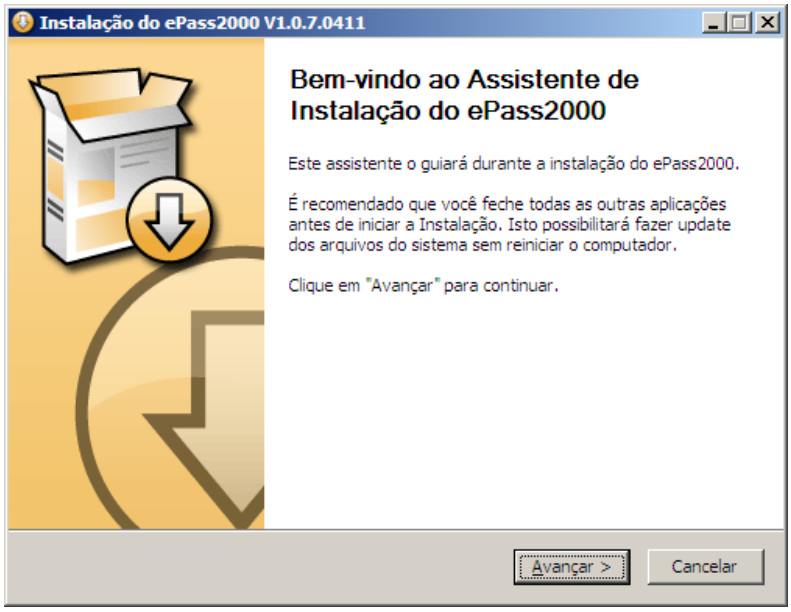
6. Instalando o software do Token USB ePass2000

6.1 Instalação nos sistemas Windows 2000, Windows XP, Windows Vista e Windows 2003

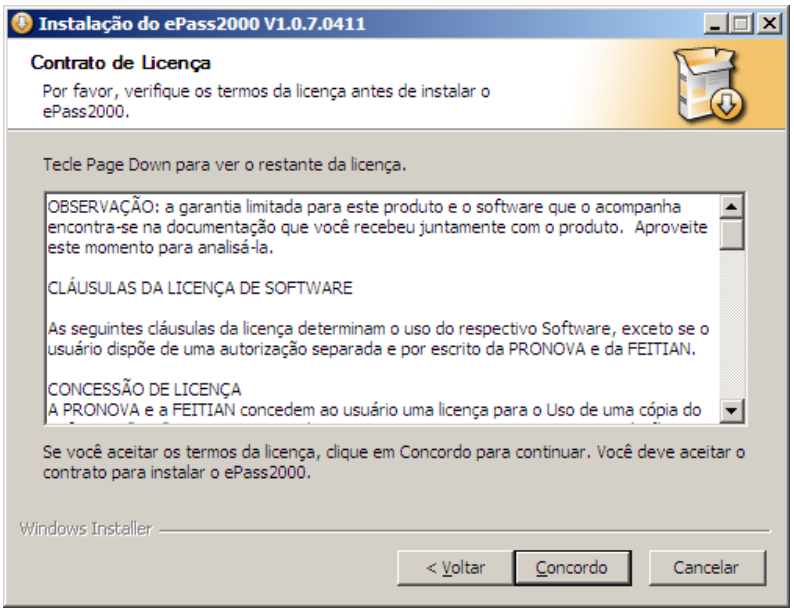
Para instalar o software do ePass2000, basta inserir CD-ROM fornecido, aguardar a execução do Instalador e seguir as instruções abaixo detalhadas. Se você não possui o CD-ROM, entre em contato com a Pronova Soluções Inteligentes e solicite o instalador.

Nota: se sua unidade de CD-ROM estiver com a função execução automática desabilitada, certamente será necessário executar de forma manual o arquivo ePass2000.exe.

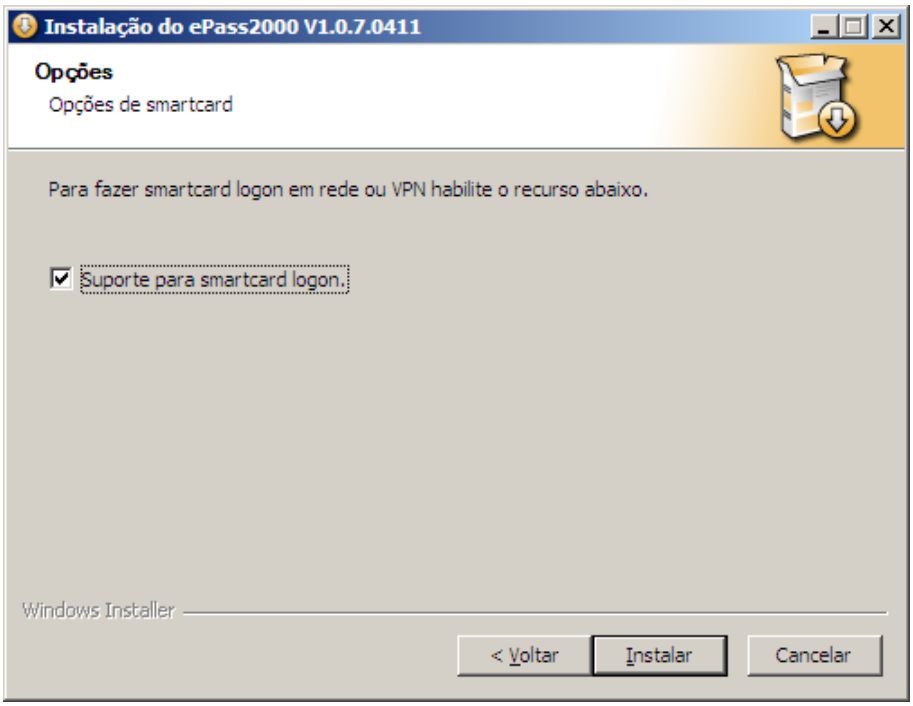
a) Clique no botão "Avançar" da janela de boas vindas



b) Para continuar com a instalação, leia com atenção o Contrato de Licença e clique no botão "Concordo".

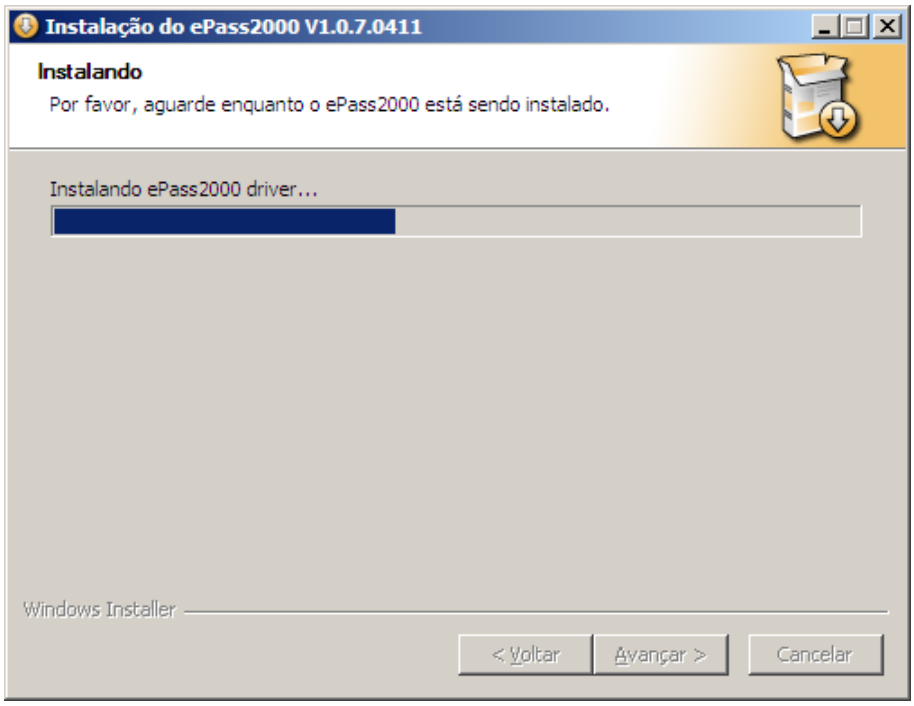


c) Se for fazer logon em rede ou VPN usando o Token como um cartão inteligente, habilite a opção "Suporte para sistema de smartcard logon em rede ou VPN". Caso contrário não habilite esta opção*. Para continuar clique no botão "Instalar".

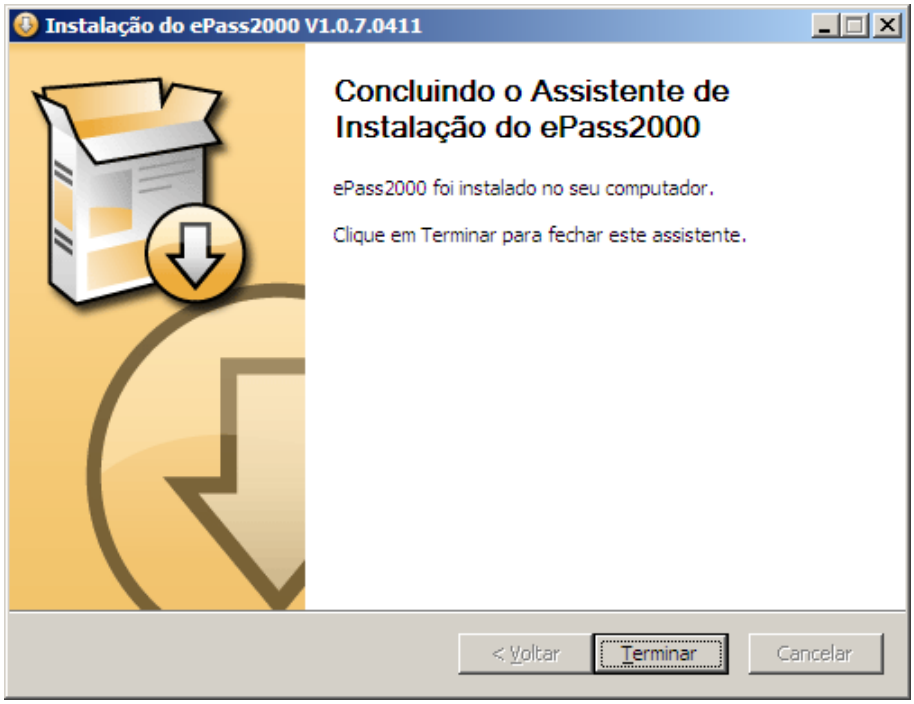


* Para fazer smartcard logon é necessário ter um certificado digital para esta finalidade. Ressaltamos ainda que esta funcionalidade somente é suportada nos sistemas operacionais Windows 2000, XP e 2003. Com relação a VPN, para esta integração ocorrer é necessário que o cliente de VPN da sua solução de firewall já esteja instalado e configurado.

c) Aguarde que o instalador copie para a sua máquina os arquivos necessários para utilizar o ePass2000;



d) Clique no botão "Terminar" para concluir a instalação do Runtime e reiniciar o seu computador, caso seja necessário.



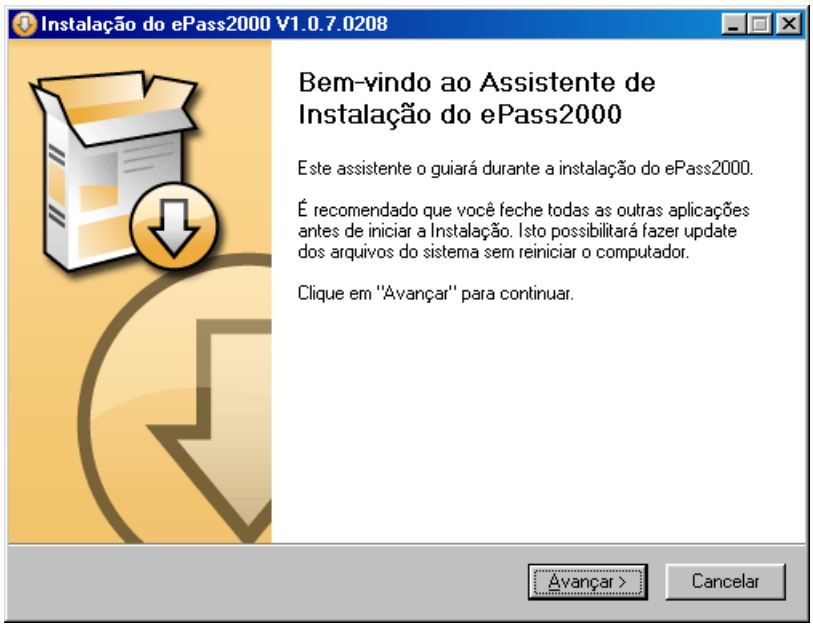
e) Ao final do novo boot, conecte o seu ePass2000 em uma porta USB livre e aguarde que o sistema operacional reconheça este novo hardware. Durante o processo de reconhecimento do novo hardware o LED (luz) do ePass2000 ficará piscando.

6.2 Instalação nos sistemas Windows 98SE e Windows ME

Para instalar o software do ePass2000, 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.

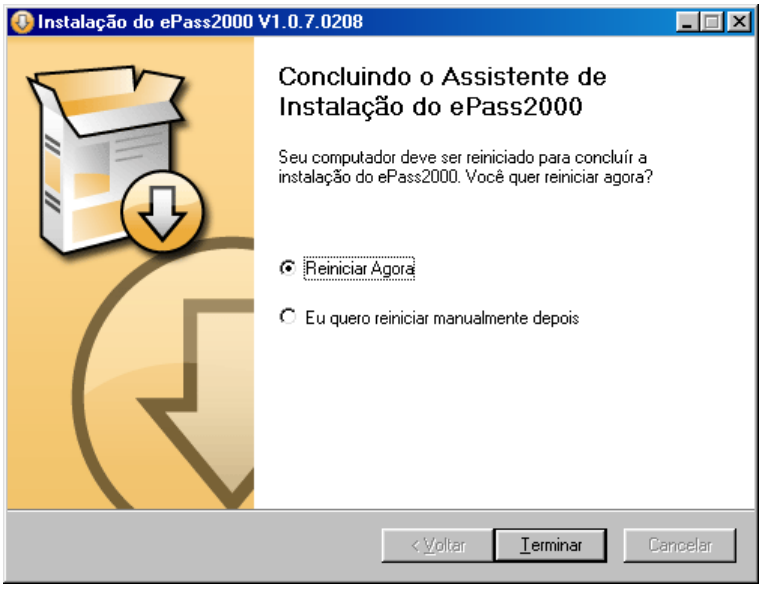
Nota: se sua unidade de CD-ROM estiver com a função autorun desabilitada, certamente será necessário executar de forma manual o arquivo ePass2000.exe.

a) Clique no botão "Avançar" da janela de boas vindas



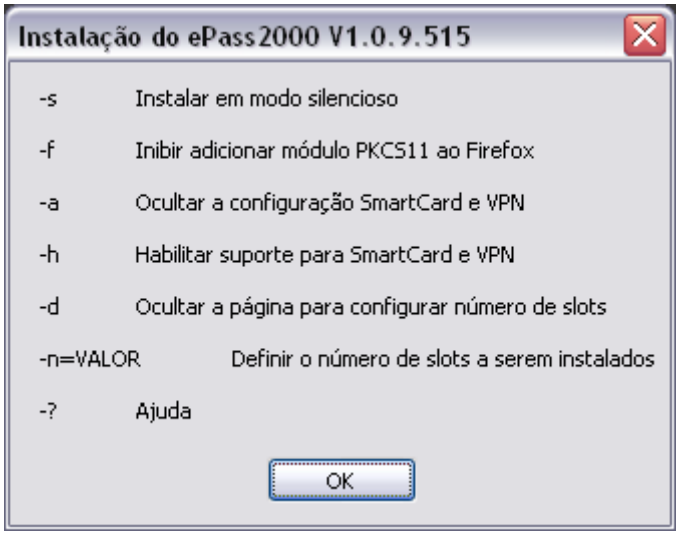
b) Aguarde que o instalador copie para a sua máquina os arquivos necessários para utilizar o ePass2000, bem como o sistema operacional reconheça os novos recursos que estão sendo instalados;

c) Clique no botão "Terminar" para concluir a instalação do Runtime e reiniciar o seu computador.



6.3 Instalação por linha de comando

Para os administradores de rede que necessitem fazer a instalação do software do ePass2000 através de scritps, o instalador do ePass2000 suporta a execução através de linha de comando. Os seguintes parâmetros hoje oferecidos são:



Com base nestas informações, se você desejar instalar o software do ePass2000 em modo silencioso, basta adicionar o parâmetro –s ao final da sintaxe de execução.

6.4 Instalando o ePass2000 em máquinas com Linux

- Copiar do CD de instalação ou baixar o pacote de instalação a partir da página de downloads do site da PRONOVA;
- Descompactar o pacote de instalação copiado do CD de instalação ou baixado do site da PRONOVA;
- Abrir uma tela do terminal;
- Logar como usuário root. Normalmente é usado o comando sudo su;
- Ir até o diretório criado pela descompactação do arquivo;
- No diretório raiz criado pela descompactação do arquivo, executar o comando ./install
- Ao final da instalação, reiniciar o computador;
- Ao final do novo boot, conectar o Token ePass2000 a uma porta USB livre;

Procedimentos Adicionais

- Abrir o arquivo instpk.html com o navegador Mozilla Firefox. Este arquivo responsável pela adição do Módulo PKCS#11 do ePass2000 estará no diretório Doc abaixo da raiz do diretório criado a partir da descompactação do arquivo que será baixado do site da PRONOVA.
- Adicionar a cadeia de certificados da Autoridade Certificadora que emitiu o certificado digital que está armazenado no ePass2000. Estas instruções DEVEM ser obtidas com o suporte técnico da Autoridade Certificadora.

NOTA: o middleware do ePass2000 para Linux oferece integração de certificados armazenados no dispositivo com o NSS (Network Security Services) no ambiente Linux Kernel 2.4 ou versões mais recentes e estáveis.

6.5 Instalando o ePass2000 em máquinas com Mac OS

- Copiar do CD de instalação ou baixar o pacote de instalação a partir da página de downloads do site da PRONOVA;
- Descompactar o pacote de instalação copiado do CD de instalação ou baixado do site da PRONOVA;
- Abrir uma tela do terminal;
- Logar como usuário root. Normalmente é usado o comando sudo su;
- Ir até o diretório criado pela descompactação do arquivo;
- No diretório raiz criado pela descompactação do arquivo, executar o comando ./install
- Ao final da instalação, reiniciar o computador;
- Ao final do novo boot, conectar o Token ePass2000 a uma porta USB livre;

Procedimentos Adicionais

- Abrir o arquivo instpk.html com o navegador Mozilla Firefox. Este arquivo responsável pela adição do Módulo PKCS#11 do ePass2000 estará na raiz do diretório criado a partir da descompactação do arquivo que será baixado do site da PRONOVA.
- Adicionar a cadeia de certificados da Autoridade Certificadora que emitiu o certificado digital que está armazenado no ePass2000. Estas instruções DEVEM ser obtidas com o suporte técnico da Autoridade Certificadora.

6.6 Monitor de Certificados - Configurando o Tempo de Vida do PIN através

Você poderá definir o tempo de vida do PIN do seu ePass2000. Este recurso pode ser configurado a partir do ícone do Monitor de Certificados que está localizado na área de notificação do Windows. Para dar início a configuração, com o seu dispositivo conectado em uma porta USB, dê dois cliques no ícone do Monitor de Certificados do ePass2000.

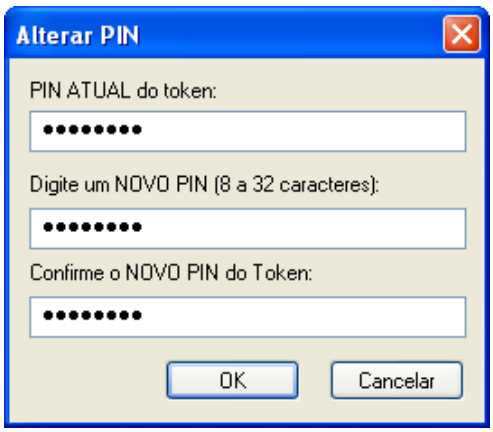
Na janela do Monitor de Certificados do ePass2000, dê um clique no botão "PIN Timeout"

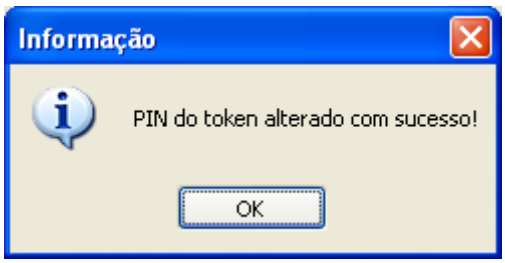
Na janela "Configuração do Tempo de Vida do PIN", selecione a opção "Tornar o PIN do Token inativo após" e no campo a seguir digite o valor em minutos desejado. Para concluir esta operação, clique no botão "OK".

