



As informações contidas neste manual estão sujeitas a alterações sem aviso prévio e não representam um compromisso por parte de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA. Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou sistemas de armazenamento e recuperação, sem o prévio consentimento, por escrito, de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA.

Windows® é marca registrada da Microsoft Corporation Pentium® é marca registrada da Intel Corporation ePassNG é marca registrada da Feitian Technologies Inc., Ltd. AMD® é marca registrada Advanced Micro Devices

Índice

- 1. Glossário
- 2. Lista de Acrônimos
- 3. Sobre a Pronova Soluções Inteligentes
- 4. Sobre o ProToken
- 5. Instalando o software do ProToken
 - 5.1 Instalação no Windows 2000, XP ou 2003
 5.2 Instalação no Windows 98SE e Windows ME
 5.3 Sobre o Gerenciador de Certificados do ProToken
 5.4 Alterando o PIN do Token
 5.5 Configurando o Tempo de Vida do PIN do ProToken
 5.6 Visualizando certificados armazenados no ProToken
 5.7 Removendo um certificado do repositório do Windows
 - 5.8 Registrando um certificado no repositório do Windows
- 6. Sobre o Gerenciador do Token
 - 6.1 O que é o PUK (PIN unlock key)?
 - 6.1.1 Alterando o PUK
 - 6.2 O que é o PIN do Usuário?
 - 6.2.1 Alterando o PIN do Token
 - 6.3 Destravando o PIN do Usuário
 - 6.4 Renomeando o dispositivo
 - 6.5 Inicializando (formatando) o ProToken
 - 6.6 Visualizando os dados armazenados no ProToken
- 7. Instalando um certificado digital emitido por uma AC Microsoft no ProToken
- 8. Intregrando o ProToken com o nevageador Mozilla Firefox 1.5x
- 9. Utilizando o Mozilla Firefox 1.5 para alterar o PIN do Usuário do ProToken
- 10. Importando um certificado digital para o ProToken a partir de um arquivo
- 11. Configurando o Microsoft Outlook para usar um certificado armazenado no ProToken
- 12. Configurando o Outlook Express para usar um certificado armazenado no ProToken

- 13. Integrando o ProToken com o cliente de e-mails Mozilla Thunderbird
- 14. Configurando sua conta de e-mail no Mozilla Thunderbird para fazer uso do certificado digital armazenado no ProToken
- 15. Adicionando a identidade digital do remetente ao catálogo de endereços do Windows
- 16. Enviando uma mensagem codificada (criptografada) usando o Outlook Express
- 17. Adicionando uma identificação digital à sua lista de contatos do Microsoft Outlook
- Enviar uma mensagem com uma assinatura digital para um destinatário da Internet usando o Microsoft Outlook
- 19. Enviar uma mensagem codificada (criptografada) para um destinatário da Internet usando o Microsoft Outlook
- 20. Como assinar um documento do Microsoft Word 2003 usando um certificado digital ICP-Brasil armazenado no ProToken?
- 21. Removendo o software do ProToken
- 22. O Gerenciador Web PKI do ProToken
- 23. Instalando o ProToken no sistema operacional Linux
- 24. Ferramentas de Teste do ProToken
- 25. Perguntas e Respostas Comuns
- 26. Suporte Técnico
- 27. Contatos

1. Glossário

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FIPS (Federal Information Processing Standards): correspondem a padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norteamericano. 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.

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.

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.

9

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 LED Light Emitting Diode LSITEC Laboratório de Sistemas Integráveis Tecnológico MAC Message Authentication Code 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 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 o ProToken

O ProToken é uma versão especial do Token USB ePass2000 que utiliza o chip criptográfico da Oberthur Card Systems o qual oferece suporte a geração do par de chaves RSA de 2048bits. Assim como o ePass2000, o ProToken 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 **ProToken** é um Token USB de autenticação que pode ser utilizado em Windows 98SE, 2000, ME, XP, 2003 e Linux. Da mesma forma que um cartão inteligente (smart card), pode executar poderosos cálculos de criptografia.