6.7 Monitor de Certificados - Alterando o PIN

Sempre que você desejar, você poderá usar o botão "Alterar PIN" disponível no Monitor de Certificados para proceder a alteração do PIN do seu ePass2000. Este recurso pode ser configurado a partir do ícone do Monitor de Certificados que está localizado na área de notificação do Windows. Para alterar o PIN, com o seu dispositivo conectado em uma porta USB, dê dois cliques no ícone do Monitor de Certificados do ePass2000. Na janela do Monitor de Certificados do ePass2000, dê um clique no botão "Alterar PIN"

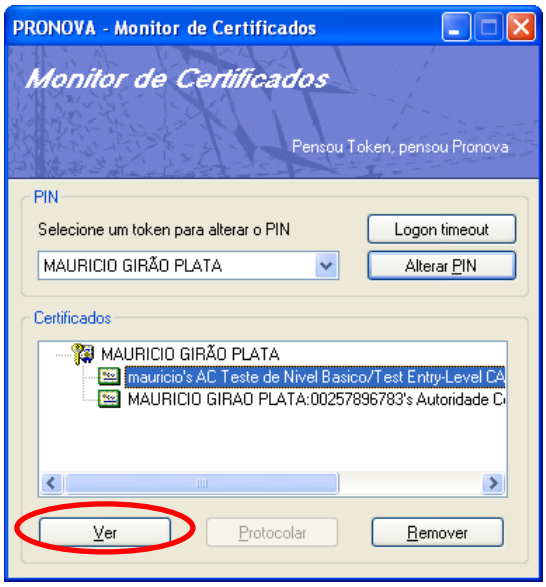
Na janela "Alterar PIN", digite o Atual PIN do seu ePass2000. Nos campos seguintes digite o NOVO PIN para o seu ePass2000. Para concluir esta operação, clique no botão "OK". Se os dados informados estiverem corretos, você irá visualizar a mensagem de que o PIN foi alterado com sucesso.





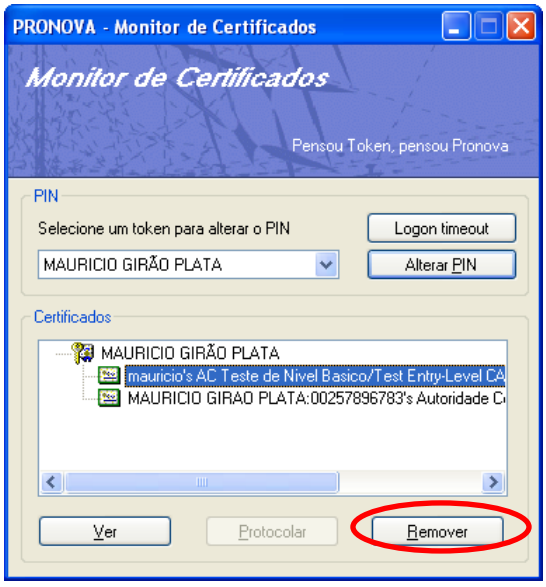
6.8 Monitor de Certificados – Visualizando Detalhes do Certificado

Você poderá usar o botão "Ver" disponível no Monitor de Certificados para visualizar os detalhes gerais de cada certificado que estiver armazenado no seu ePass2000. Com o seu dispositivo conectado em uma porta USB, dê dois cliques no ícone do Monitor de Certificados do ePass2000 e na janela do Monitor de Certificados do ePass2000, selecione o seu certificado e dê um clique no botão "Ver"



6.9 Monitor de Certificados – Removendo um Certificado do Repositório do Windows

Todos os certificados armazenados no ePass2000 são automaticamente transferidos para o repositório do Windows quando o Token ePass2000 é conectado a porta USB do computador. Todavia, se você desejar que nem todos os certificados sejam transferidos automaticamente, você poderá fazer uso do recurso "Remover" do Monitor de Certificados. Para isso, com o seu dispositivo conectado em uma porta USB, dê dois cliques no ícone do Monitor de Certificados do ePass2000. Na janela do Monitor de Certificados do ePass2000, selecione o seu certificado e dê um clique no botão "Remover"



NOTA: o uso deste recurso não exclui nenhum certificado digital ou informação armazenada na memória do ePass2000.

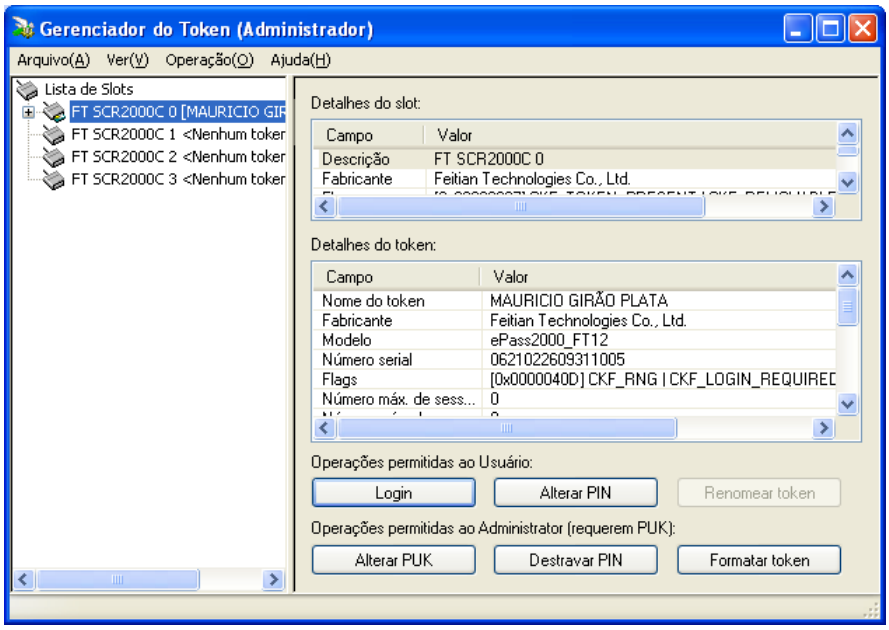
6.10 Monitor de Certificados – Devolvendo um Certificado do Repositório do Windows

Sempre que você selecionar um certificado e o botão "Protocolar" estiver habilitado, isso é sinal que o certificado não está sendo transferido de forma automática para o repositório do Windows. Para que este certificado volte a ser transferido automaticamente para o repositório do Windows, selecione-o e depois clique no botão "Protocolar".

NOTA: o uso deste recurso não exclui nenhum certificado digital ou informação armazenada na memória do ePass2000.

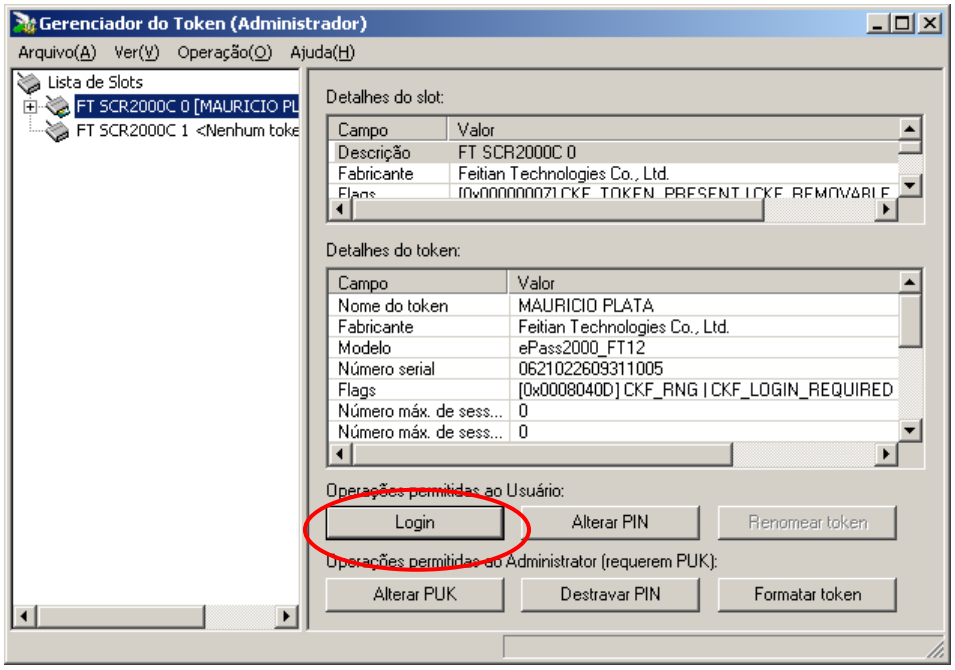
7. Gerenciador PKI do ePass2000

O Gerenciador PKI do ePass2000 é uma ferramenta de administração que possui duas versões, uma para Administradores e outra para Usuários. A versão para Administradores possui todas as funções que requerem que o uso do PUK (PIN Unlock Key). A versão para Usuários, possui as funções que requerem apenas o PIN (Personal Identification Number) com o detalhe de não permitir que nenhum dado armazenado no ePass2000 seja excluído.



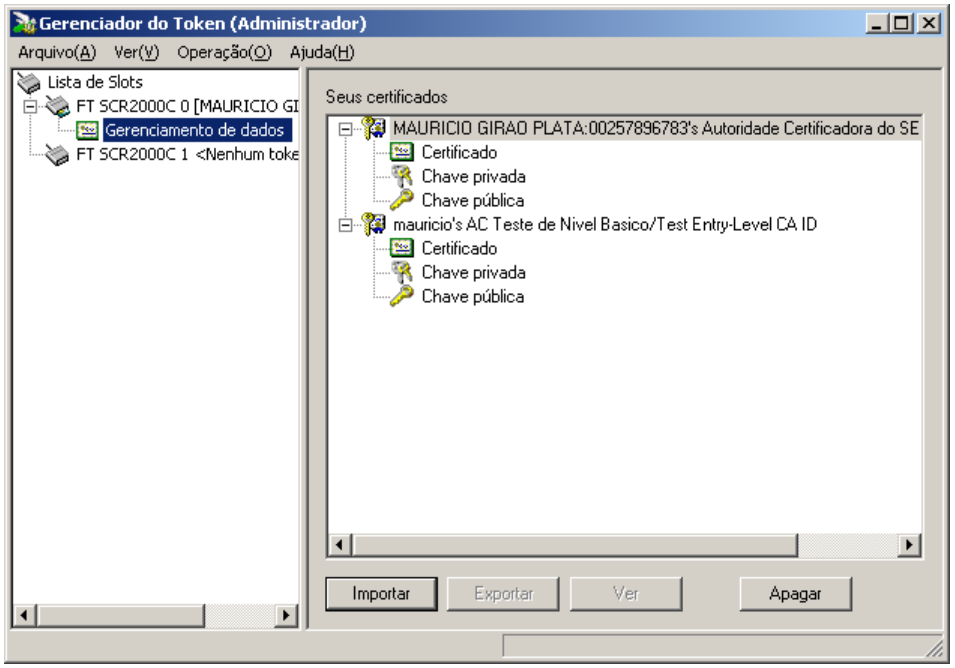
7.1 Gerenciador PKI – Login

A Função "Login" do Gerenciador PKI é a porta de entrada para permitir o acesso do usuário do ePass2000 aos dados privados que estão armazenados na memória protegida e também a função "Renomear token".



7.1.1 Visualizando certificados e dados gravados no Token ePass2000

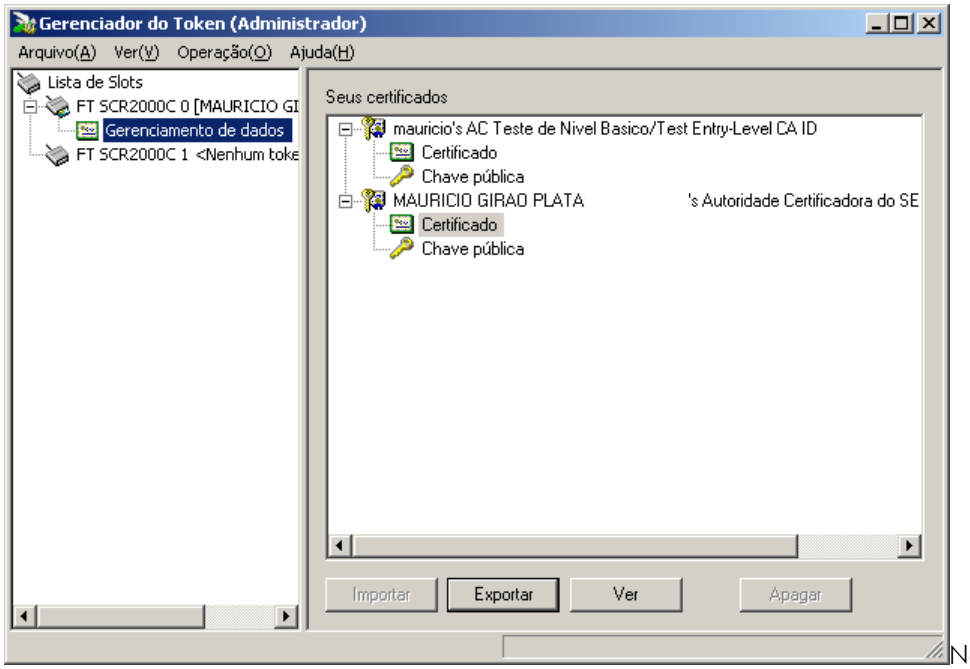
Uma vez autenticado no ePass2000, ou seja, depois de ter clicado no botão "Login" e de ter digitado o PIN do ePass2000, o usuário é redirecionado para a área "Seus certificados", como ilustrado na imagem abaixo.



Autenticado

Se você não se autenticar, ou seja, se não clicar no botão "Login" e clicar diretamente em Gerenciamento de Dados, você não irá visualizar as chaves privadas armazenadas no seu ePass2000, como ilustrado na imagem abaixo.

Destacamos que quando você não está autenticado, os únicos botões que ficarão habilitados ao clicar em um objeto exibido são "Exportar" e "Ver"

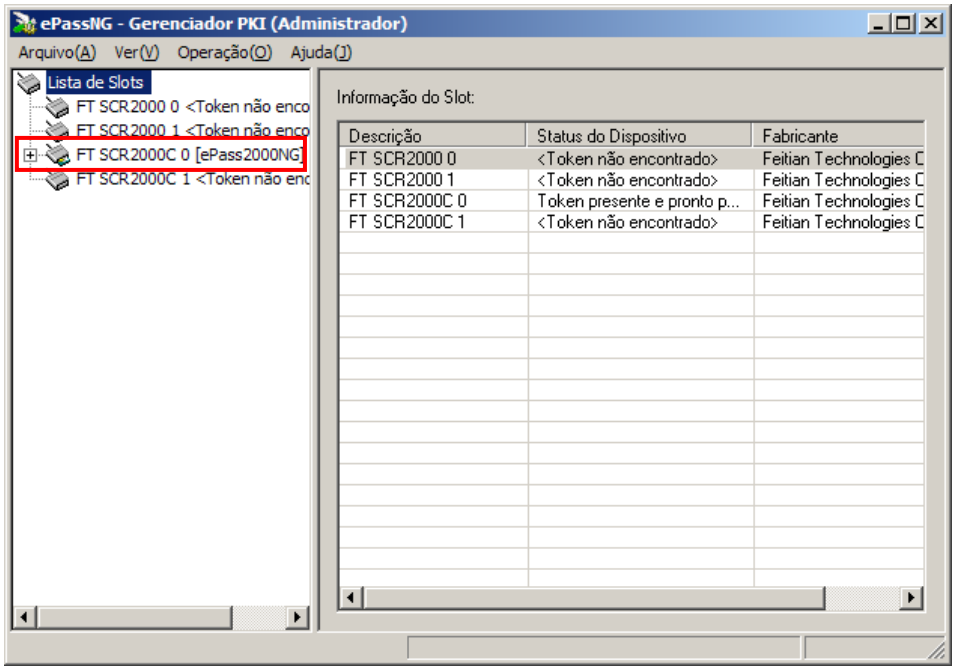


Não autenticado

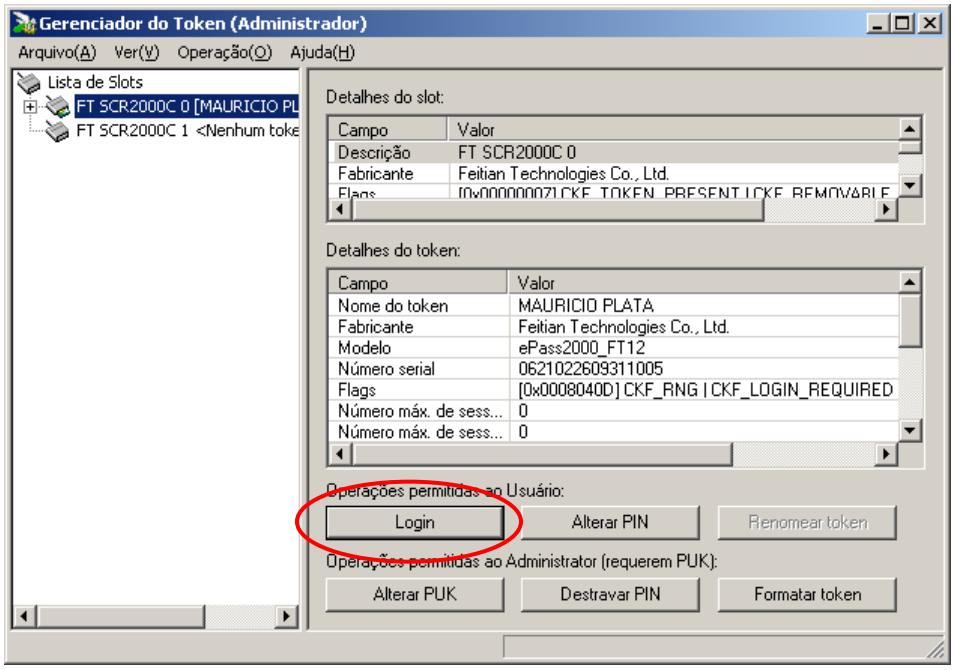
Se você desejar exportar a parte pública de seu certificado digital do Token para um arquivo .CER, basta selecionar o seu certificado e em seguida clicar no botão "Exportar" e seguir as instruções do Gerenciador PKI do ePass2000.

7.1.2 Excluindo dados gravados no Token ePass2000

Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | Pronova | ePassNG | Gerenciador do Token. Clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas.

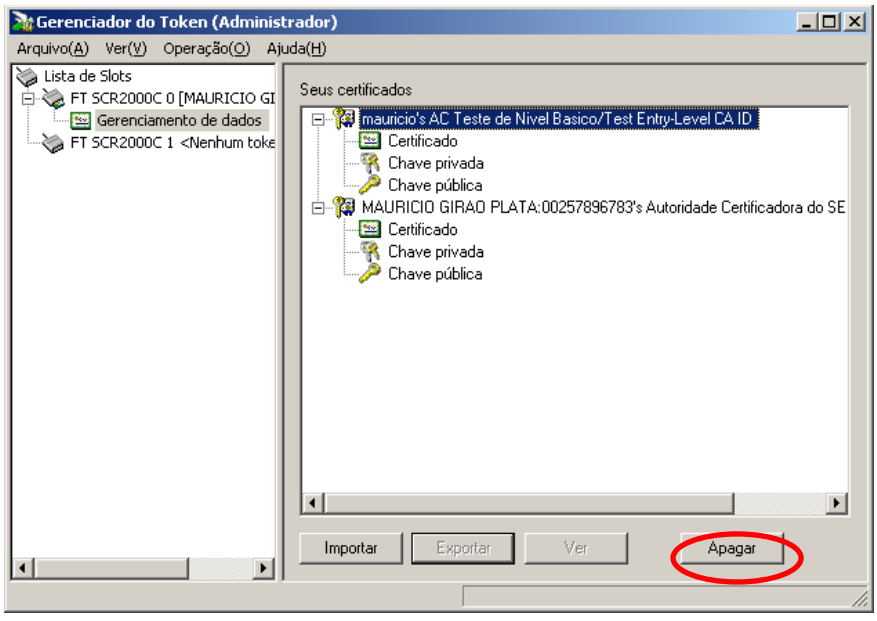


Para ter uma visão total de todos os dados, você terá que se autenticar no ePass2000. Clique no botão 'Login' e em seguida informe o PIN do seu ePass2000.

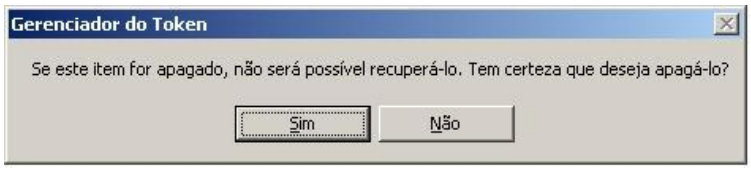


Uma vez autenticado, você será redirecionado automaticamente para a área Gerenciamento de dados. Se você não se autenticar e clicar diretamente em Gerenciamento de Dados, *você não irá visualizar* as chaves privadas armazenadas no seu ePass2000.

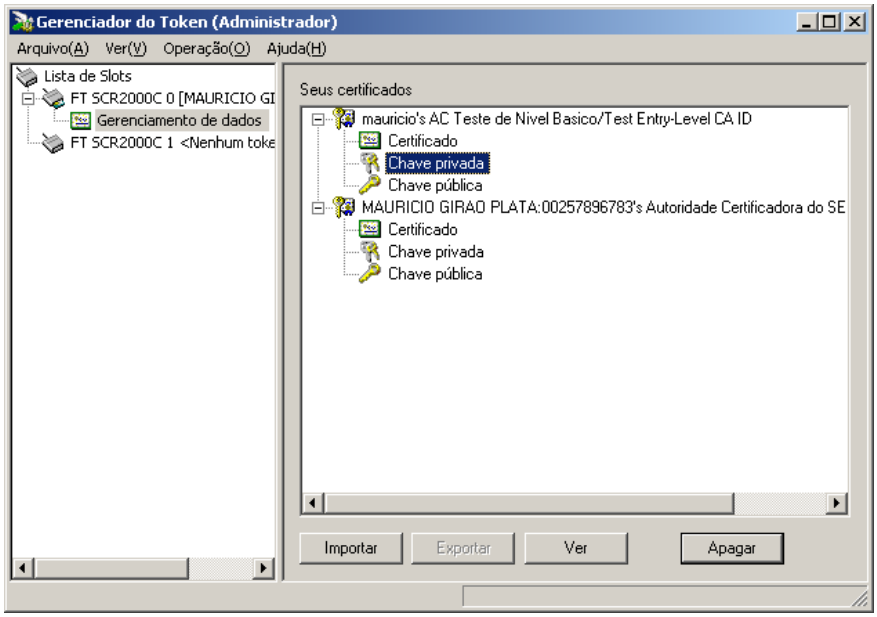
Para apagar um certificado digital e seu respectivo par de chaves, selecione o topo da estrutura e a seguir clique no botão "Apagar"



O Gerenciador irá alertar você com relação a este procedimento. Se você estiver certo, clique no botão "Sim" do contrário, clique no botão "Não".



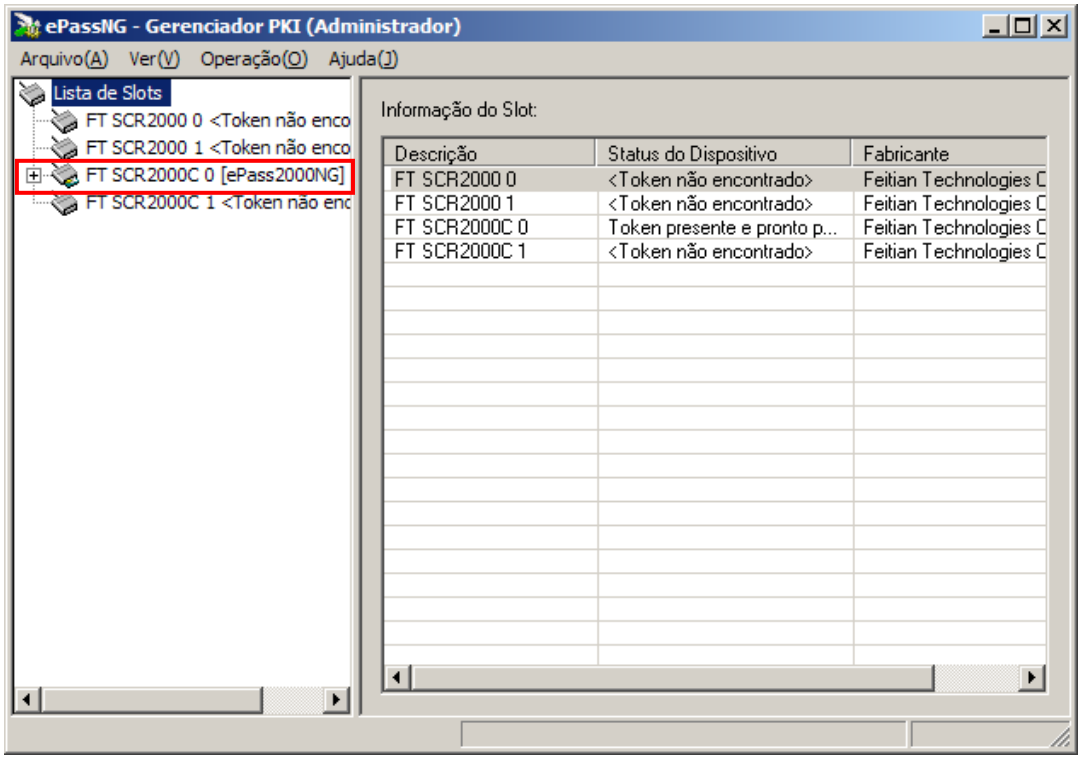
Se desejar apagar um objeto específico, selecione apenas este objeto e clique no botão “Apagar”



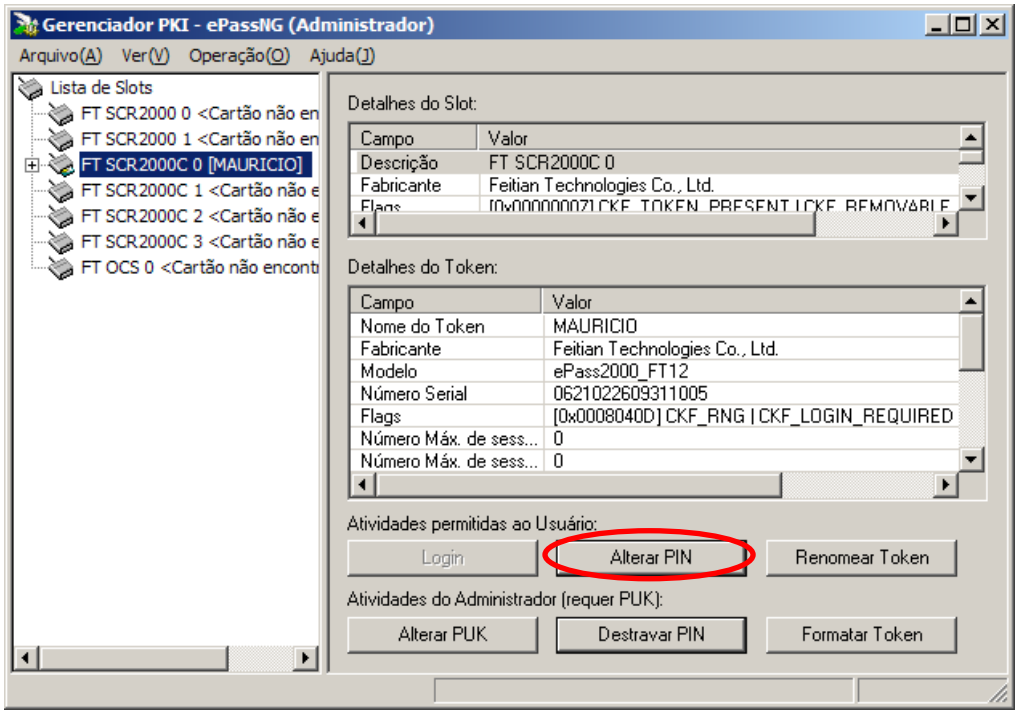
7.2 Gerenciador PKI – Alterar PIN

Para alterar o PIN do Usuário, siga as instruções a seguir:

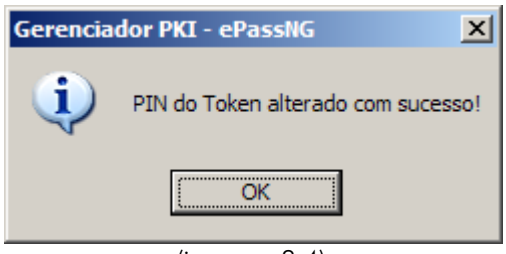
Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | Pronova | ePassNG | Gerenciador do Token. A seguir, clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas.



Clique no botão 'Alterar PIN' para ter acesso a janela 'Alterar PIN'.



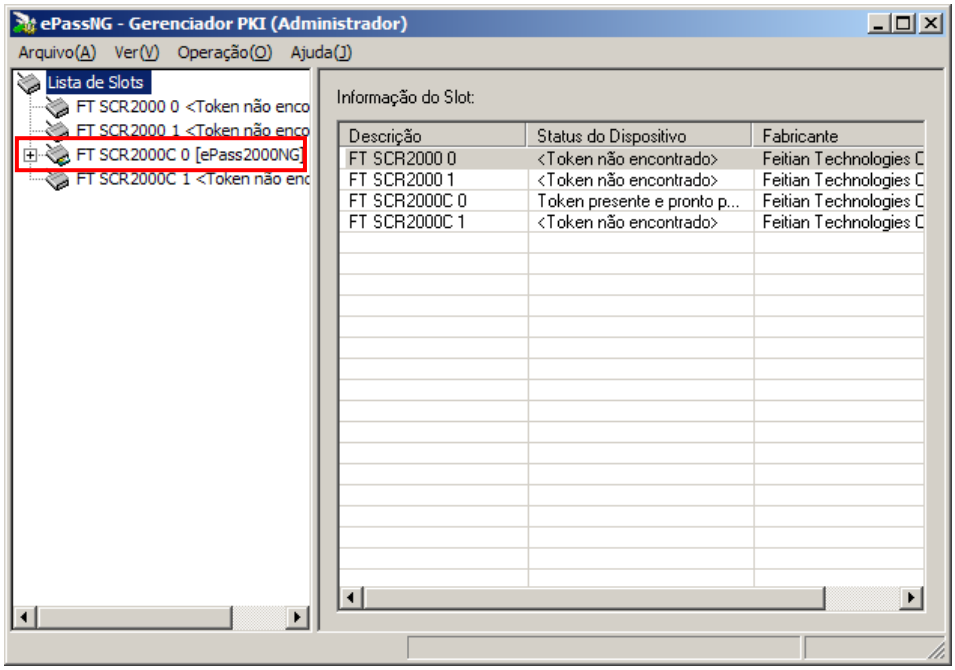
Se você estiver usando seu ePass2000 pela primeira vez, certamente ele ainda deverá estar com o PIN de fábrica que é "12345678" (sem as aspas). Neste caso, no campo 'Digite o ATUAL PIN', digite *12345678* e nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN' digite o PIN mais apropriado para você. Por questões de segurança, recomendamos que este PIN tenha no mínimo 8 caracteres e que seja composto de letras e números. Depois de preencher todos os campos clique no botão OK e aguarde que a mensagem 'PIN alterado com sucesso!' seja exibida (imagem 8.4).



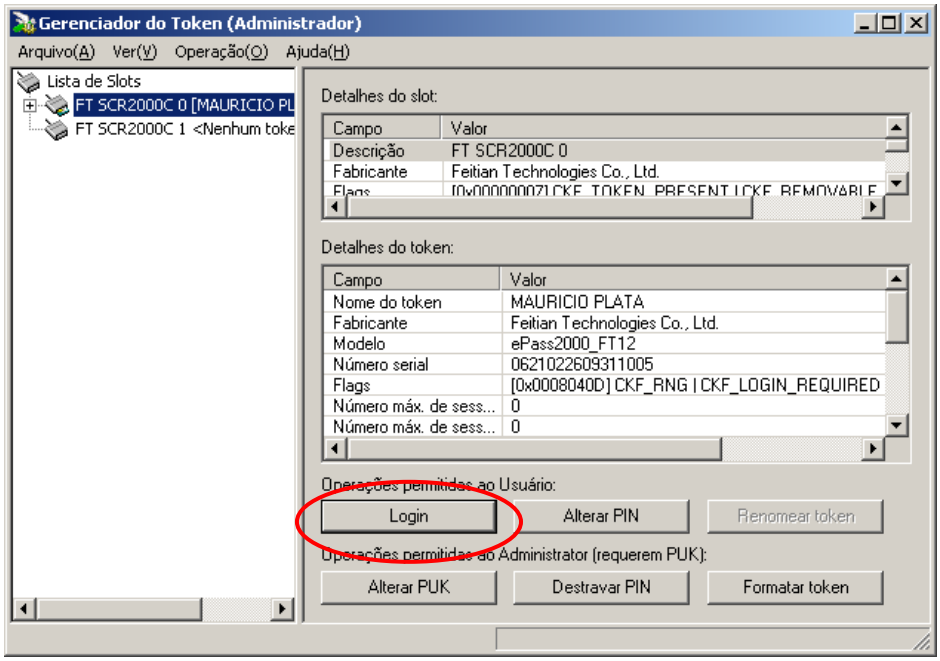
(imagem 8.4)

7.3 Gerenciador PKI – Renomear Token

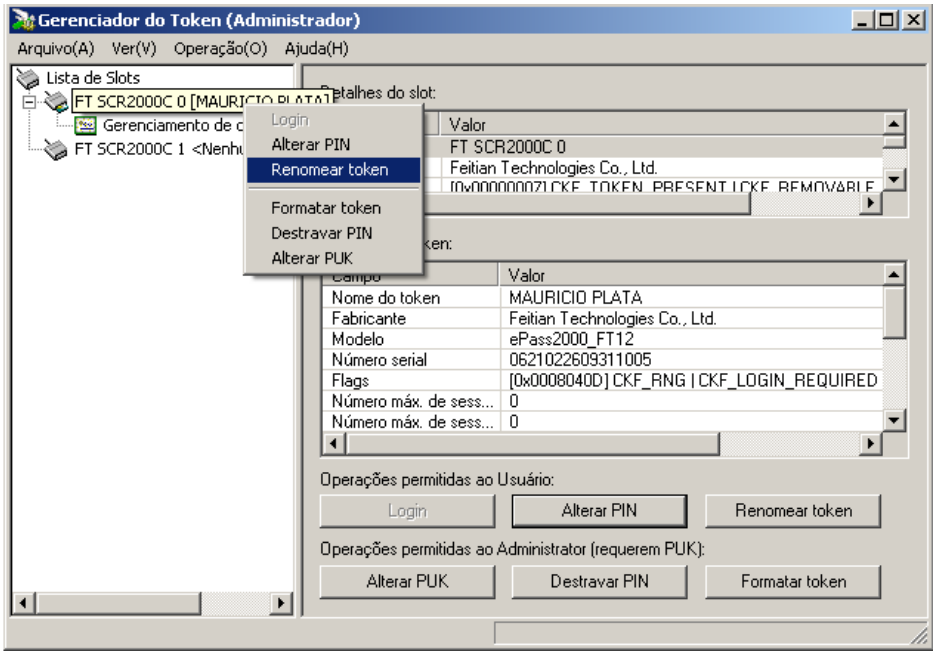
Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | Pronova | ePassNG | Gerenciador do Token. Clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas.



Esta função somente ficará habilitada, após a sua autenticação no dispositivo. Clique no botão 'Login' e em seguida informe o PIN do seu ePass2000.



Uma vez autenticado no ePass2000, clique com o botão direito do mouse no slot do seu Token e em seguida selecione a opção "Renomear token"

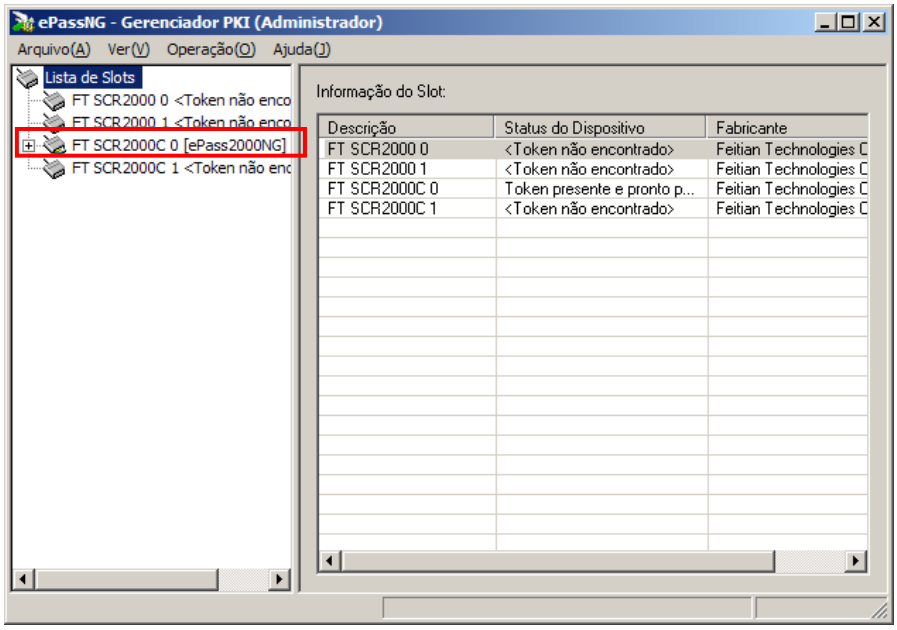


Na janela "Renomear token, digite o novo nome (label) para o ePass2000 e clique no botão OK.

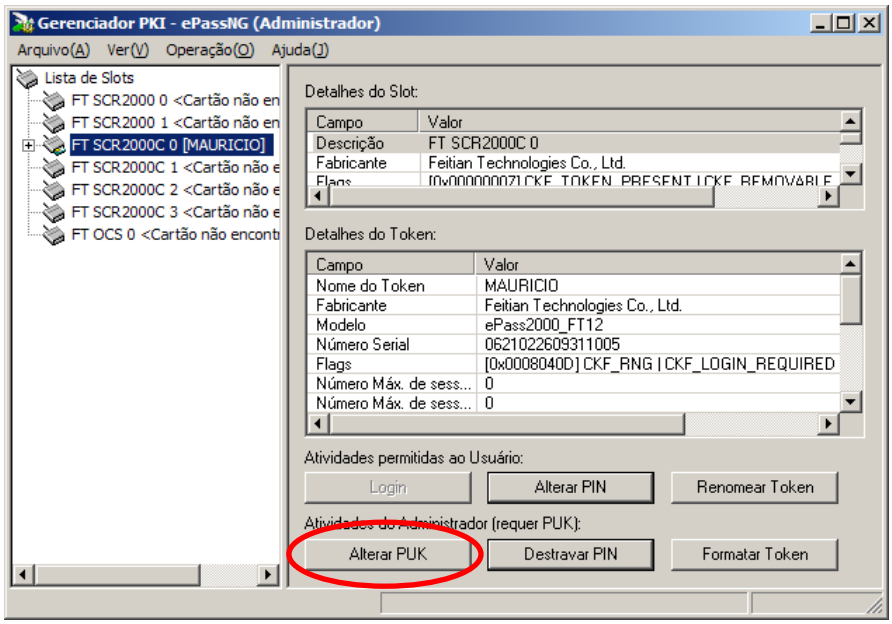
Ao final, você receberá visualizará a mensagem de que a operação foi realizada com sucesso.

7.4 Gerenciador PKI – Alterar PUK

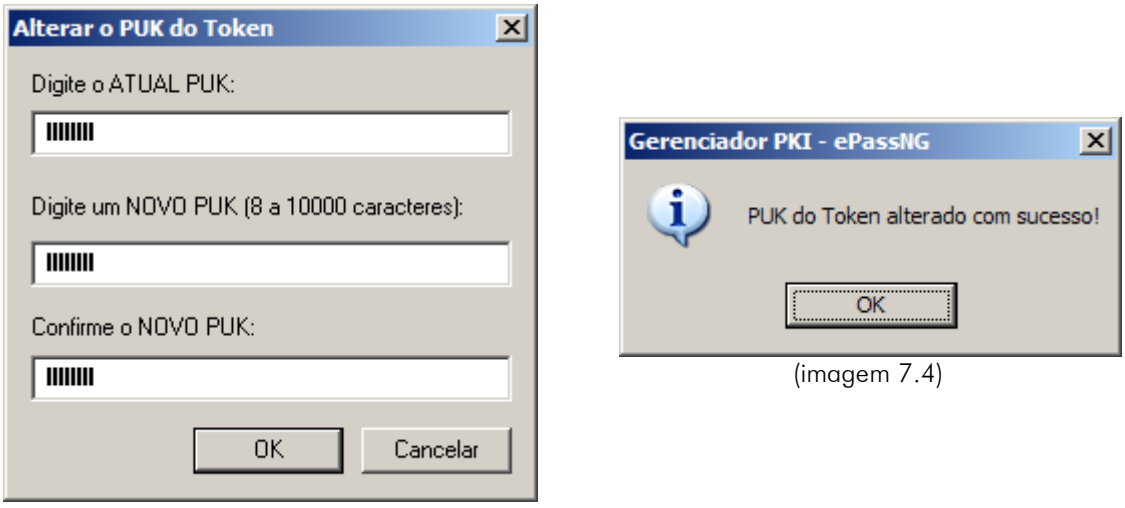
Esta é uma tarefa muito simples. Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | Pronova | ePassNG | Gerenciador do Token. No Gerenciador, clique no slot referente ao seu ePass2000.