A seguir os principais recursos oferecidos pelo Token USB ProToken

- → Geração no próprio dispositivo (on board) do par de chaves RSA 1024bits e RSA 2048bits;
- → Suporte nativo para os algoritmos DES, 3DES, RSA, SHA-1, SHA-2 (256), AES (128 bits), Elliptic Curves (EC-DSA)
- → Suporte padrão para aplicações Microsoft Crypto API;
- \rightarrow Compativel com Windows 2000 PC/SC;
- → Geração de números aleatórios em hardware;
- \rightarrow 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, e FIPS (Certificado FIPS 140-2 L2 número 668);
- \rightarrow Chassi tamper evident;
- \rightarrow Capa protetora do conector USB;
- \rightarrow Gerenciamento através de um PIN e de um PUK;
- \rightarrow LED monocromático para indicação de funcionamento

 \rightarrow Software de Gerenciamento do dispositivo em Português do Brasil.

4.1 Especificações Técnicas

Sistemas Operacionais:	Windows 98SE, 2000, ME, XP, 2003 e Linux (kernel 2.4 ou mais recente)	
Certificações e Padrões:	PKCS#11, MS CAPI, PC/SC, X.509 v3, SSL v3, IPSec/IKE, ISO 7816 3-4, FCC, CE e FIPS 140-2 L2	
Processador:	8 bits	
Memória do Dispositivo	64KB	
Memória Disponível para o usuário:	ЗОКВ	
Algoritmos On-Board:	DES, 3DES, RSA, SHA-1, SHA-2 (256), AES (128 bits), Elliptic Curves (EC-DSA)	
Máscara	ID-One Cosmo 64 v5	
Nível de Segurança do Chip Criptográfico	Nível 3 da certificação FIPS 140-2	
Dimensões:	61mm x 23mm x 12mm	
Peso:	8g	
Dissipação de Energia:	< 250 mW	
Temperatura de Operação:	0 até 70°C	
Temperatura de Armazenamento:	-20 até 85°C	
Faixa de umidade:	0 até 100% - 0 até 100% sem condensação	
Conector:	USB (Universal Serial Bus), tipo A, 1.0 compatível com 2.0	
Chassi:	Tipo tamper evident	
LED:	Monocromátrico	
Retenção de Dados de memória:	10 anos	
Capa protetora do conector USB	Sim	

4.2 Requisitos mínimos do sistema:

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

Sistema Operacional	Windows 98SE, ME, 2000, 2003, XP ou Linux (kernel 2.4 ou mais recente)	
Espaço em disco	Pelo menos 10 MB	
Porta USB	Pelo menos uma porta USB tipo A livre	

Direitos	O usuário deverá ter direito de instalar dispositivos no sistema operacional
	operaciónai

4.3 Vantagens Oferecidas pelo Token USB ProToken

- 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 ProToken possui memória segura para armazenar simultaneamente certificados digitais, chaves privadas, senhas e outras credenciais pessoais, ou seja, suporte a múltiplas aplicações PKI.
- Alta confiabilidade: o Protoken pode armazenar de forma segura credenciais por pelo menos 10 anos.

4.4 Recursos do Hardware

- Criptografia: o dispositivo suporta os seguintes algoritmos: RSA 1024bits e 2048bits (assinatura e verificação), DES, 3DES, SHA-1, SHA-2 (256), AES (128 bits), Elliptic Curves (EC-DSA).
- Geração do par de chaves: o par de chaves RSA 1024bits 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 ProToken. O sistema de arquivos permite que usuários definam um ou mais privilégios de segurança para o gerenciamento de chave.

4.5 Arquitetura

É oferecida uma API padrão PC/SC. Desenvolvedores podem fazer uso da função padrão Microsoft Win32 PC/SC para manipular o **ProToken**.



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

Camada Hardware: consiste no circuito do dispositivo, programa firmware e cabo de conexão. Ele troca dados com o computador via protocolo de comunicação USB da porta USB.

Camada Kernel Driver: manipula a interação de dados entre o PC e a Camada de Hardware, e o acesso ao Token requer a camada de aplicação superior. É a interface do driver PC/SC padrão. As camadas de aplicação superiores podem acessar o **ProToken** através do conjunto de funções padrão Win32 PC/SC

Camada Interface do Usuário: as interfaces nesta camada são a PKCS#11 API e a Microsoft CryptoAPI. Elas são suportadas por interfaces inferiores, compatíveis com as aplicações existentes e podem ser desenvolvidas novamente. Por exemplo, algumas aplicações requerem que os usuários assinem digitalmente o conteúdo que eles submetem pelo navegador com o **ProToken**. Funções como esta requerem a camada de interface superior.

Camada Aplicação: programas na camada de aplicação incluem geralmente aplicações disponíveis. As interfaces fornecidas pela Feitian são baseadas nos padrões da indústria e são conhecidos da maioria dos desenvolvedores. Os desenvolvedores devem integrar suas aplicações com o **ProToken** usando as interfaces fornecidas.