Clique no botão "Alterar PUK" ter acesso à janela "Alterar PUK"



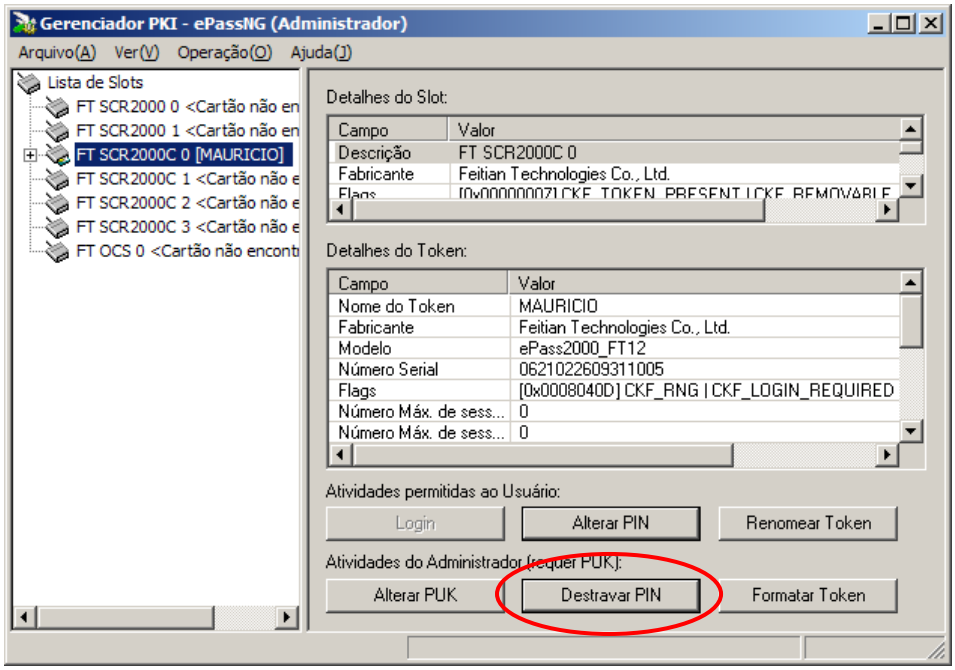
Se esta for a sua primeira utilização, no campo 'Digite o ATUAL PUK', digite *12345678* que é o valor de fábrica do PUK. No campo 'Digite um NOVO PUK' digite o valor que você deseja para o seu dispositivo. Confirme este valor no campo 'Confirme o NOVO PUK'. Para concluir esta operação, clique no botão "OK" e aguarde a exibição da mensagem "PUK do Token alterado com sucesso" (imagem 7.4):



(imagem 7.4)

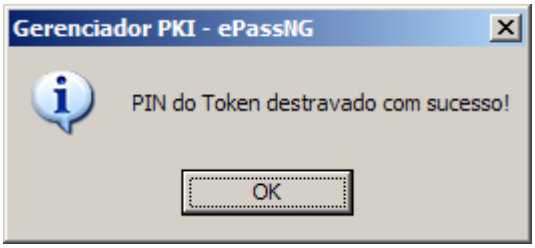
7.5 Gerenciador PKI – Destravar PIN

Se o número de tentativas de acerto do PIN foi excedido, você terá que usar a função "Destravar PIN" para definir um novo PIN. Com o seu dispositivo conectado, execute o Gerenciador do ePass2000, clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas. Depois, clique no botão 'Destravar PIN' para ter acesso a janela 'Destravar PIN do Usuário'



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 será totalmente travado e será necessário re-formatar o seu ePass2000, perdendo assim todas as informações que estão armazenadas no equipamento.

No campo 'Digite o PUK do Token', digite o PUK do seu dispositivo. Nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN' digite um novo PIN para o seu ePass2000. Após preencher todos os campos, clique no botão OK e aguarde que a mensagem 'PIN do Token destravado com sucesso!' (imagem 8.1.4).

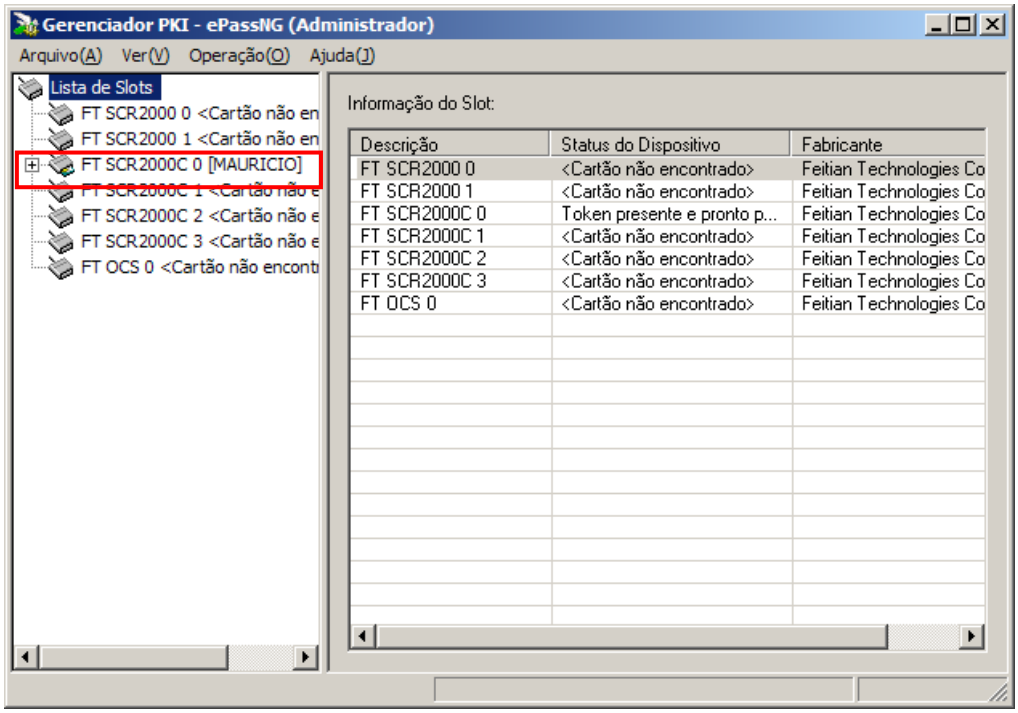


(imagem 8.1.4)

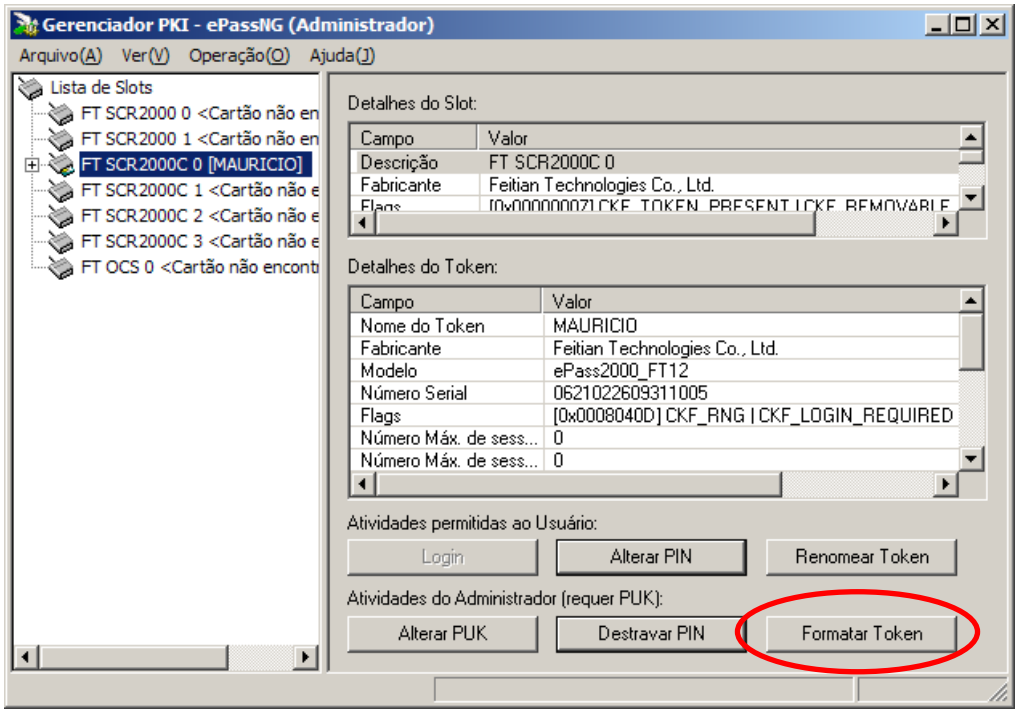
7.6 Gerenciador PKI – Formatar Token

Sempre que você julgar necessário apagar todo o conteúdo (certificados e chaves criptográficas) do ePass2000, faça uso do recurso "Formatar Token" do Gerenciador. Para tal, execute-o a partir do atalho criado no Grupo Pronova que pode ser acessado a partir do botão "Iniciar do Windows. Clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas

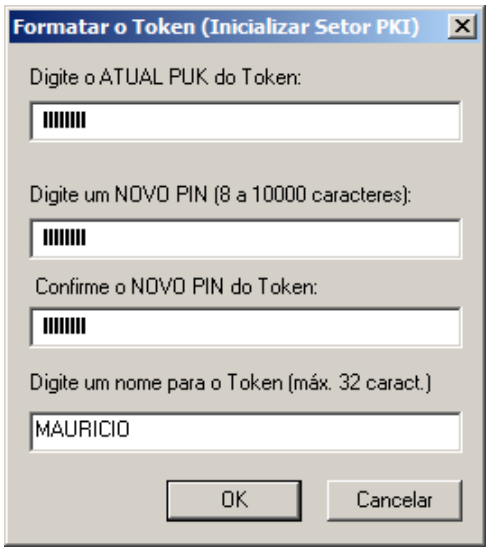
ATENÇÃO: esta é uma ação irreversível e que vai apagar todas as informações que estiverem armazenadas no ePass2000.

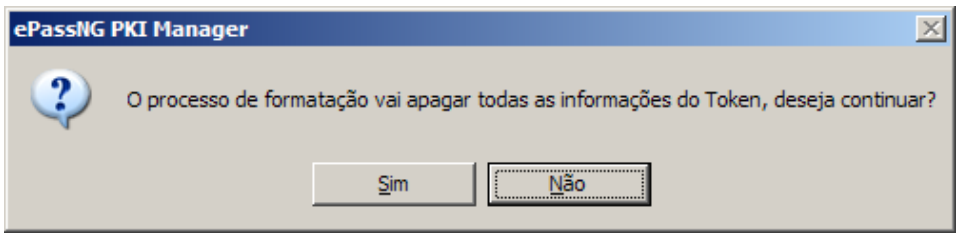


Clique no botão 'Formatar Token' para ter acesso a janela 'Formatar o Token (Inicializar Setor PKI)'.



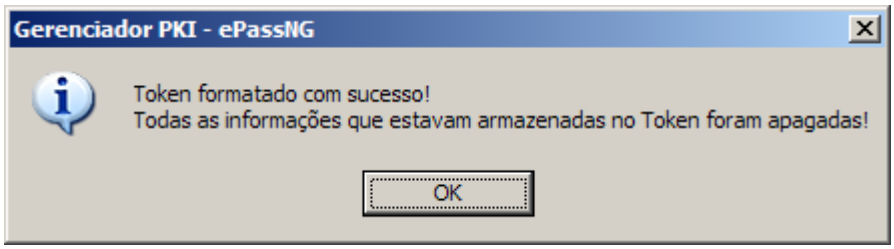
No campo 'Digite o ATUAL PUK do Token' digite o PUK. Nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN', digite um novo PIN para o seu ePass2000. Se desejar que o seu dispositivo tenha um nome específico, digite o nome desejado no campo 'Digite um nome para o Token'. Depois de preencher todos os campos, clique no botão "OK". Uma janela (imagem 9.4) informando que o processo vai apagar todas as informações do Token será exibida. Se você estiver certo de que deseja apagar TODOS os dados que estão armazenados no equipamento, clique no botão 'Sim' para continuar. Do contrário, clique no botão 'Não' para cancelar a operação.





(imagem 9.4)

Se você clicou no botão 'Sim' a mensagem "Token formatado com sucesso! Todas as informações que estavam armazenadas no Token foram apagadas" será exibida (imagem 9.5).



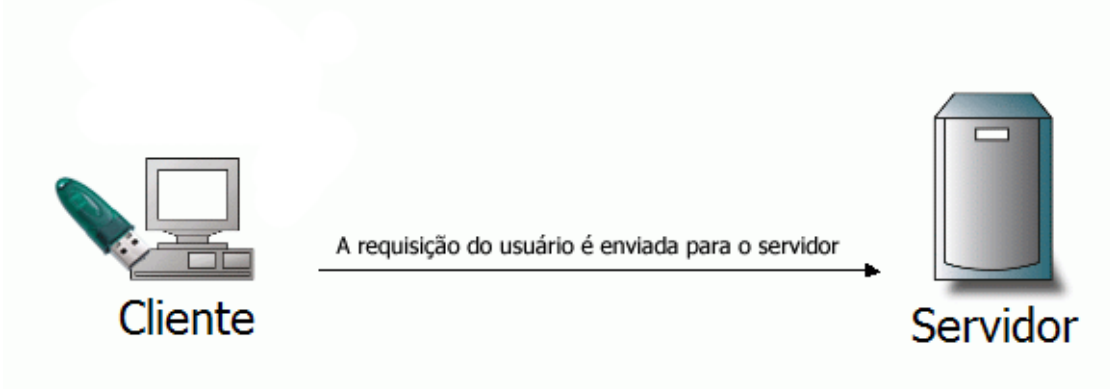
(imagem 9.5)

8. Suporte ao Mecanismo de chalenge/response (desafio/resposta)

O ePass2000 é um Token USB que suporta mecanismo de desafio/resposta. A seguir ilustraremos com funciona este mecanismo com a utilização do algoritmo MD5.

(1)

(2)



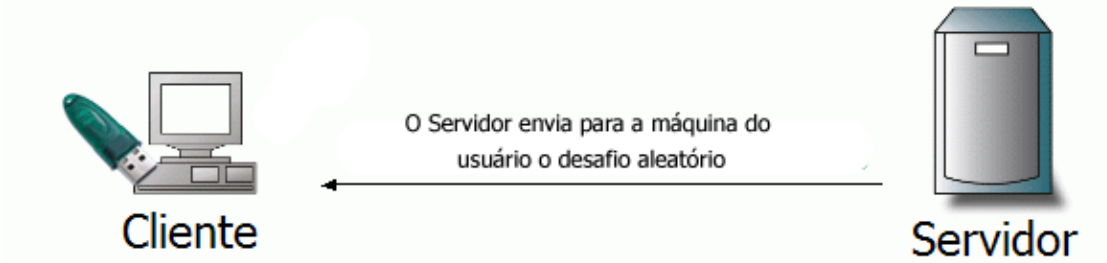
(3)


O Servidor recebe
a requisição
Cliente
Servidor

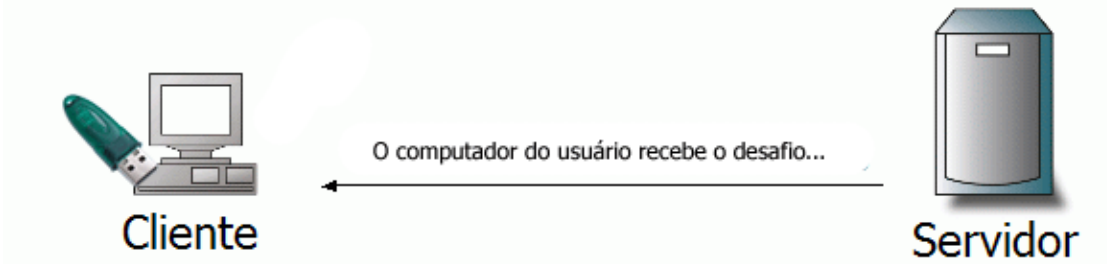
(4)


Assim que o pedido é recebido,
este gera e prepara o envio de
um desafio aleatório
Cliente
Servidor

(5)


O Servidor envia para a máquina do
usuário o desafio aleatório
Cliente
Servidor

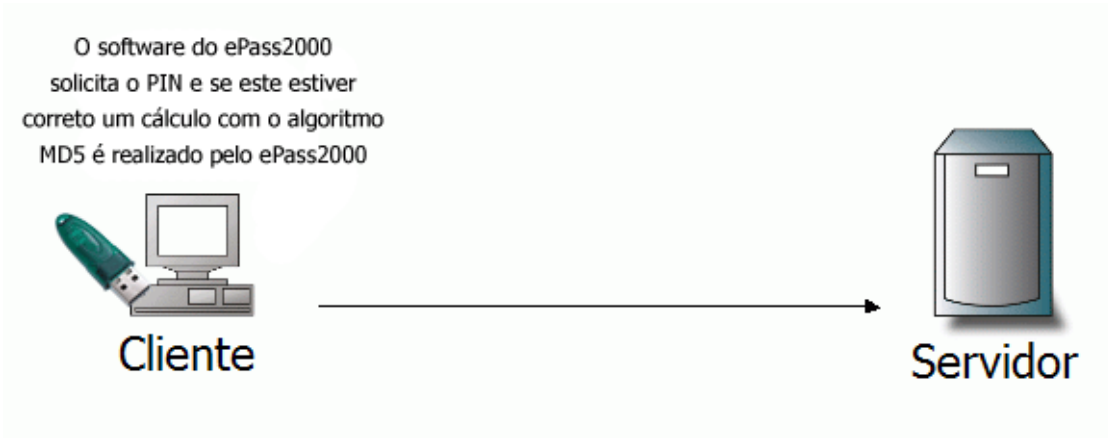
(6)


O computador do usuário recebe o desafio...
Cliente
Servidor

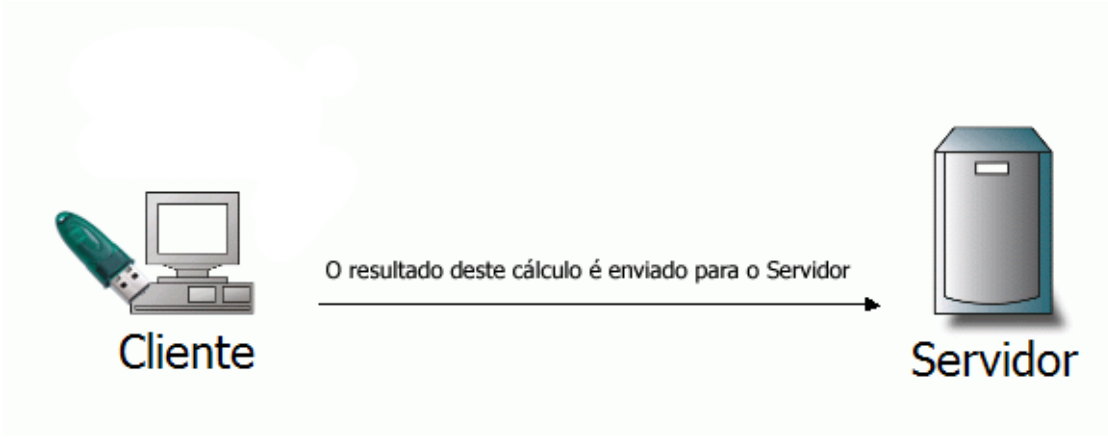
(7)


E este desafio é encaminhado
para o ePass2000
Cliente
Servidor

(8)


O software do ePass2000
solicita o PIN e se este estiver
correto um cálculo com o algoritmo
MD5 é realizado pelo ePass2000
Cliente
Servidor

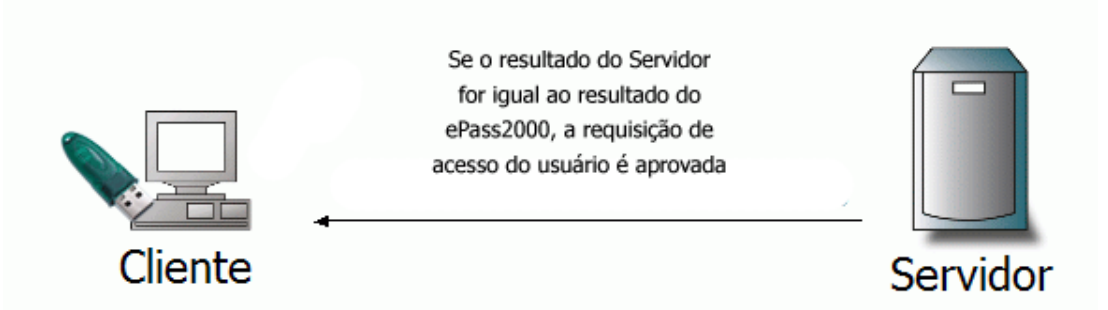
(9)


O resultado deste cálculo é enviado para o Servidor
Cliente
Servidor

(10)


O Servidor realiza o
mesmo cálculo com o
algoritmo MD5
Cliente
Servidor

(11)


Se o resultado do Servidor
for igual ao resultado do
ePass2000, a requisição de
acesso do usuário é aprovada
Cliente
Servidor

10. Instalando um certificado digital emitido por uma Autoridade Certificadora (AC) Microsoft no ePass2000

Este tópico foi escrito para demonstrar o suporte do ePass2000 ao padrão Microsoft Crypto API, como também para apresentar ao usuário do ePass2000 o CSP (Cryptographic Service Provider – Provedor de Soluções de Criptografia), o qual é requerido por autoridades certificadoras no âmbito da ICP-Brasil para a solicitar e gravar o certificado digital, além de gerar o par de chaves de criptografia RSA

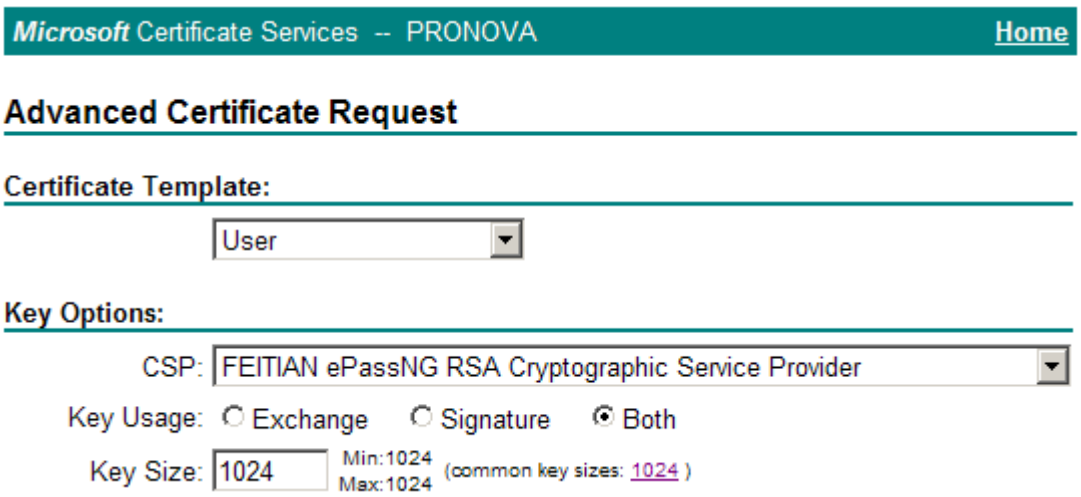
ATENÇÃO: você apenas poderá executar os passos descritos neste tópico se você ou sua empresa possuir um servidor Windows 2000 ou Windows 2003 com o serviço Autoridade Certificadora (Certificate Authority) instalado e configurado. *Se você não possui esta estrutura instalada em sua rede, procure uma Autoridade Certificadora credenciada à ICP-Brasil. Maiores informações sobre as ACs credenciadas à ICP-Brasil, consulte* www.iti.gov.br e os nossos boletins técnicos que estão disponíveis no CD-ROM de instalação.

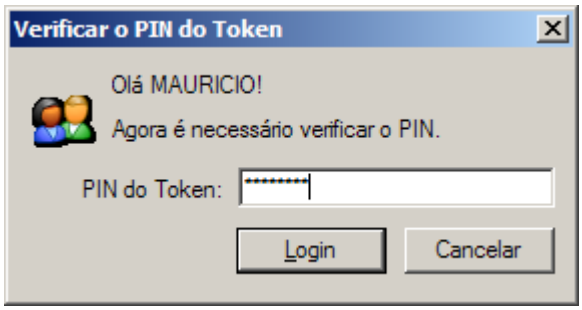
Instalar um certificado digital no ePass2000 é uma tarefa muito simples. Entretanto, é importante ressaltar que o processo deverá ser concluído no mesmo computador onde o processo de solicitação foi iniciado.

Você poderá instalar qualquer certificado digital cujo par de chaves seja de até 1024bits, inclusive ICP-Brasil (desde que solicitado a partir de uma AC credenciada a ICP-Brasil), mas é necessário aqui estar atento à capacidade de armazenamento do seu dispositivo, ou seja, a quantidade de certificados armazenados vai variar do tamanho destes e da memória de 32K do seu ePass2000. Com o seu dispositivo conectado em uma porta USB, acesse a página web onde será feita a solicitação do certificado digital.

Nosso exemplo fará uso da Autoridade Certificadora PRONOVA que roda em uma plataforma Microsoft. Não registraremos aqui neste guia as telas iniciais onde o usuário informa o nome, o e-mail, telefone e demais dados cadastrais.

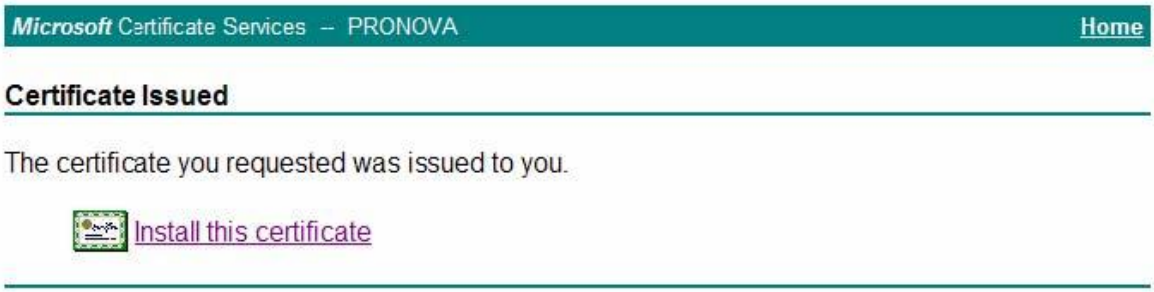
Apresentaremos o processo a partir da tela onde o usuário terá que selecionar o CSP (Cryptographic Solution Provider) do dispositivo. Na imagem abaixo, note que estamos selecionando a opção "FEITIAN ePassNG RSA Cryptographic Service Provider".





Ao clicar no botão "Submit" da página de solicitação do certificado digital, uma tela solicitando o PIN do Usuário irá surgir. Informe o PIN e clique no botão "Login".

Se o PIN informado for o correto, observe as mensagens que serão exibidas na área de notificação do Windows. Ao informar PIN correto o par de chaves será gerado dentro do seu ePass2000 e ao término deste processo o usuário é encaminhado para a próxima página.



Para concluir a instalação, clique no link "Install this certificate" e a próxima página será exibida.

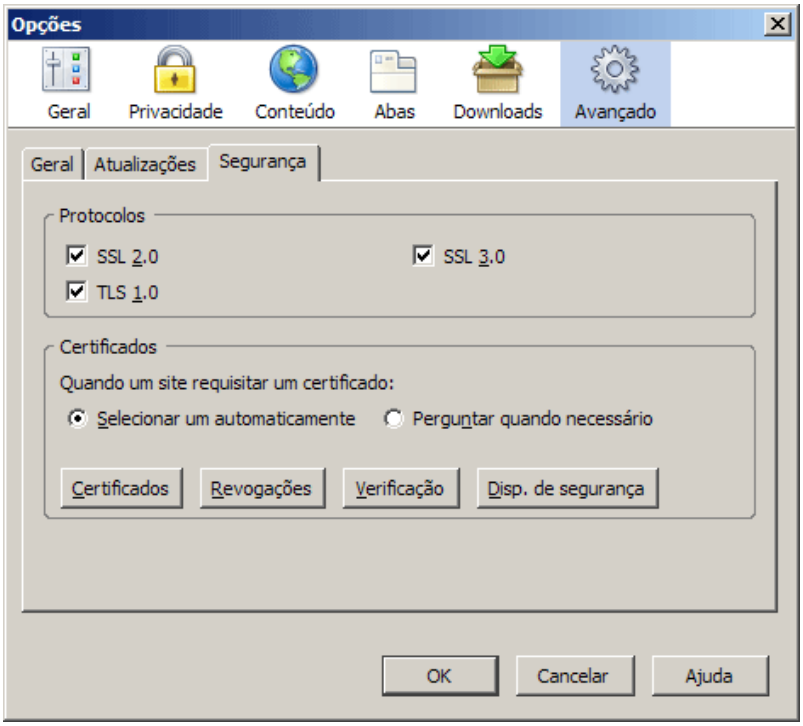
Pronto, seu certificado já está armazenado no ePass2000!

ATENÇÃO: se você deseja maiores informações sobre os procedimentos de solicitação, validação e gravação de seu certificado digital ICP-Brasil em seu ePass2000, consulte a Autoridade Certificadora ou se preferir os nossos boletins técnicos que estão disponíveis no diretório TOKENS\Boletins_Tecnicos do CD-ROM de instalação do ePass2000.

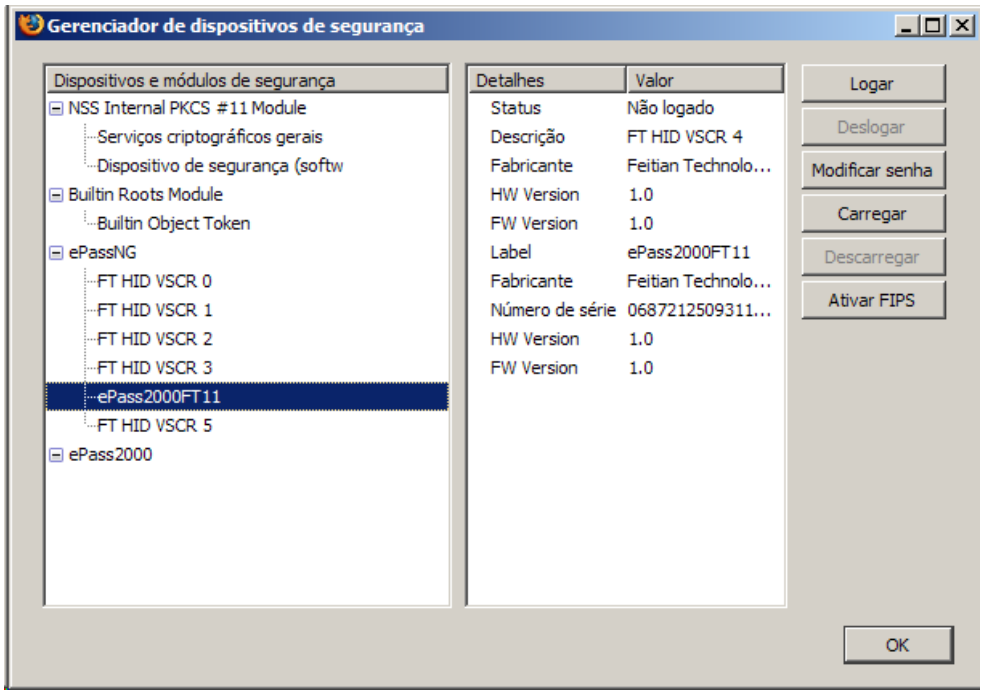
11. Utilizando o Mozilla Firefox para alterar o PIN do ePass2000

a) Clique em "Ferramentas" da barra de menu e depois em "Opções..."

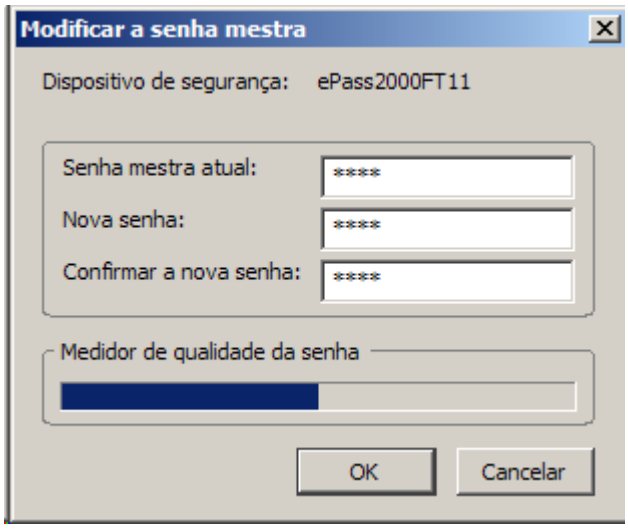
b) Na janela "Opões", clique na opção "Avançado" e depois no botão "Disp. De segurança"



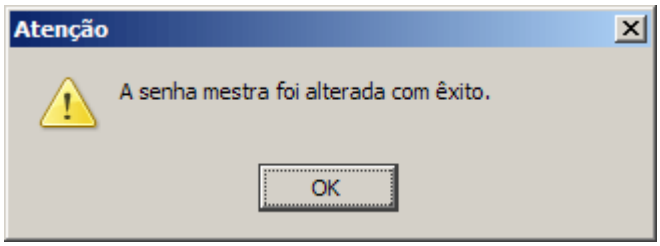
c) Na janela "Gerenciador de dispositivos de segurança", clique no nome do seu ePassNG e depois no botão "Modificar Senha"



d) Uma janela chamada “Modificar a senha mestra” será exibida. No campo “Senha mestra atual” digite o atual PIN do Usuário, nos campos seguintes digite o novo PIN do Usuário. Ao final, clique no botão “OK” para concluir a operação



e) Assim que a operação for concluída, clique no botão “OK” da janela “Aviso”



f) Clique no botão “OK” da janela “Gerenciador de dispositivos de segurança”

g) Clique no botão “OK” da janela “Opções” para concluir.

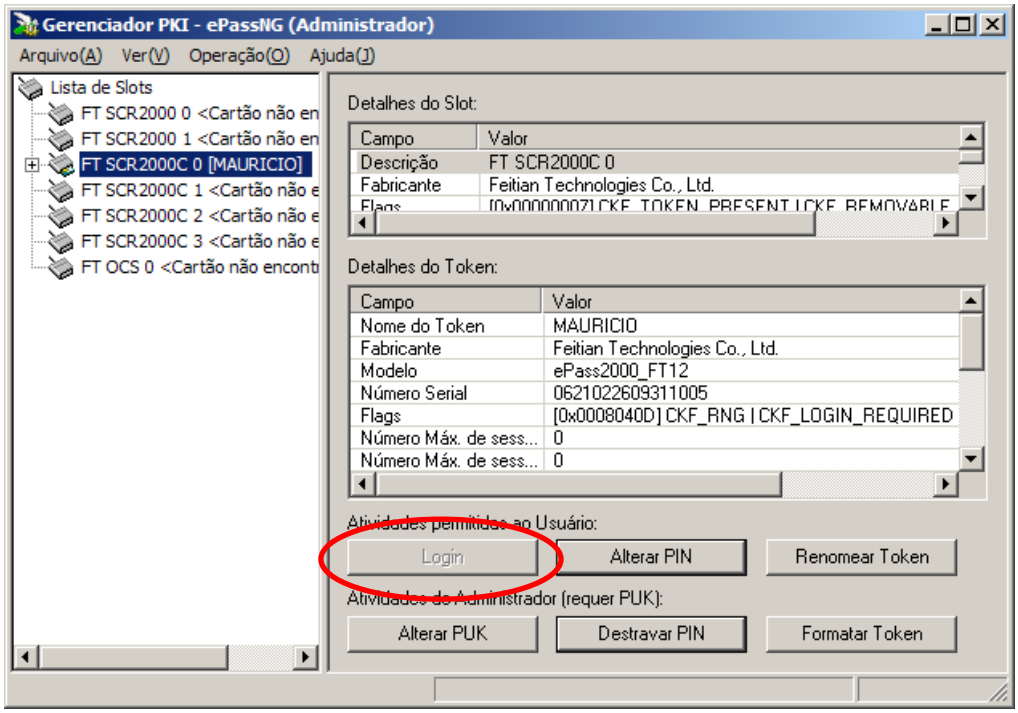
12. Importando um certificado digital para o ePass2000 a partir de um arquivo

NOTA: certificados digitais do tipo A3 não possuem cópia de segurança em arquivo formato .PFX ou .P12, pois de acordo com as normas da ICP-Brasil o par de chaves DEVE ser gerado dentro de um dispositivo criptográfico (Token USB ou Cartão Inteligente), tal norma determina que a chave privada não poderá ser exportada para fora do dispositivo criptográfico, impedindo assim a geração deste tipo de arquivo de backup.

Se você possui uma cópia do seu certificado digital em um arquivo .PFX ou .P12 e deseja importá-lo para o ePass2000 é necessário que você possua a senha do seu arquivo. De posse deste arquivo e da senha do mesmo, siga os seguintes passos:

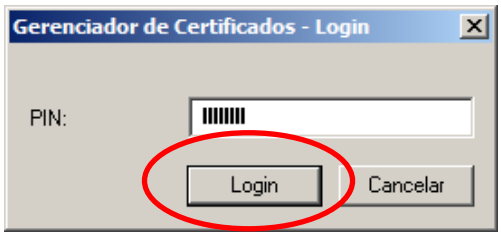
a) Execute o Gerenciador a partir do atalho criado em no grupo INICIAR | PROGRAMAS | Pronova

b) Clique no slot referente ao seu ePass2000 para que as opções de operação sejam exibidas



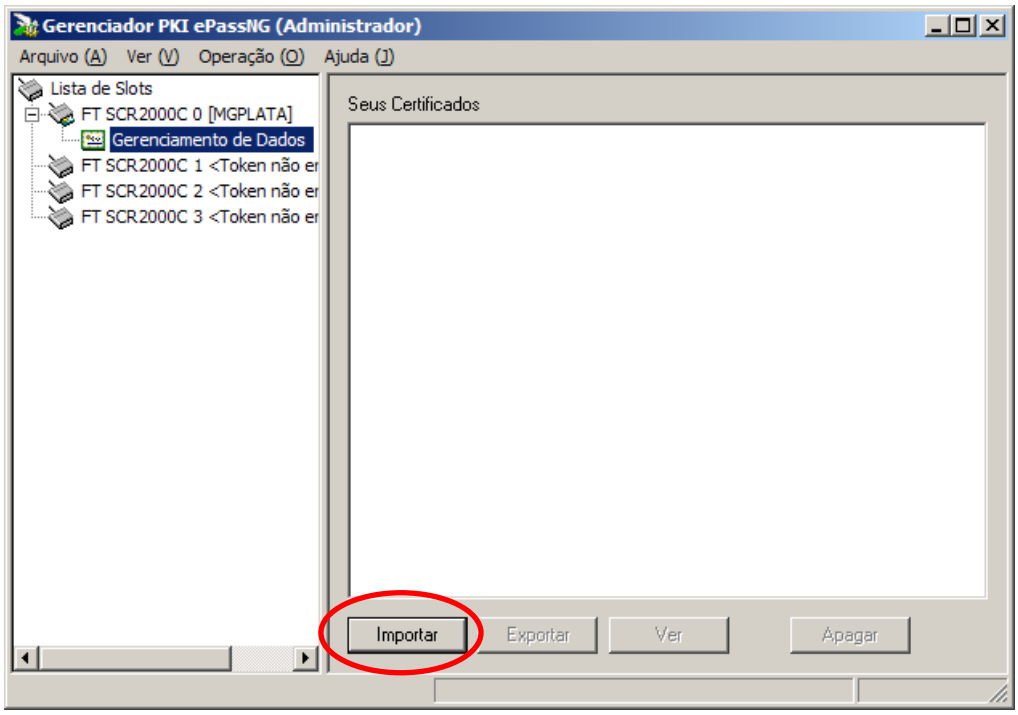
(imagem 13.1)

Clique no botão 'Login' (imagem 13.1) para que a janela 'Gerenciador de Certificados – Login' (imagem 13.2) seja exibida. Nela digite o PIN do seu Token e clique no botão 'Login' para continuar.

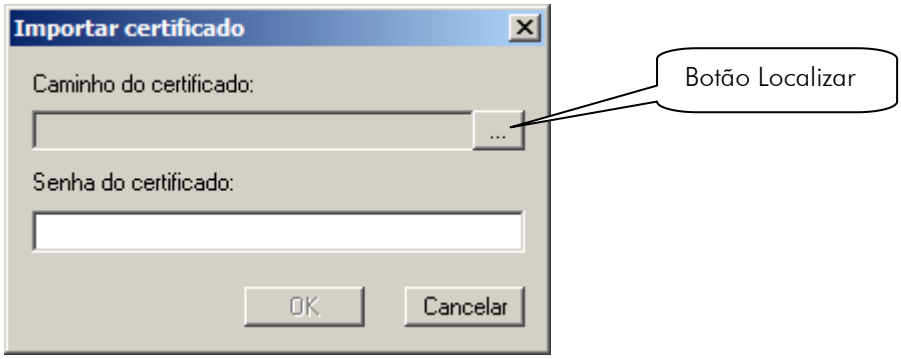


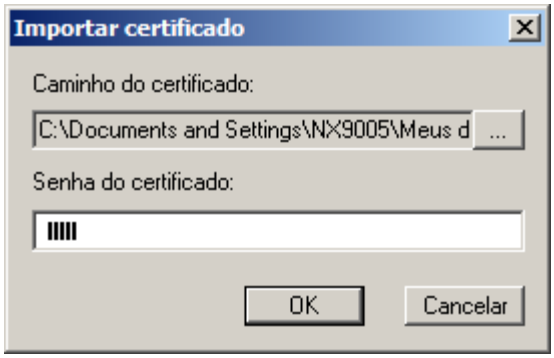
(imagem 13.2)

De volta a janela do Gerenciador, você será redirecionado para 'Gerenciamento de dados', para continuar clique no botão 'Importar' para que a janela 'Importar certificado' seja exibida.

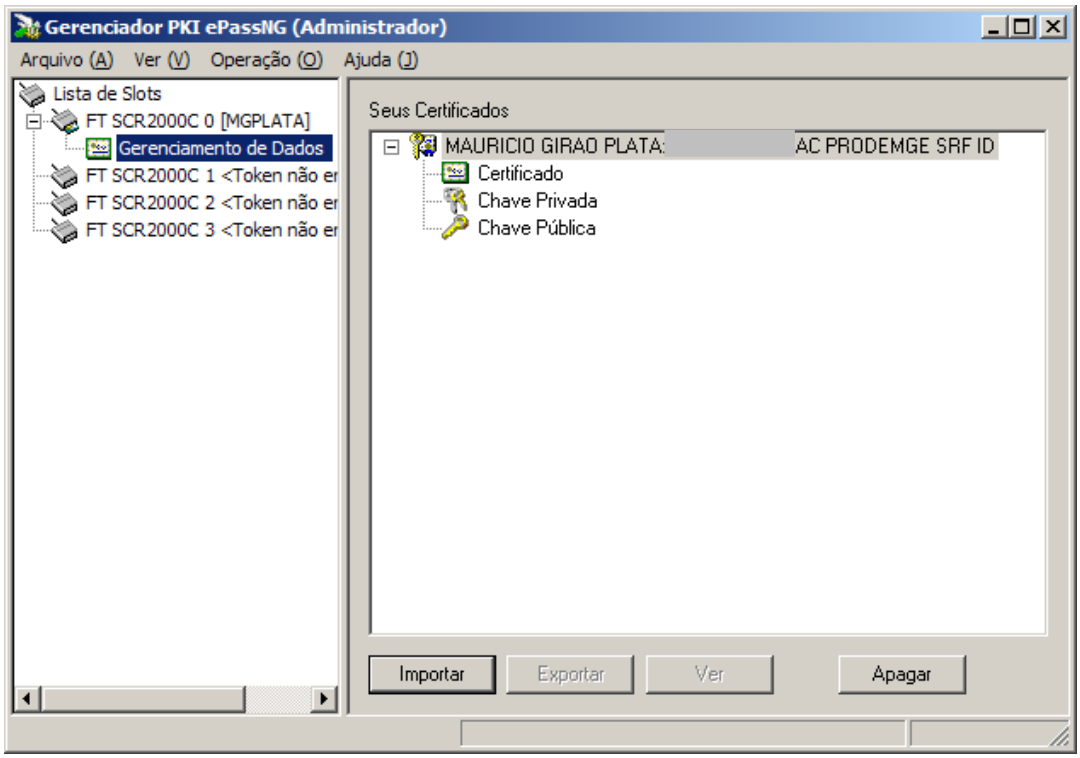


Clique no botão 'localizar' para informar o local onde está o arquivo .PFX (ou .P12) e a senha deste arquivo.