5. Instalando o software do ProToken

5.1 Instalação nos Sistemas Operacionais Windows 2000, XP e 2003.

Para instalar o software do **ProToken**, 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 ProToken runtime.exe.

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

🕖 Instalação do ePass2000 V1.0.6.0120			
	Bem-vindo ao Assistente de Instalação do ePass2000 Este assistente o guiará durante a instalação do ePass2000. É recomendado que você feche todas as outras aplicações antes de iniciar a Instalação. Isto possibilitará fazer update dos arquivos do sistema sem reiniciar o computador. Clique em "Avançar" para continuar.		
	Avançar > Cancelar		

b) 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*

🚯 Instalação do ePass2000 V1.0.6.0120	
Opções Opções do SmartCard	
Por favor selecione o recurso smartcard logon, o qual ?necessário para sistema	de smartcard
Suporte para sistema de smartcard logon em rede ou VPN.	
Windows Installer	Cancelar

^{*} 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 ProToken;

🚯 Instalação do ePass2000 V1.0.6.0120		_ 🗆 🗵
Instalando Por favor, aguarde enquanto o ePass2000 está	sendo instalado.	
Copiando ePass2000 Instalando arquivos		
Windows Installer		
	<⊻oltar <u>A</u> vançar>	Cancelar

d) Se durante a instalação, você receber uma janela com a mensagem "O software que você está instalando para este hardware: USB Smart Chip Device não passou no teste do logotipo do Windows que verifica sua compatibilidade com o Windows XP", não se preocupe, clique no botão "Continuar assim mesmo" para continuar a instalação.

ío de hardware
O software que você está instalando para este hardware: USB Smart Chip Device
não passou no teste do logotipo do Windows que verifica sua compatibilidade com o Windows XP. (Por que este teste é importante.)
A continuação da instalação deste software pode prejudicar ou desestabilizar o correto funcionamento do sistema no momento ou no futuro. A Microsoft
Continuar assim mesmo

e) Clique no botão "Terminar" para concluir a instalação do Runtime.

🚯 Instalação do ProToken		
	Concluindo o Assistente de Instalação do ProToken Seu computador deve ser reiniciado para concluír a instalação do ProToken. Você quer reiniciar agora? Reiniciar Agora C Eu quero reiniciar manualmente depois	
	< <u>V</u> oltar <u>T</u> erminar ⊂a	ancelar

e) Conecte o seu ProToken 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 do ProToken ficará piscando.

5.2 Instalação nos Sistemas Operacionais Windows 98SE e Windows ME

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 ProToken runtime.exe.

🕔 Instalação do ProToken	
	Bem-vindo ao Assistente de Instalação do ProToken Este assistente o guiará durante a instalação do ProToken. É recomendado que você feche todas as outras aplicações antes de iniciar a Instalação. Isto possibilitará fazer update dos arquivos do sistema sem reiniciar o computador. Clique em "Avançar" para continuar.
	<u>Avançar≻</u> Cancelar

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 ProToken;

🕖 Instalação do ProToken	
Instalando Por favor, aguarde enquanto o ProToken está sendo instalado.	
Instalando ProToken driver	
Windows Installer	
< <u>⊻</u> oltar <u>A</u> van	çar > Cancelar

c) Clique no botão "Terminar" para reiniciar o Windows e concluir a instalação do Runtime;

🕔 Instalação do ProToken		- 🗆 🗵
	Concluindo o Assistente de Instalação do ProToken Seu computador deve ser reiniciado para concluír a instalação do ProToken. Você quer reiniciar agora? Reiniciar Agora C Eu quero reiniciar manualmente depois	
	< <u>⊻</u> oltar <u>T</u> erminar C	ancelar

d) Conecte o seu ProToken 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 do ProToken ficará piscando.

Caso você receba um alerta de segurança, não se preocupe, este é um recurso do seu ProToken. Caso você deseje alterar o PIN do seu dispositivo, basta dar um clique no botão "OK" (figura 6.5). Se desejar não alterar o PIN, basta habilitar a caixa de verificação "Eu já alterei o PIN, não pergunte de novo!" e a seguir clicar no botão "OK" (figura 6.6).