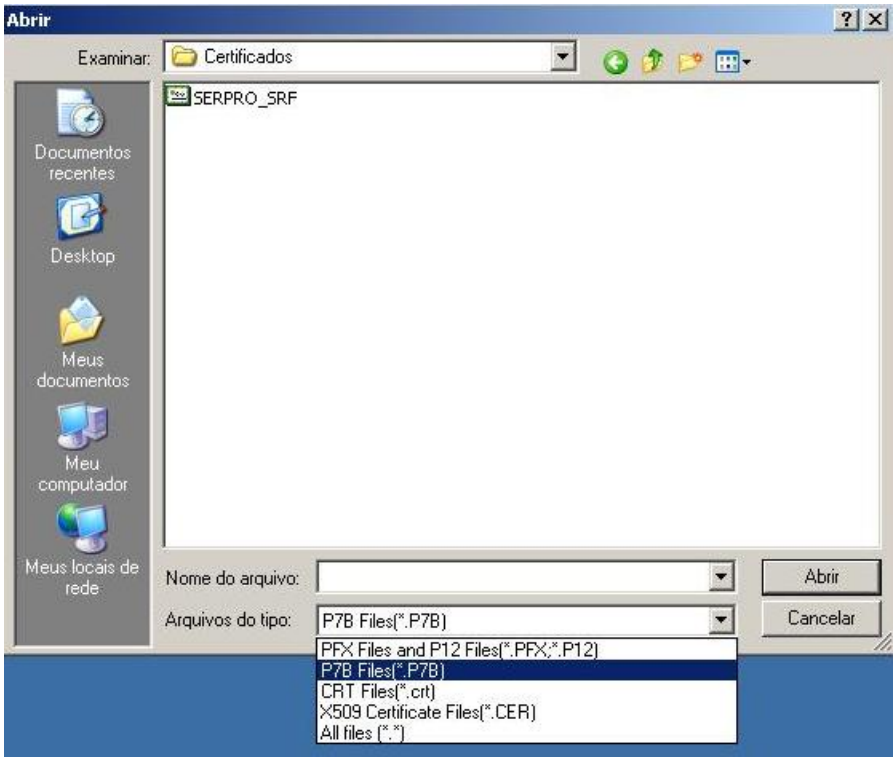




Assim que o certificado for importado para o seu dispositivo, você terá condições de verificar algumas informações do certificado.



Você também poderá importar para a memória do seu ePass2000 certificados em formato PKCS#7 (arquivo .P7B). Para isso, na janela abrir, você terá que selecionar a opção arquivos P7B (*.P7B). Caso deseje importar arquivos do tipo .CER, basta alterar o tipo para este formato de arquivo.

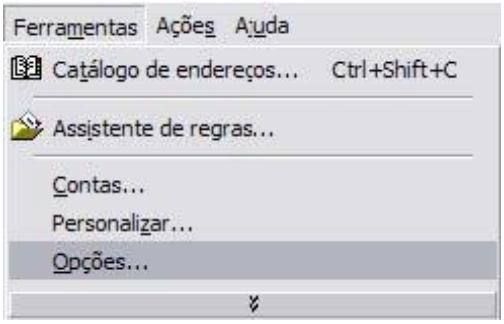


13. Configurando o Microsoft Outlook para usar um certificado armazenado no ePass2000

Para que as instruções citadas neste capítulo tenham resultado positivo, é necessário observar que o e-mail que está incluso no certificado digital armazenado no Token seja o mesmo da conta do Microsoft Outlook. Siga os passos apresentados neste tópico para que seja possível fazer uso de um certificado digital armazenado no ePass2000.

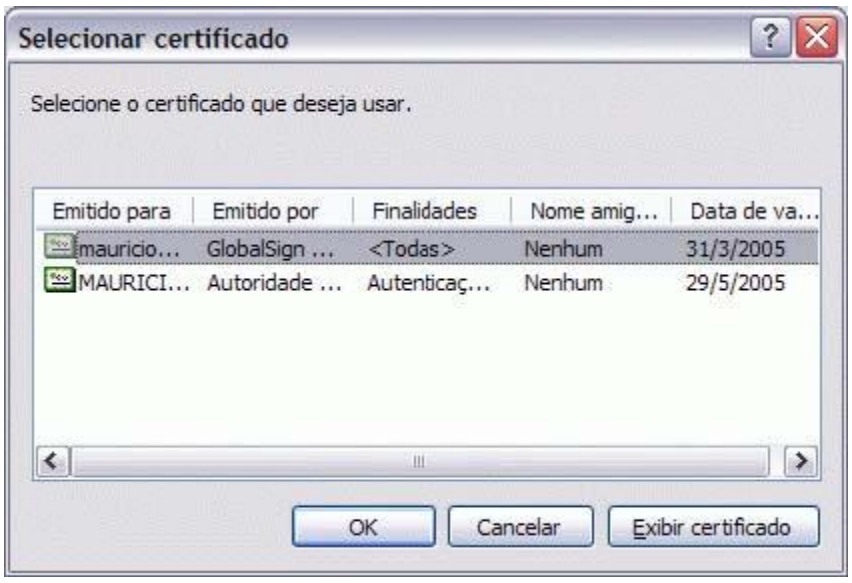
a) Conecte o seu dispositivo e depois execute o Microsoft Outlook;

b) Clique em "Ferramentas" da barra de menu e depois em "Opções";



c) Na janela "Opções", clique na guia "Segurança" e depois no botão "Configurações"

d) Na janela "Alterar configurações de segurança" clique no botão "Escolher" que está à direita do campo "Certificado de Autenticação". Da lista de certificados disponíveis, clique no certificado que corresponde a sua conta de e-mail. Depois no botão "OK";



e) Ainda na janela "Alterar configurações de segurança" clique no botão "Escolher" que está à direita do campo "Certificado de Criptografia". Da lista de certificados disponíveis, clique no certificado que corresponde a sua conta de e-mail. Depois no botão "OK";

f) Ainda na guia "Segurança", clique na opção "Adicionar assinatura digital a mensagens enviadas". Para concluir clique no botão "OK".

g) Ao final da seleção a janela "Alterar configurações de segurança" poderá ser fechada. Clique no botão "OK" para continuar.

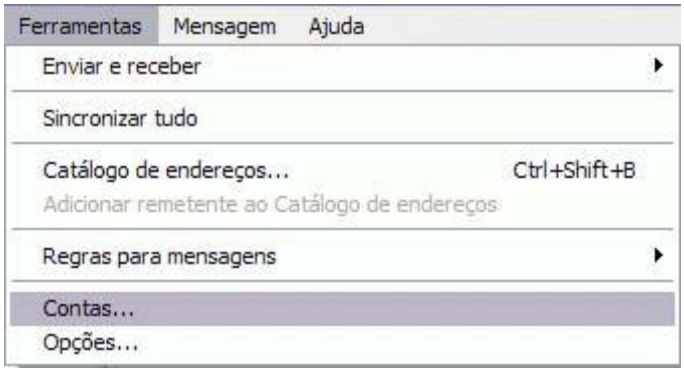
h) Na primeira vez que você for enviar uma mensagem assinada, será necessário informar o PIN do Usuário do seu dispositivo.

14. Configurando o Outlook Express para usar um certificado armazenado no ePass2000

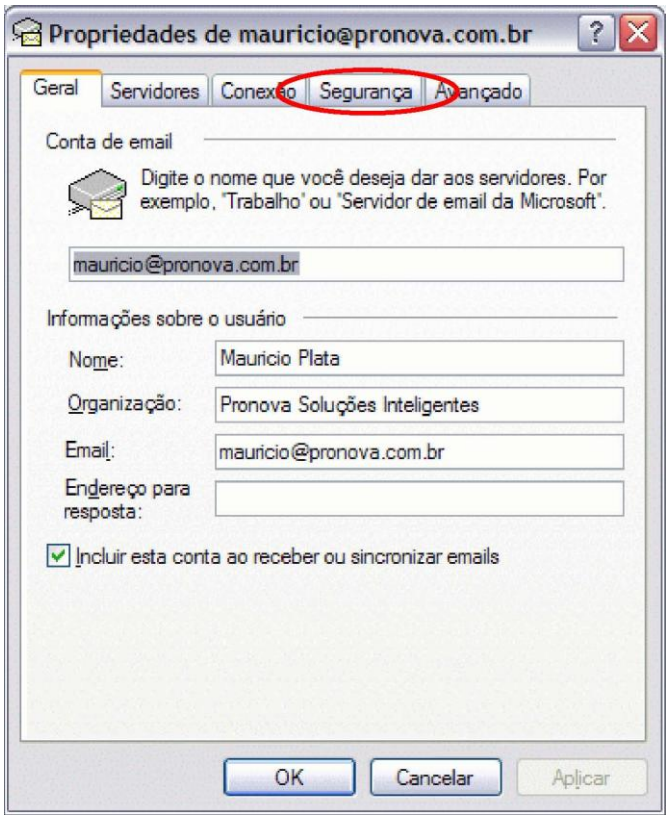
Para que as instruções citadas neste capítulo tenham resultado positivo, é necessário observar que o e-mail que está incluso no certificado digital armazenado no Token seja o mesmo da conta do Microsoft Outlook Express. Siga os passos apresentados neste tópico para que seja possível fazer uso de um certificado digital armazenado no seu dispositivo.

a) Conecte o seu dispositivo e depois execute o Outlook Express;

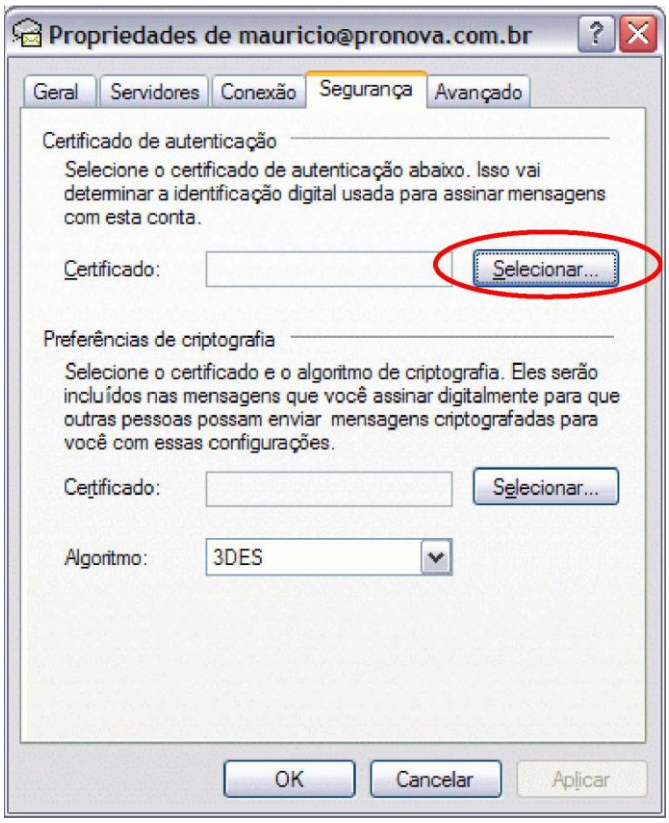
b) Clique em "Ferramentas" da barra de menu e depois em "Contas..."



c) Na janela "Propriedades de..." clique na guia "Segurança"



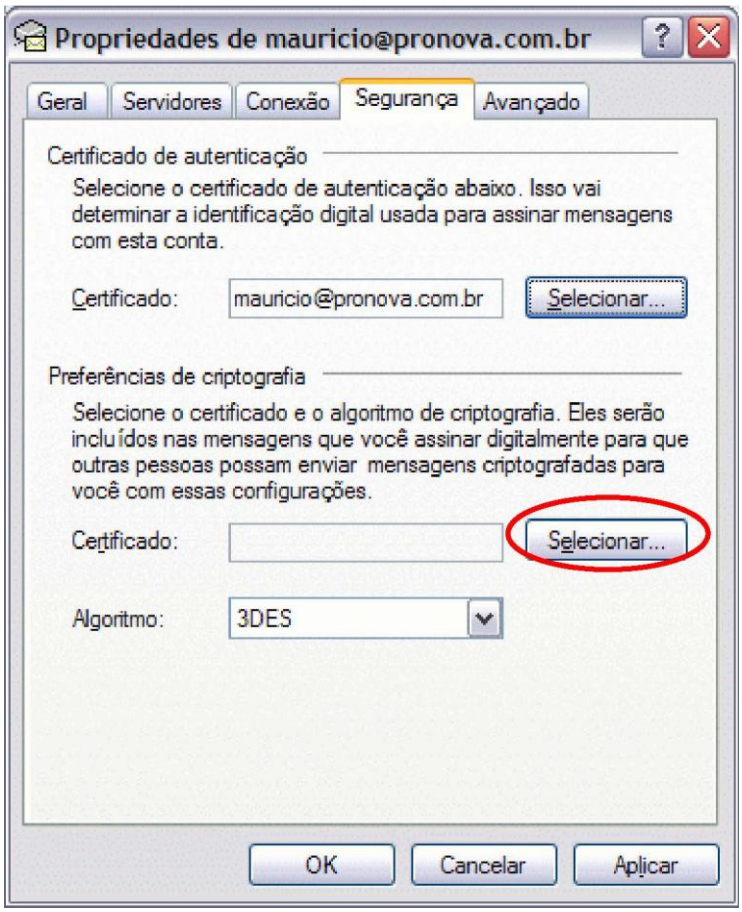
d) Na guia "Segurança", clique no botão "Selecionar" que está à direita do campo "Certificado" da área "Certificado de autenticação



e) Na janela "Selecionar identificação digital padrão da conta", selecione o certificado digital referente à conta em uso, em seguida clique no botão "OK".

Se você desejar visualizar as informações sobre o certificado digital, clique no botão "Exibir Certificado"

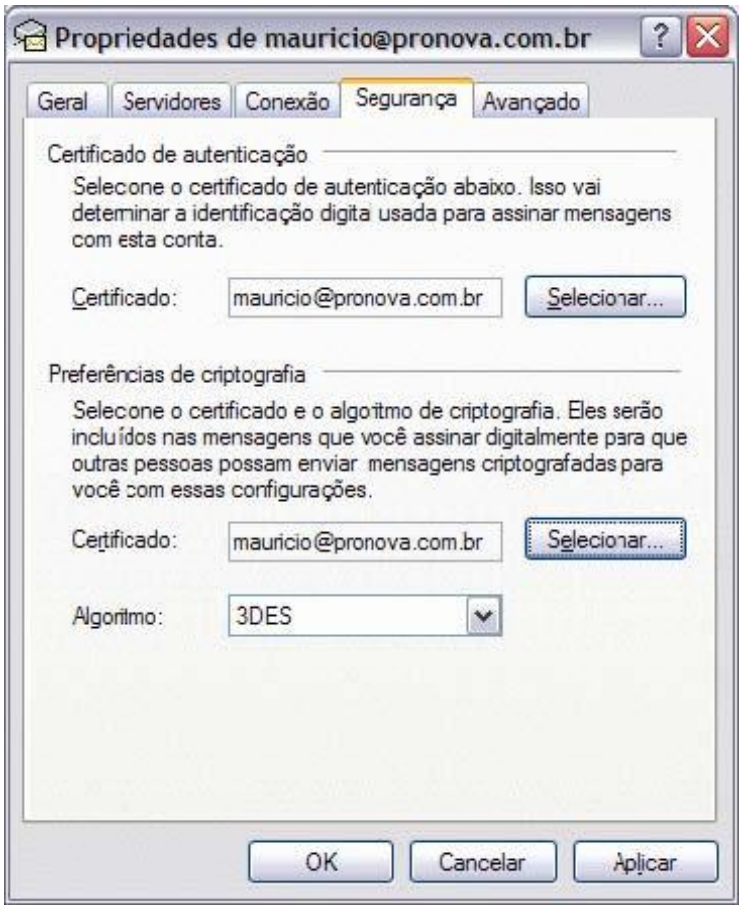
f) De volta a janela "Propriedades de...", clique no botão "Selecionar" que está à direita do campo "Certificado" da área "Preferências de criptografia"



g) Na janela "Selecionar identificação digital padrão da conta", selecione o certificado digital referente à conta em uso, em seguida clique no botão "OK".

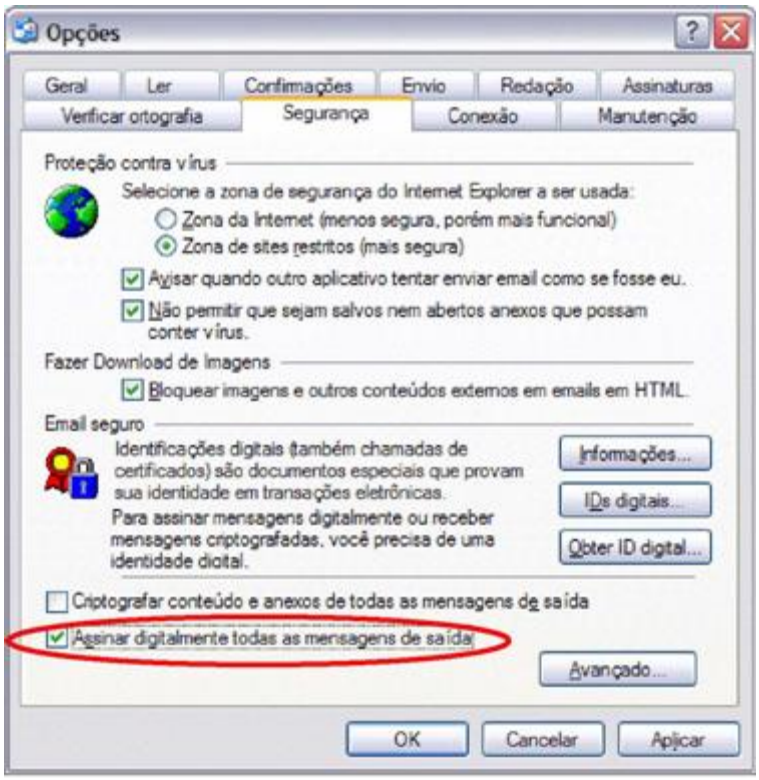
Se você desejar visualizar as informações sobre o certificado digital, clique no botão "Exibir Certificado"

h) Agora que você informou o Outlook Express os certificados que serão utilizados para assinar e codificar (criptografar) e-mails, basta clicar no botão "OK"

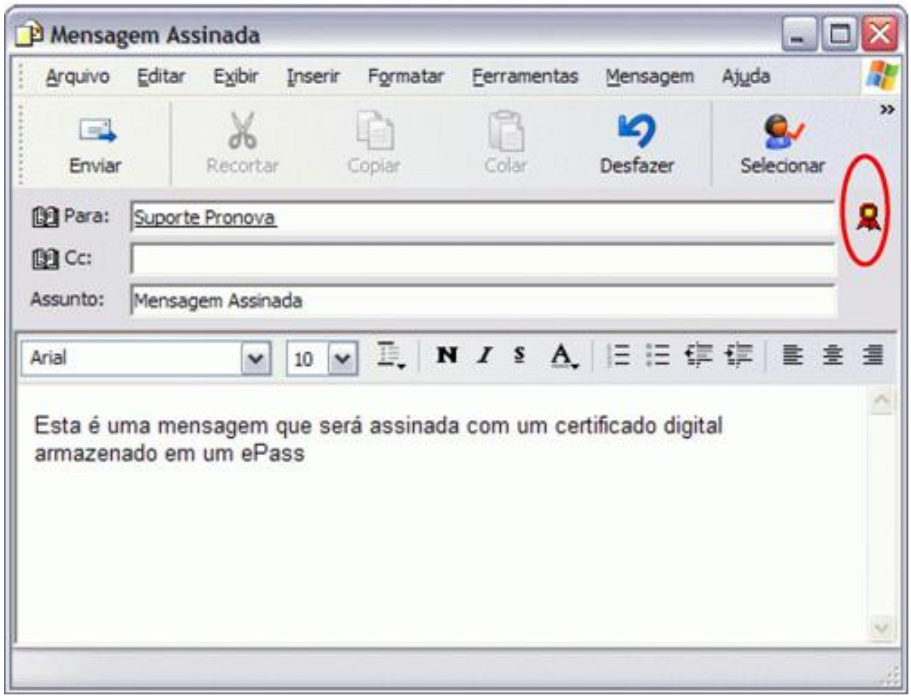


i) Clique mais uma vez em "Ferramentas" da barra de menu e depois em "Opções..."

j) Na janela "Opções", clique na guia "Segurança". Em seguida habilite a opção "Assinar digitalmente todas as mensagens de saída" e clique no botão "OK"