ProToken - Alerta de Segurança 🔀		ProToker	n - Alerta de Segurança 🔀
⚠	Primeira utilização após a inicialização. Se você alterou o PIN de Fábrica, ignore este alerta. Caso contrário, clique no botão OK.	♪	Primeira utilização após a inicialização. Se você alterou o PIN de Fábrica, ignore este alerta. Caso contrário, clique no botão OK.
🔲 Eu alterei o PIN, não pergunte de novo!			Eu alterei o PIN, não pergunte de novol
	OK Cancelar		OK Cancelar
	Figura 6.5		Figura 6.6

5.3 Sobre o Monitor de Certificados do ProToken

O Monitor de Certificados do ProToken é uma ferramenta que é carregada na inicialização do Windows e que permite ao proprietário do dispositivo alterar o PIN, configurar o tempo de vida do PIN, visualizar, remover e registrar certificados do repositório do Windows.

5.4 Alterando o PIN

Para alterar o PIN do seu dispositivo, dê dois cliques no ícone do Monitor de Certificados 🌌 que está localizado na área de notificação do Windows. Na janela do Monitor, dê um novo clique no botão "Alterar PIN"

PRONOVA - Monitor de Certificados	
Monitor de Certificados	www.pronova.com.br
PIN-	
Selecione um Token para alterar o PIN.	PIN <u>T</u> imeout
PROTOKEN	Alterar <u>P</u> IN
Certificados	
<u>⊻</u> er <u>P</u> rotocolar	<u>R</u> emover

Na janela "Alterar o PIN do Token", digite o atual valor do PIN do seu dispositivo. Se esta for a primeira utilização, digite "12345678" (sem as aspas). Nos campos seguintes, digite o NOVO PIN. Para continuar clique no botão "OK". Ao final você receberá a seguinte mensagem "PIN alterado com sucesso" (figura 6.9)

Alterar o PIN do Token 🛛 🗙	1
PIN ATUAL do Token:	
1111111	Informação 🔀
Digite um NOVO PIN (8 a 1000 caracteres):	PIN alterado com sucesso!
	· · · · · · · · · · · · · · · · · · ·
Confirme o NOVO PIN do Token:	ОК
	Figura 6.9
OK Cancelar	

Se ao clicar no botão "OK" você receber a mensagem "Falha na alteração do PIN" [0x000000A0] (figura 6.10), certamente o valor informado no campo "PIN atual do Usuário" está incorreto, verifique-o e digite-o novamente o atual PIN do ProToken e clique no botão "OK" para continuar. Se esta mensagem persistir, tenha cuidado para não exceder as cinco tentativas consecutivas de acerto do PIN, do contrário, você receberá a mensagem "O PIN está travado, por favor, entre em contato com o seu Administrador!" (figura 6.11). Se você receber esta mensagem, consulte o Tópico 7.3 Destravando o PIN do Usuário.



Erro	×
8	O PIN está travado, por favor entre em contato com o seu Administrador!
	OK
	Figura 6.11

5.5 Configurando o Tempo de Vida do PIN do ProToken

Você poderá definir o tempo de vida do PIN do seu ProToken. 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 ProToken.

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

PRONOVA - Monitor de Certificados
PIN Selectione um Token para alterar o PIN. PINimeout PROTOKEN Alterar PIN
Certificados
<u>⊻</u> er <u>P</u> rotocolar <u>R</u> emover

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".

C	onfiguração do Tempo de Vida do PIN	×
	Selecione a opção de controle do tempo de vida do PIN	
	C PIN ativo enquanto o Token estiver conectado na porta USB.	
	 Tornar o PIN do Token inativo após minutos. 	
	OK Cancelar	

5.6 Visualizando os certificados armazenados no ProToken

Para visualizar o(s) certificado(s) armazenado(s) seu dispositivo, dê dois cliques no ícone do Monitor de Certificados Mue está localizado na área de notificação do Windows. Na janela do Monitor, selecione o certificado e depois dê um clique no botão "Ver".

PRONOVA - Monitor de Certificados	
Monitor de Certilicados	www.pronova.com.br
PIN	
Selecione um Token para alterar o PIN.	PIN <u>T</u> imeout
PROTOKEN	Alterar <u>P</u> IN
Certificados	
PROTOKEN	
Ver <u>Protocolar</u>	<u>R</u> emover

Uma nova janela chamada "Certificates Daemon" será exibida, nela você terá condições de ver todas as informações do seu certificado digital (figura 6.15). Para fechar esta janela, clique no botão "OK".

Certificates Daemon		? ×
Geral Detalhes Caminho de cer	tificação	
Mostrar: <a> 		
Campo Versão Número de série Algoritmo de assinatura Emissor Válido a partir de Válido até Assunto Chave pública	Valor V3 4c 01 8e 17 00 00 00 00 00 09 sha IRSA PRONOVA, SUPORTE, PRONO sexta-feira, 8 de setembro de sábado, 8 de setembro de 200 Mauricio Girão Plata, SUPORTE RSA (2048 Bits)	
Editar p	ropriedades	/0
		Figura 6.1

5.7 Removendo um certificado do repositório do Windows

Todos os certificados digitais que estão armazenados no ProToken são transferidos automaticamente para o repositório do Windows a partir do momento em que o dispositivo é conectado na porta USB, todavia se você desejar que um determinado certificado não seja registrado automaticamente, dê dois cliques no ícone do Monitor de Certificados in que está localizado na área de notificação do Windows. Na janela do Monitor, selecione o certificado e depois dê um clique no botão "Remover". Ao final você receberá a mensagem "Certificado removido do registro com sucesso!" (figura 6.17)

Monitor de Certificados do ProToken	
Monitor de Certificado	
Monnor de Cenincado.	> www.protoken.com.br
PIN	
Selecione um Token para alterar o PIN.	PIN <u>T</u> imeout
ProToken	▼ Alterar o <u>P</u> IN
- Carlina das	
Mauricio Girão Plata's PRON	IDVAID
<u>V</u> er <u>P</u> rotocolar	<u>R</u> emover
	Figura 6.16
Certificates Daemon	X
Certificado removido do regi	stro com sucesso!
ОК	Figura 6.17

5.8 Registrando um certificado no repositório do Windows

Se você desejar que os certificados que não são registrados de forma automática no repositório do Windows voltem a ser registrados automaticamente, dê dois cliques no ícone do Monitor de

Certificados Ma que está localizado na área de notificação do Windows. Na janela do Monitor, selecione o certificado e depois dê um clique no botão "Protocolar". Ao final você receberá a mensagem "Certificado registrado com sucesso!" (figura 6.19)

Monitor de Certificados do ProToken	
Monitor de Certilicados	L
	www.protoken.com.br
_ PIN	
Selecione um Token para alterar o PIN.	PIN <u>T</u> imeout
ProToken 💌	Alterar o <u>P</u> IN
Certificados	
ProToken	
Mauricio Girão Plata's PRONOVA	A ID
Ver Protocolar	Bemover
Terestored	
	Figura 6.18

Certificat	es Daemon 🛛 🗙	
į	Certificado registrado com sucesso!	
	OK	Figura 6.19

6. Sobre o Gerenciador do ProToken

O Gerenciador e uma ferramenta utilizada para realizar operações que não estão presentes no Monitor de Certificados do ProToken. Veja a seguir as janelas principais do Gerenciador PKI ePassNG



Ao clicar em um slot, eis a tela do Gerenciador PKI

😹 Gerenciador PKI - ePassNG (Administrador)				
Arquivo(A) Ver(V) Operação(O) Ajuda(1) Barra de Menu				
Lista de Slots FT OCS 0 [ProToken] Gerenciamento de Dados Área de Gerenciament o de dados	Detalhes do Slot: Campo Valor Descrição FT OCS Fabricante Feitian Flacs Πν∩ΠΠΩ ↓ Detalhes do Token:	3 0 Technologies Co., Ltd. 100071 CKF TOKEN PRES		
Operações que requerem o uso do PIN	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máx. de sess Número Máx. de sess	Valor ProToken Feitian Technologies Co., I ePassHD 77E 910000090006A [0x0000040D] CKF_RNG I 0	_td. CKF_LOGIN_REQUIRED	
Operações que requerem o uso do PUK	Operações permitidas ao l Login Operações permitidas ao A Alterar PUK	Jsuário: Alterar PIN Administrador: Destravar PIN	Renomear Token Inicializar Token	

6.1 O que é o PUK (PIN unlock key)?

O PUK (PIN unlock key) é um código máster que permite ao usuário recuperar o PIN do Usuário e, também Inicializar (formatar) o ProToken. O valor de fábrica deste código é "12345678" (sem as aspas).

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

6.1.1 Como alterar o PUK?

Esta é uma tarefa muito simples. Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR do Windows.