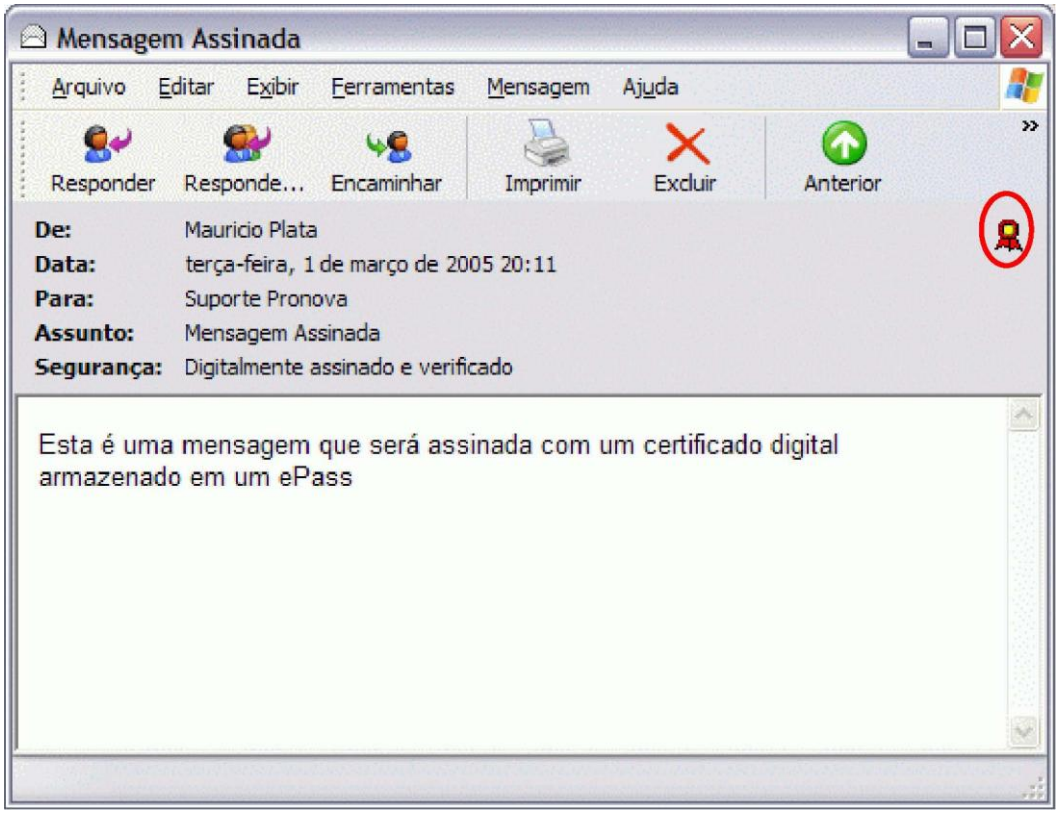
Toda vez que uma nova mensagem for criada observe que um novo ícone estará presente. Este indica que a mensagem será assinada com o certificado disponível no sistema



k) Toda vez que uma nova mensagem for criada note que um novo ícone estará presente. Este indica que a mensagem será assinada com o certificado digital da conta em uso

l) Ao clicar no botão enviar, será necessário informar o PIN do seu dispositivo. Digite-o no campo "PIN do Usuário" e depois clique no botão "Login"

m) Verifique nos itens enviados do Outlook Express se sua mensagem possui o selo indicando que a mensagem foi assinada



15. Integrando o ePass2000 com o Mozilla Thunderbird

ATENÇÃO: os procedimentos mencionados a seguir são exclusivos para este cliente de e-mail. A integração com o Microsoft Outlook e Outlook Express estão em um capítulo a parte.

Para integrar o ePass2000 com o Mozilla Thunderbird, execute os seguintes passos:

a) Execute o Mozilla Thunderbird, clique em "Ferramentas" da barra de menu e depois em "Opções"

b) Na janela Opções, clique em "Avançado"

c) Em seguida, clique no sinal a esquerda de "Certificados" e depois clique no botão "Dispositivos"

d) Uma nova janela chamada "Gerenciador de dispositivos de segurança" será exibida, clique no botão "Carregar" para continuar.

e) Na janela "Carregar dispositivo PKCS#11", clique no botão "Arquivo" para informar a localização do da biblioteca PKCS#11 (C:\WINDOWS\SYSTEM32\ngp11v211.dll)

f) Ao localizar o arquivo, clique sobre o mesmo e depois no botão "Abrir". De volta a janela "Carregar dispositivo PKCS#11, substitua "Novo módulo PKCS#11" no campo "Nome do módulo" por ePassNG e depois clique no botão "OK"

g) Clique no botão "OK" da janela "Confirmar"

h) A mensagem abaixo será exibida, clique no botão "OK" para continuar.

i) Um novo módulo ePass2000 será apresentado

j) Clique no botão "OK" da janela "Gerenciador de dispositivos de segurança"

k) Clique no botão "OK" da janela "Opções"

Atenção: não esqueça de instalar a cadeia de certificados da Autoridade Certificadora que emitiu o seu certificado digital, do contrário o Mozilla Thunderbird não irá reconhecer o seu certificado como válido!

16. Configurando sua conta de e-mail no Mozilla Thunderbird para fazer uso do certificado digital armazenado no ePass2000

a) Execute o Mozilla Thunderbird, clique em "Ferramentas" da barra de menu e depois em "Configurar contas..."

b) Na janela "Configurar contas", clique na opção "Segurança" e em seguida no botão "Selecionar" da área Assinatura digital

c) Ao clicar no botão "Selecionar" será necessário informar o PIN do seu dispositivo e depois clique no botão "OK" para continuar

d) Na janela "Selecionar certificado" serão apresentados os detalhes do certificado armazenado no seu dispositivo. Para continuar, clique no botão "OK"

e) O Mozilla Thunderbird irá perguntar se você deseja usar o mesmo certificado para criptografar mensagens. Se você desejar usar o mesmo certificado, clique no botão "OK", caso contrário clique no botão "Cancelar". No nosso guia, faremos uso do mesmo certificado, por esta razão orientamos clicar no botão "OK"

g) Antes de concluir, recomendamos que você habilite a opção "Assinar mensagens digitalmente (por padrão)"

h) Ainda na janela "Configurar contas", clique no botão "Certificados" da área "Gerenciamento"

i) Na janela "Gerenciador de certificados", verifique se a entidade certificadora que emitiu o seu certificado digital consta da lista, caso contrário baixe o certificado da autoridade certificadora e depois clique no botão "Importar"

j) Localize o certificado da sua Autoridade Certificadora e clique no botão "Abrir"

k) Na janela "Efetuando o donwload do certificado" habilite as finalidades e clique no botão "OK"

l) De volta a janela "Gerenciador de certificados", clique no botão "OK" para continuar

m) Para concluir clique no botão "OK" da janela "Configurar contas"

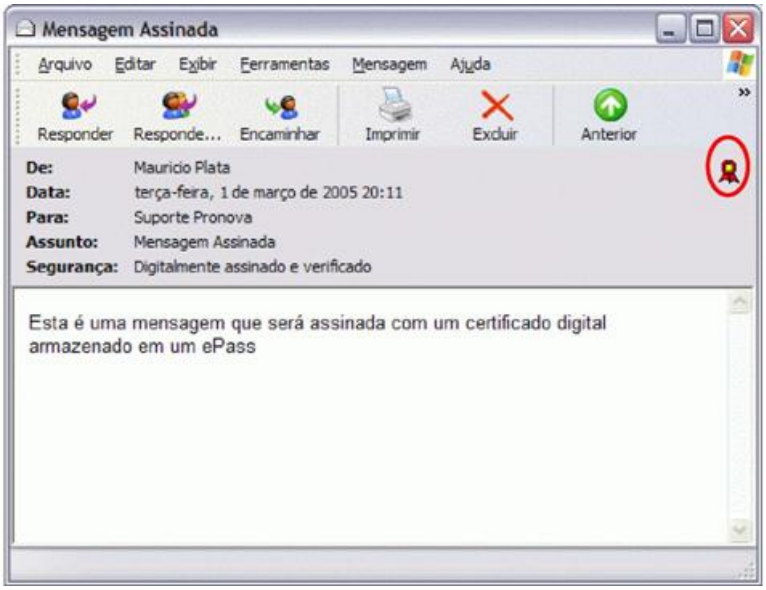
Pronto, agora o seu Mozilla Thunderbird fará uso do certificado digital armazenado no seu ePass2000.

17. Adicionando a identidade digital do remetente ao catálogo de endereços do Windows

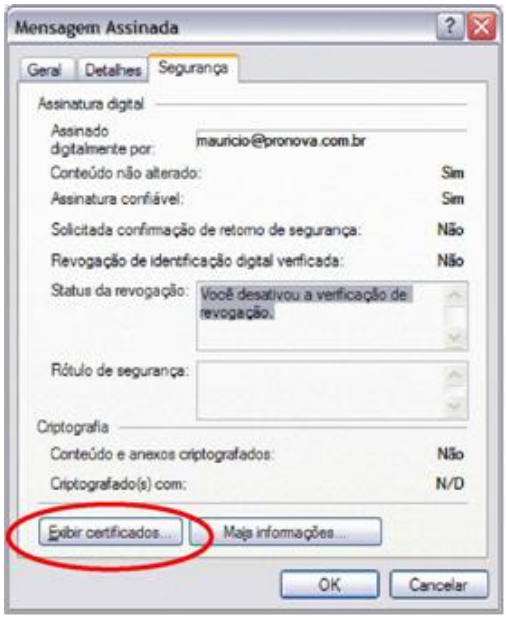
Para que seja possível a troca de e-mails criptografados usando o Microsoft Outlook e o Outlook Express, é necessário que a identidade digital da pessoa com quem você deseja trocar e-mails criptografados seja adicionada ao seu catálogo de endereços. Lembramos que não é possível trocar e-mails criptografados se uma das partes não possuir um certificado digital.

Para adicionar a identidade digital siga as seguintes instruções:

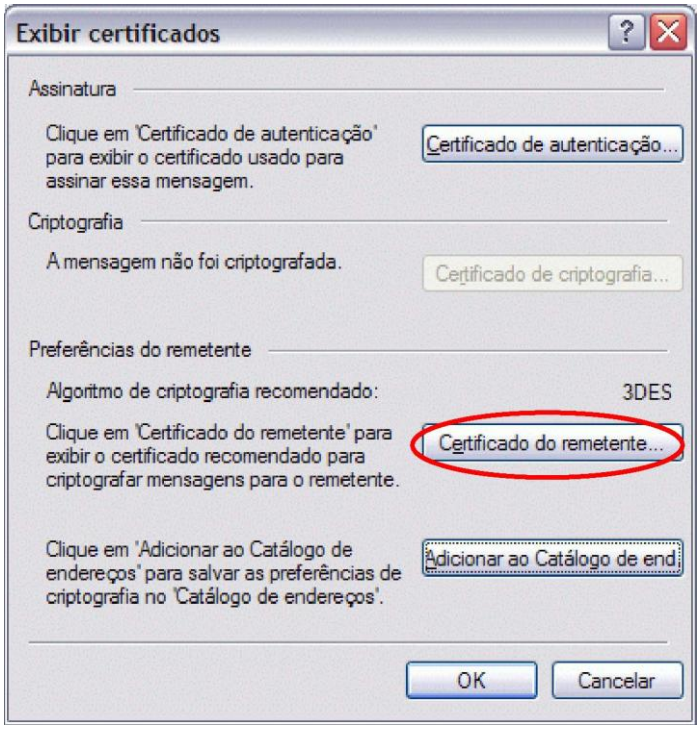
a) Abra a mensagem assinada com um certificado digital que foi enviada pela pessoa com quem você deseja trocar mensagens criptografadas. Na janela da mensagem assinada, clique no selo.



b) A janela "Mensagem assinada" será exibida. Nesta janela, clique no botão "Exibir certificados..."



c) Na janela "Exibir Certificados", clique no botão "Adicionar ao Catálogo de endereços"



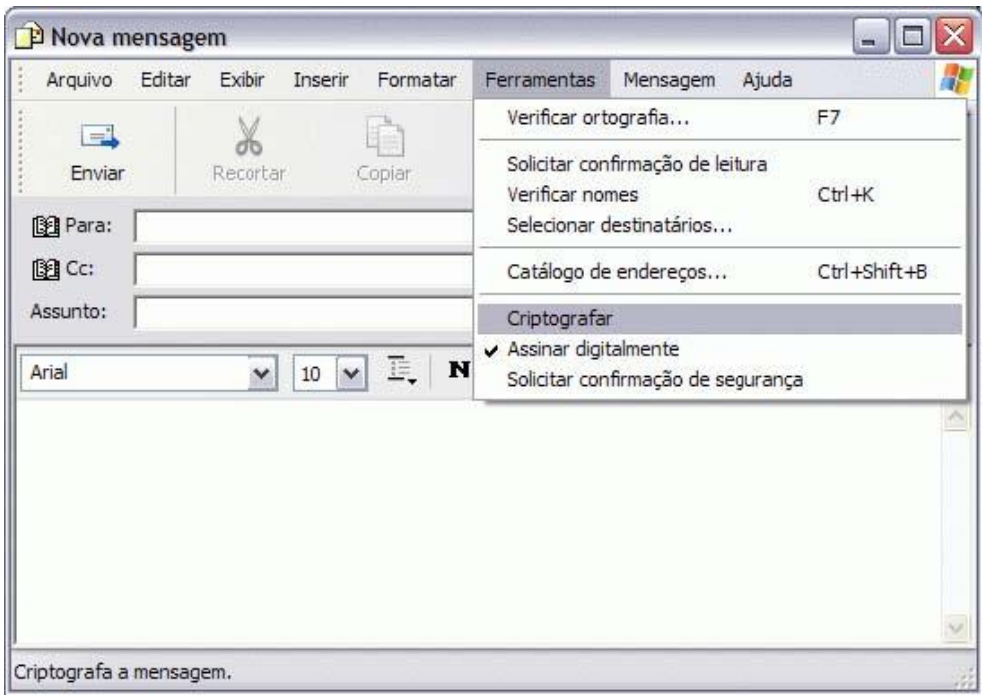
d) Uma janela de confirmação do Outlook Express será exibida, clique no botão "OK" para continuar

18. Enviando uma mensagem criptografada usando o Outlook Express

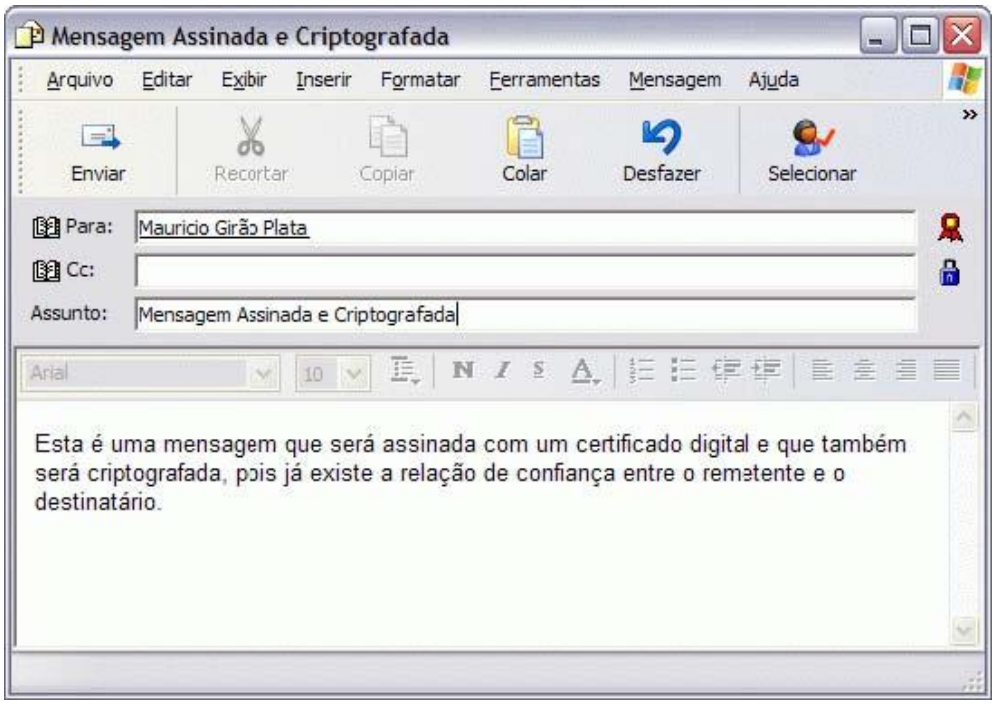
Uma vez que você adicionou a identificação digital ao catálogo de endereços, agora é possível enviar uma mensagem criptografada, como demonstraremos a seguir:

a) Crie uma nova mensagem

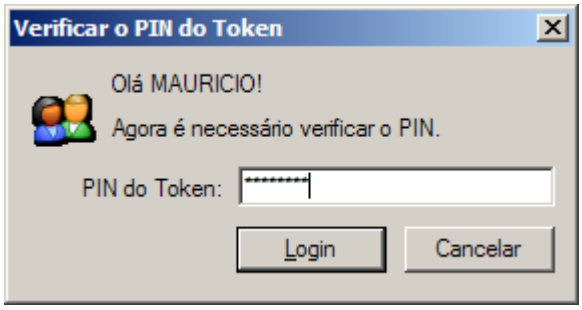
b) Clique em "Ferramentas" da barra de menu e depois selecione a opção "Criptografar"



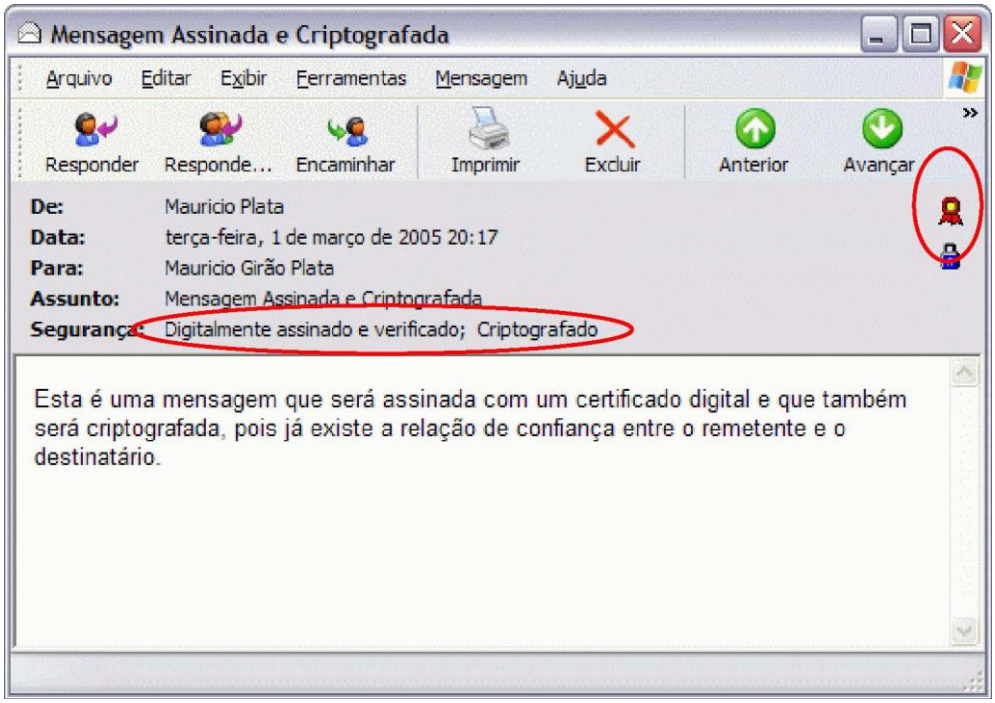
c) Note que um novo ícone será adicionado à janela. Para continuar, digite o conteúdo da mensagem, o assunto e o e-mail da pessoa que já consta no seu catálogo de endereços, a qual teve a identidade digital adicionada ao mesmo. Ao final clique no botão "Enviar"



d) Se você fechou e abriu o Outlook Express ou desconectou e conectou o seu dispositivo, será necessário informar mais uma vez o PIN do Usuário, pois a função que utiliza a chave privada do certificado terá que ser ativada mais uma vez. Digite-o no campo "PIN do Usuário" e depois clique no botão "Login"



e) A tela abaixo apresenta a mensagem enviada com os selos de assinatura e criptografia, além de uma nota informando que a mensagem está assinada digitalmente, verificada e criptografada.



f) Ao clicar no ícone do cadeado azul uma janela com informações sobre a mensagem será exibida. Observe que a área "Criptografia" informa que o conteúdo e anexos estão criptografados e que o algoritmo utilizado foi o 3-DES

g) Se você desejar que todas as mensagens enviadas sejam criptografadas, vá até "Ferramentas" da barra de menu depois selecione "Opções" e na janela "Opções", habilite o item "Criptografar conteúdo e anexos de todas as mensagens de saída"

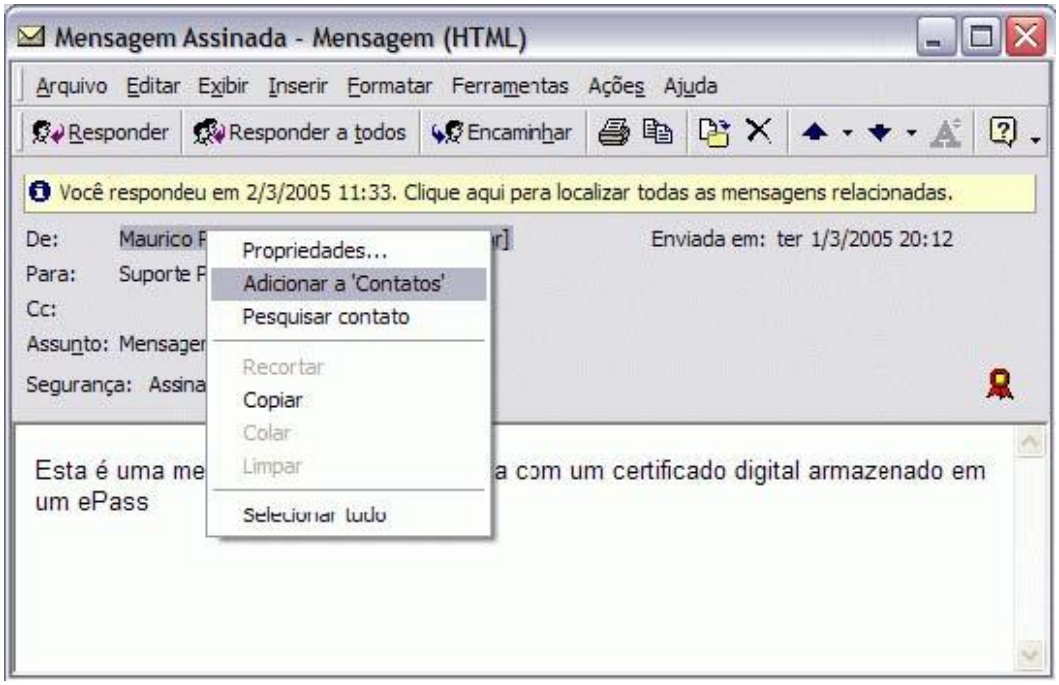
Nota: não se esqueça que para trocar mensagens criptografadas é necessário adicionar a identidade digital do destinatário ao seu catálogo de endereços.