à Gerenciador PKI ePassNG (Admin	istrador)		
Arquivo (A) Ver (V) Operação (O) Aj	juda (J)		
Arquivo (A) ver (y) Operação (y) A Lista de Slots FT SCR2000 0 <token enc<br="" não="">FT SCR2000A 0 <token enc<br="" não="">FT SCR2000A 0 <token er<br="" não="">FT SCR2000C 0 <token er<br="" não="">FT SCR2000C 1 <token er<br="" não="">FT SCR2000C 1 <token er<br="" não="">FT OCS 0 [PROTOKEN]</token></token></token></token></token></token>	Informações dos Slots: Descrição FT SCR2000 0 FT SCR2000A 0 FT SCR2000A 1 FT SCR2000C 0 FT SCR2000C 1 FT OCS 0	Status do Dispositivo <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> Token não encontrado> Token presente e pronto p</token></token></token></token></token>	Fabricante Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co

Clique no slot referente ao seu ProToken para que as opções de operação sejam exibidas

à Gerenciador PKI - ePassNG (Adm	ninistrador)		
Arquivo(<u>A</u>) Ver(<u>V</u>) Operação(<u>O</u>) Aju	ida(<u>]</u>)		
 Lista de Slots FT SCR2000 0 <cartão en<="" li="" não=""> FT SCR2000 1 <cartão en<="" li="" não=""> FT SCR2000A 0 <cartão e<="" li="" não=""> FT SCR2000C 0 <cartão e<="" li="" não=""> FT SCR2000C 1 <cartão e<="" li="" não=""> FT SCR2000C 1 <cartão e<="" li="" não=""> FT SCR2000C 2 <cartão e<="" li="" não=""> FT SCR2000C 2 <cartão e<="" li="" não=""> </cartão></cartão></cartão></cartão></cartão></cartão></cartão></cartão>	Detalhes do Slot: Campo Valor Descrição FT OCS Fabricante Feitian Flace ∏ov0001 ◀ Detalhes do Token:	6 0 Technologies Co., Ltd. 100071 CKF TOKEN PRESEI	
E SUPORTE	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máx. de sess Número Máx. de sess	Valor SUPORTE Feitian Technologies Co., Lto ePassHD 6062690000207900 [0x0000040D] CKF_RNG C 0 0	I. KF_LOGIN_REQUIRED
	Atividades permitidas ao L	Isuário:	
	Login	Alterar PIN	Renomear Token
	Atividades do Administrad	or (requer PUK):	
I	Alterar PUK	Destravar PIN	Formatar Token

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

Alterar o PUK do Token	×
Digite o ATUAL PUK:	
Digite um NOVO PUK (8 a 1000 caracteres):	
Confirme o NOVO PUK:	
OK Cancelar	

Se esta for a sua primeira utilização, no campo 'Por favor, informe o PUK', digite 12345678 que é o valor de fábrica do PUK. No campo 'Informe PIN' digite o PIN que você deseja para o seu dispositivo. Confirme este PIN no campo 'Confirme PIN'. Se desejar dar um nome para o seu ProToken, no campo 'Informe nome do Token', digite, por exemplo, o seu nome. Para concluir esta operação, clique no botão "OK" e aguarde a exibição da seguinte mensagem:



6.2. O que é o PIN do Usuário

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 (três) tentativas consecutivas de acerto desta senha. Ao contrário do PUK, você poderá destravar o PIN do Usuário (mais informações, consulte o tópico 7.3 "Destravando o PIN do Usuário").

6.2.1 Alterando o PIN do Usuário

Para alterar o PIN, conecte o seu dispositivo em uma porta USB e em seguida execute o *Gerenciador* a partir do atalho criado em INICIAR do Windows.

à Gerenciador PKI ePassNG (Admin	iistrador)		
Arquivo (A) Ver (V) Operação (O) Aj	juda (J)		
Arquivo (A) Ver (Y) Operação (Q) A Ista de Slots FT SCR2000 0 <token enc<="" não="" td=""> FT SCR2000 1 <token enc<="" não="" td=""> FT SCR2000A 0 <token enc<="" não="" td=""> FT SCR2000A 0 <token er<="" não="" td=""> FT SCR2000A 1 <token er<="" não="" td=""> FT SCR2000C 0 <token er<="" não="" td=""> FT SCR2000C 0 <token er<="" não="" td=""> FT SCR2000C 1 <token er<="" não="" td=""> FT SCR2000C 1 <token er<="" não="" td=""> FT SCR2000C 1 <token er<="" não="" td=""> FT OCS 0 [PROTOKEN] FT OCS 0 [PROTOKEN]</token></token></token></token></token></token></token></token></token></token>	Informações dos Slots: Descrição FT SCR2000 0 FT SCR2000 1 FT SCR2000A 0 FT SCR2000A 0 FT SCR2000C 0 FT SCR2000C 1 FT OCS 0	Status do Dispositivo <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> Token presente e pronto p</token></token></token></token></token>	Fabricante Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co
T	<		

Clique no slot referente ao seu ProToken para que as opções de operação sejam exibidas

à Gerenciador PKI - ePassNG (Adn	ninistrador)		
Arquivo(A) Ver(V) Operação(O) Aju	ıda(<u>]</u>)		
Lista de Slots FT SCR2000 0 <cartão en<br="" não="">FT SCR2000 1 <cartão en<br="" não="">FT SCR2000A 0 <cartão e<br="" não="">FT SCR2000C 0 <cartão e<br="" não="">FT SCR2000C 1 <cartão e<br="" não="">FT SCR2000C 2 <cartão e<br="" não="">FT SCR2000C 3 <cartão e<="" não="" td=""><td>Detalhes do Slot: Campo Valor Descrição FT 0CS Fabricante Feitian Flans Ωνηθηρ Φ Detalhes do Token:</td><td>) 0 Technologies Co., Ltd. 100071 CKF TOKEN PRESE</td><td></td></cartão></cartão></cartão></cartão></cartão></cartão></cartão>	Detalhes do Slot: Campo Valor Descrição FT 0CS Fabricante Feitian Flans Ωνηθηρ Φ Detalhes do Token:) 0 Technologies Co., Ltd. 100071 CKF TOKEN PRESE	
FT OCS 0 [SUPORTE]	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máx. de sess Número Máx. de sess	Valor SUPORTE Feitian Technologies Co., Ltr ePassHD 6062690000207900 [0x0000040D] CKF_RNG C 0 0	d. KF_LOGIN_REQUIRED
• • •	Atividades permittades do E	Alterar PIN or (requer PUK): Destravar PIN	Renomear Token Formatar Token

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

Alterar o PIN do Token	×
Digite o ATUAL PIN:	
Digite um NOVO PIN (8 a 1000 caracteres):	
Confirme o NOVO PIN:	
OK Cancelar	

Se você não formatou o seu dispositivo, certamente ele ainda deverá estar com o PIN de fábrica que é "12345678" (sem as aspas). Neste caso, no campo 'Favor informar antigo PIN', digite 12345678 e nos campos 'Digite o 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 do Token alterado com sucesso!' seja exibida.

6.3 Destravando o PIN do Usuário

Para destravar o PIN do Usuário, conecte o seu dispositivo em uma porta USB e execute o Gerenciador a partir do atalho criado em INICIAR do Windows.

à Gerenciador PKI ePassNG (Admi	nistrador)		
Arquivo (A) Ver (V) Operação (O) A	Ajuda (])		
Arquivo (A) Ver (V) Operação (Q) A ista de Slots FT SCR2000 0 <token enc<br="" não="">FT SCR2000 1 <token enc<br="" não="">FT SCR2000A 0 <token enc<br="" não="">FT SCR2000A 0 <token enc<br="" não="">FT SCR2000A 1 <token enc<br="" não="">FT SCR2000C 0 <token enc<br="" não="">FT SCR2000C 0 <token enc<br="" não="">FT SCR2000C 1 <token enc<br="" não="">FT SCR2000C 1 <token enc<br="" não="">FT OCS 0 [PROTOKEN]</token></token></token></token></token></token></token></token></token>	Ajuda (1) Informações dos Slots: Descrição FT SCR2000 0 FT SCR2000 1 FT SCR2000A 0 FT SCR2000A 1 FT SCR2000C 0 FT SCR2000C 1 FT OCS 0	Status do Dispositivo <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> Token presente e pronto p</token></token></token></token></token></token>	Fabricante Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co
• • • • • • • • • • • • • • • • • • •			

Clique no slot referente ao seu ProToken para que as opções de operação sejam exibidas