19. Adicionando uma identificação digital à sua lista de contatos do Microsoft Outlook

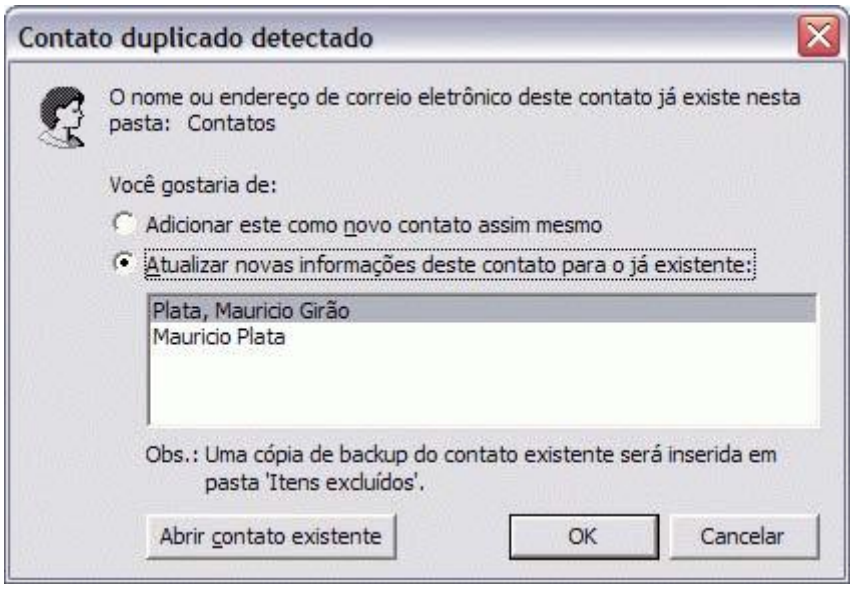
a) Abra uma mensagem que tenha uma identificação digital anexada

Nota: para que o remetente anexe uma identificação digital a uma mensagem, solicite que ele lhe envie uma mensagem de correio eletrônico assinada digitalmente.

b) Clique com o botão direito do mouse no campo "De" e, em seguida, clique em "Adicionar a Contatos" no menu de atalho

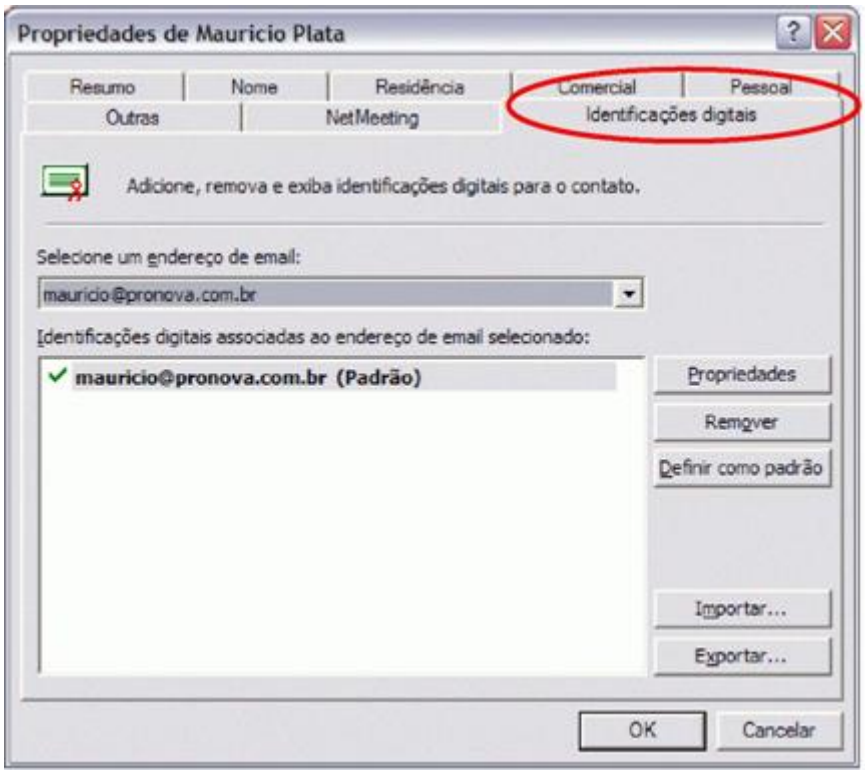


c) Se já houver uma entrada para essa pessoa na sua lista de contatos, selecione a opção "Atualizar novas informações deste contato para o já existente" e depois clique no botão "OK"



Com este procedimento a identificação digital estará agora armazenada com a sua entrada de contato para esse destinatário. Você poderá, então, enviar mensagens de correio eletrônico criptografadas para essa pessoa.

Para exibir os certificados de um contato, clique duas vezes no nome da pessoa e, em seguida, clique na guia "Identificações Pessoais"



20. Enviar uma mensagem com uma assinatura digital para um destinatário da Internet usando o Microsoft Outlook

a) Redija uma mensagem.

b) Na mensagem, clique em "Opções"

c) Marque a caixa de seleção "Adicionar assinatura digital à mensagem sendo enviada"

d) Para modificar as opções de segurança para essa mensagem, clique no menu "Arquivo", clique em "Propriedades" e, em seguida, clique na guia "Segurança"

e) Habilite a opção "Adicionar assinatura digital à mensagem e clique no botão "OK"

f) De volta a mensagem, clique em "Enviar".

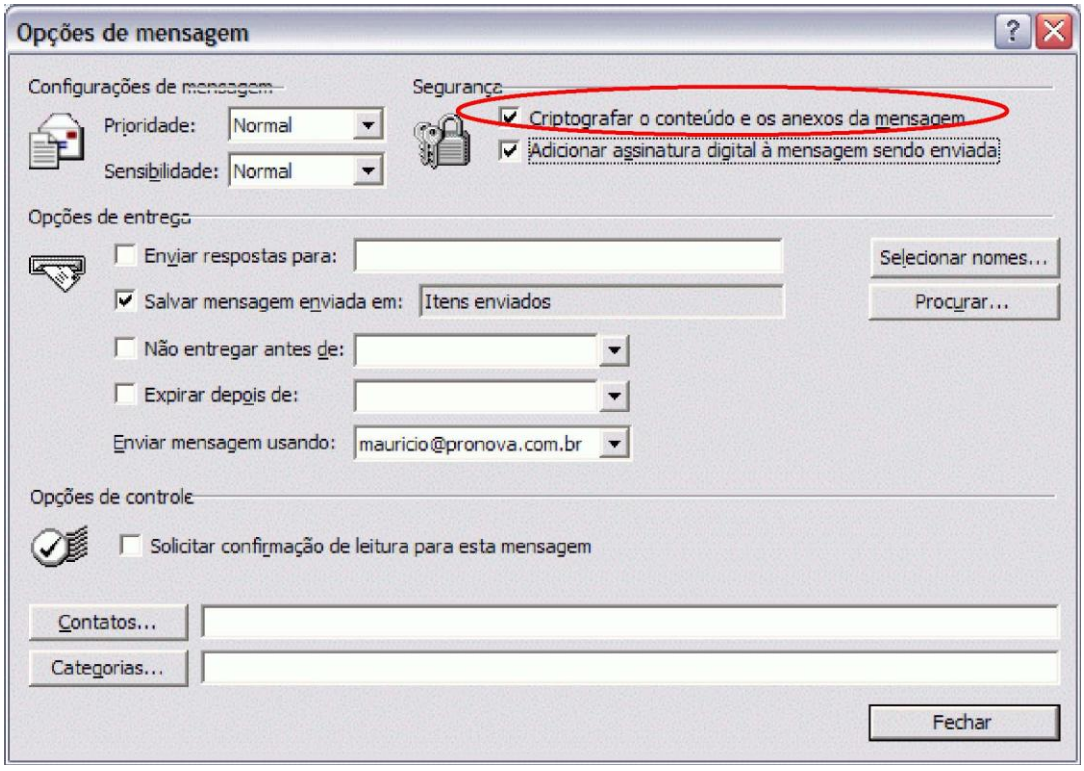
Observação:

- Para adicionar uma assinatura digital a todas as mensagens que você envia, clique no menu "Ferramentas" na janela principal do Outlook, clique em "Opções" e, em seguida, na guia "Segurança". Marque a caixa de seleção "Adicionar assinatura digital a mensagens sendo enviadas".

21. Enviar uma mensagem criptografada para um destinatário da Internet usando o Microsoft Outlook

a) Redija uma mensagem.

b) Na mensagem, clique em "Opções". Marque a caixa de seleção "Criptografar o conteúdo e os anexos da mensagem"



c) Clique em "Enviar".

Observações:

- Para criptografar todas as mensagens enviadas, no menu "Ferramentas", clique em "Opções" e, em seguida, clique na guia "Segurança". Marque a caixa de seleção "Criptografar conteúdo e anexos de mensagens sendo enviadas".
- Para modificar as configurações de segurança de uma mensagem específica, clique no menu "Arquivo" na janela de mensagens e, em seguida, clique em "Propriedades".

22. Removendo o software do ePass2000

Para remover o software do ePass2000, vá até o Painel de Controle "Adicionar ou Remover Programas", localize a opção "ePass2000 (Somente remover) e clique no botão "Alterar / Remover" e sigas as instruções do guia.

23. Perguntas e Respostas Comuns

a) Ao tentar formatar o meu dispositivo recebo a mensagem "Desculpe, mas o PUK informado está incorreto" O que pode estar errado?

R: Esta mensagem é exibida, pois PUK informado não é o correto. Para formatar o ePass2000, é necessário informar o atual PUK no campo "Digite o ATUAL PUK do Token' da janela "Formatar o Token (Inicializar Setor PKI)". Tenha cuidado para não informar cinco vezes o valor errado do PUK, pois se você fizer isso, o seu ePass2000 será bloqueado. Para desbloqueá-lo será necessário reformatá-lo, perdendo-se assim todas as informações que estão armazenadas nele.

Nota: *se você for um usuário corporativo e não possui o PUK do seu dispositivo, entre em contato com o Administrador de Sistemas da sua empresa*. Lembramos que existe um número pré-determinado de tentativas de acerto do PUK. Se estas forem excedidas o seu dispositivo será bloqueado e todo o conteúdo do dispositivo ficará indisponível.

b) O botão "OK" da janela 'Formatar Token' não está disponível para uso. O que pode estar errado?

R: Verifique os valores digitados nos campos "Digite um NOVO PIN" e "Confirme o NOVO PIN", certamente eles não possuem o mesmo valor ou tamanho.

c) Tenho um certificado digital ICP-Brasil no meu dispositivo, mas não consigo fazer uso em aplicações no Internet Explorer. O que pode estar errado?

R: Certamente o seu navegador não possui a cadeia de certificados da ICP-Brasil e da Autoridade Certificadora que emitiu o seu certificado digital. Para resolver este problema, é necessário proceder a instalação da cadeia de certificados, consulte a equipe de suporte da sua Autoridade Certificadora para conhecer os procedimentos de instalação da cadeia de certificados. Se você não tem acesso a Internet, use o diretório ICP-Brasil do CD-ROM de instalação do seu ePass2000. Nele colocamos os arquivos de cadeia de certificado da grande maioria de ACs credenciadas à ICP-Brasil

d) Ao conectar o meu ePass2000 na porta USB, a luz dele fica piscando ele não é reconhecido. O que pode estar errado?

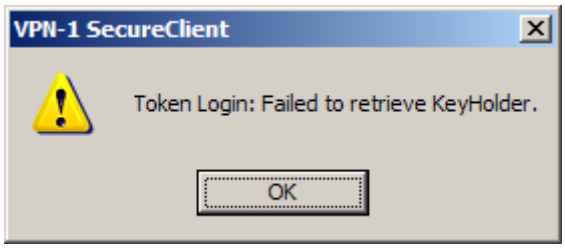
R: Certamente o software do ePass2000 não está instalado, execute o programa de instalação que está disponível no CD-ROM de instalação e siga as instruções do instalador. Maiores detalhes poderão ser encontrados no Tópico 4 "Instalando o software do ePass2000".

Se o problema persistir, verifique se a controladora USB do seu micro está habilitada na BIOS da sua placa-mãe.

e) Ao conectar o meu ePass2000 na porta USB, a luz dele não liga ele não é reconhecido. O que pode estar errado?

R: Certamente a porta USB do seu computador não está instalada fisicamente. Consulte um técnico para fazer a verificação desta porta USB ou tente conectar o seu ePass2000 em um outro computador. Se o problema persistir entre em contato com a Pronova.

f) O Cliente VPN-1 SecuRemote da Check Point não consegue localizar o meu certificado que está armazenado no ePass2000. Se eu insisto, o cliente SecuRemote consegue identificar, mas ao selecionar o certificado ele exibe a mensagem "Token Login: Failed to retrieve KeyHolder". O que pode estar errado?



R: Este é um problema clássico de ausência do caminho (path) da autoridade certificadora que emitiu o seu certificado. Sem esta informação, certamente o seu certificado é tratado pelo sistema operacional como um certificado inválido. Para resolver este problema, basta instalar o certificado raiz da autoridade certificadora no repositório do Windows ou importar para o ePass2000 o certificado raiz da AC que emitiu o seu certificado digital.

g) Tenho meu certificado digital ICP-Brasil armazenado no ePass2000, mas ao tentar acessar o site da Receita Federal recebo a mensagem "É necessário instalar um certificado digital de cliente para ter acesso ao e-CAC." O que pode estar errado?

R: Este tipo de comportamento ocorre quando a cadeia de certificados da Autoridade Certificadora não está instalada no seu navegador (Internet Explorer ou Mozilla Firefox). Instale no navegador a cadeia de certificados da AC que emitiu o seu certificado digital, reinicie o seu micro e tente fazer um novo acesso.

h) Tenho meu certificado digital ICP-Brasil armazenado no ePass2000, mas quando tento enviar uma declaração para receita via certificado o campo para inserir o PIN não aparece, ocasionando a não transmissão da mesma. O que pode estar errado?

R: Este tipo de comportamento ocorre quando a cadeia de certificados da Autoridade Certificadora não está instalada no seu computador. Instale no navegador a cadeia de certificados da AC que emitiu o seu certificado digital, reinicie o seu micro e tente fazer um novo acesso.

i) Travei o PUK do meu ePass2000, perdi o meu dispositivo?

R: Não, você não perdeu o seu dispositivo. Todavia, para reativar o acesso ao seu ePass2000, será necessário reinicializar o seu equipamento para as condições originais de fábrica. Em outras palavras, ao usar a ferramenta ePassNG Init. Procure no CD-ROM de instalação o instalador desta ferramenta no diretório "Formatador", instale a ferramenta, mas antes de utiliza-la consulte o PDF que poderá ser acessado a partir do atalho criado no menu INICIAR do Windows. Lembramos que ao utilizar esta o ePassNG Init todas as informações que estiverem armazenadas no seu ePass200 serão apagadas e serão restaurados os padrões de fábrica do ePass2000.

j) Posso instalar mais de um certificado no meu ePass2000?

R: Sim, você poderá instalar mais de um certificado no seu ePass2000, mas tenha em mente que existe uma limitação que é a quantidade de memória do seu dispositivo (32K). Normalmente conseguimos colocar até 05 (cinco) ou 06 (seis) certificados. Observe ainda que você se você usar seu certificado para codificar mensagens e/ou documentos talvez você terá que guardar este seu certificado por um tempo após a expiração deste, para que seja possível a decodificação destes dados.

Tendo em vista que a chave privada gerada no ePass2000 não pode ser exportada, recomendamos que não sejam armazenados no mesmo ePass2000, certificados que não tenham relação entre sim. Por exemplo, um certificado e-CNPJ de uma empresa X mais um certificado e-CNPJ de uma empresa Y. Imagine que a empresa X deseja ter com ela o seu certificado. Como a chave privada é parte integrante do certificado e-CNPJ, para resolver este impasse será necessário revogar o certificado da empresa X. A seguir fazer uma nova aquisição de um e-CNPJ para a empresa X em outro ePass2000.

k) O ePass2000 pode ser utilizado em outros sistemas operacionais?

R: Sim, o ePass2000 poderá ser utilizado nos sistemas operacional Linux ou MacOS. O software necessário para instalar o ePass2000 nestes sistemas operacionais poderá ser encontrado nos diretórios Linux e MacOS do CD-ROM de instalação do ePass2000.

As instruções para instalação poderão ser encontradas no arquivo README contigo dentro dos arquivos .tar.gz.

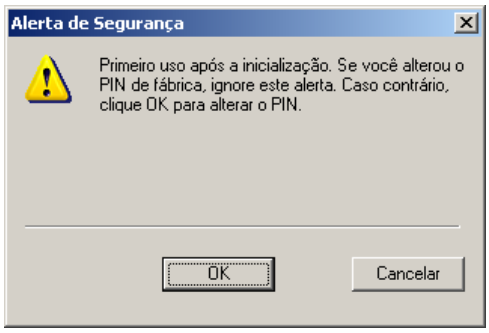
l) Instalei o software do ePass2000 e não tive nenhum tipo de problema, mas depois que eu reinicio o meu computador o "Monitor de Certificados" não é exibido na área de notificação do Windows e o meu certificado não fica disponível para que eu possa fazer uso. O que pode ter ocorrido?

R: Certamente, algum anti-vírus ou aplicação que protege a sua máquina está inibindo a execução do aplicativo "epsng_certd.exe" que é carregado na inicialização do Windows. Verifique nos logs do seu anti-vírus ou aplicação este registro e proceda a liberação do carregamento automático do programa "epsng_certd.exe".

m) Fora o manual do ePass2000, existe algum outro tipo de material de consulta?

R: Sim, a Pronova disponibiliza além do Manual vários boletins técnicos que poderão ser encontrados no diretório "Boletins Técnicos" do CD-ROM de instalação do ePass2000.

n) Depois de instalar o software do ePass2000, quando conecto ele na porta USB, um alerta de segurança informando que devo trocar o PIN é exibido, isto é normal? O que devo fazer?



R: Sim, isto é normal. Em decorrência ao atendimento a novas normas do Comitê Gestor da ICP-Brasil, este é um recurso que foi adicionado ao software do ePass2000. Este recurso visa forçar a troca do PIN de fábrica do ePass2000. Para isso, clique em OK e preencha os campos corretamente.

O) Estou tentando solicitar meu certificado digital no meu computador com o Windows Vista, mas na página da Autoridade Certificadora, a lista de CSP não aparece? O que devo fazer?

R: Nas versões anteriores do Windows, a DLL responsável pelo carregamento da lista de CSP era o arquivo "xenroll.dll" que no Windows Vista passou a se chamar "certenroll.dll". A página da autoridade certificadora, procura no seu computador a antiga DLL que não existe no Windows Vista. Por esta razão, a lista de CSP no Windows Vista não é carregada. Para que você possa solicitar seu certificado, use uma máquina com uma versão anterior ao Windows Vista, como, por exemplo, o Windows XP. Depois que você gravar o seu certificado no Token, você poderá usá-lo sem problemas no Windows Vista.

24. 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.

25. Contatos

Pronova Soluções Inteligentes (Importador e Distribuidor Autorizado)

Endereço	Av. 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 103)
E-mail	suporte@pronova.com.br ou sac@pronova.com.br
Sites	www.pronova.com.br ou www.lojapronova.com.br

Feitian Technologies Inc., Ltd. (Fabricante)

Endereço	3Fl., No.5 Building, Jimen Hotel, Xueyuan Road, Haidian District, Beijing, 100088, República Popular da China
Telefones	+86-10-62360800 e +86-10-62360900
Fax	+86-10-82070027
Site	www.FTsafe.com

Feitian Technologies Co., Ltd. é uma empresa ISO 9001