🔉 Gerenciador PKI - ePassNG (Adn	ninistrador)		
Arquivo(A) Ver(V) Operação(O) Aju	uda(<u>J</u>)		
 Lista de Slots FT SCR2000 0 <cartão en<="" li="" não=""> FT SCR2000 1 <cartão en<="" li="" não=""> FT SCR2000A 0 <cartão e<="" li="" não=""> FT SCR2000C 0 <cartão e<="" li="" não=""> </cartão></cartão></cartão></cartão>	Detalhes do Slot: Campo Valor Descrição FT 00 Fabricante Feitiar Flaos (000	S 0 1 Technologies Co., Ltd. 1000021 CKE_TOKEN_PRESEN	
FT SCR2000C 1 <cartao e<="" não="" td=""><td>•</td><td></td><td></td></cartao>	•		
FT SCR2000C 3 <cartão e<="" não="" td=""><td>Detalhes do Token:</td><td>0.1</td><td></td></cartão>	Detalhes do Token:	0.1	
	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máy, de sess	SUPORTE Feitian Technologies Co., Ltd ePassHD 6062690000207900 [0x0000040D] CKF_RNG Cl 0	
	Número Máx. de sess.	Ŏ	▼
	Atividades permitidas ao	Usuário:	
	Login	Alterar PIN	Renomear Token
	Atividades do Administra	dor (requer PUK).	
	Alterar PUK	Destravar PIN	Formatar Token
······································			

Clique no botão 'Destravar PIN' para ter acesso a janela 'Destravar PIN do Usuário'

Destravar o PIN do Token	×
Digite o PUK do Token:	
Digite um NOVO PIN (8 a 1000 caracteres):	
Confirme o NOVO PIN:	
OK Cancelar	

No campo 'PUK', digite o PUK do seu dispositivo. Nos campos 'Informe Novo PIN' e 'Confirme Novo PIN' digite um novo PIN para o seu ProToken. Após preencher todos os campos, clique no botão OK e aguarde que a mensagem 'PIN do Token destravado com sucesso!'.

Gerenciador PKI - ePassNG		
į)	PIN do Token destravado com sucesso!	
	ОК	

6.4 Renomeando o dispositivo

Você poderá alterar o label (nome) do seu dispositivo a qualquer momento. Esta é a única tarefa que não exige a utilização do PIN ou do PUK do dispositivo. Para alterar o label do seu Token, clique no slot referente ao seu dispositivo e a seguir dê um novo clique no botão "Renomear Token" para que a janela "Renomear Token" seja exibida (figura 7.14). Nela, digite o NOVO label do seu dispositivo e clique no botão "OK" para continuar. Ao final uma mensagem será exibida (figura 7.15)

Renomear o Token	×
Atual nome do Token:	Gerenciador PKI - ePassNG
SUPORTE	
Informe um novo nome (máx. 32 caracteres):	Token renomeado com sucesso
SUPORTE	ОК
0K Cancelar	Figura 7.15
Figura 7.14	

6.5. Formatando o ProToken

Sempre que você julgar necessário apagar todo o conteúdo do ProToken, faça uso do recurso "Formatar Token" do Gerenciador PKI. Para tal, execute-o a partir do atalho que pode ser acessado a partir do botão "Iniciar do Windows.

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

😹 Gerenciador PKI ePassNG (Admin	iistrador)		
Arquivo (A) Ver (V) Operação (O) Aj	juda (])		
Arquivo (A) Ver (V) Operação (Q) Ar ista de Slots FT SCR2000 0 <token enc<br="" não="">FT SCR2000 1 <token enc<br="" não="">FT SCR2000A 0 <token er<br="" não="">FT SCR2000C 0 <token er<br="" não="">FT SCR2000C 0 <token er<br="" não="">FT SCR2000C 1 <token er<br="" não="">FT SCR2000C 1 <token er<br="" não="">FT OCS 0 [PROTOKEN]</token></token></token></token></token></token></token>	juda (2) Informações dos Slots: Descrição FT SCR2000 0 FT SCR2000 1 FT SCR2000A 0 FT SCR2000A 1 FT SCR2000C 0 FT SCR2000C 1 FT OCS 0	Status do Dispositivo <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> Token presente e pronto p</token></token></token></token></token></token>	Fabricante Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co
	•		

Clique no slot referente ao seu ProToken para que as opções de operação sejam exibidas

à Gerenciador PKI - ePassNG (Adn	ninistrador)		
Arquivo(A) Ver(V) Operação(O) Aju	uda(<u>J</u>)		
Lista de Slots FT SCR2000 0 <cartão en<br="" não="">FT SCR2000 1 <cartão en<br="" não="">FT SCR2000A 0 <cartão e<br="" não="">FT SCR2000C 0 <cartão e<br="" não="">FT SCR2000C 1 <cartão e<br="" não="">FT SCR2000C 2 <cartão e<br="" não="">FT SCR2000C 2 <cartão e<="" não="" td=""><td>Detalhes do Slot: Campo Valor Descrição FT OCS Fabricante Feitian Flacs ΓΩνΩΩΩΩ ↓ Detalhes do Token:</td><td>3 0 Technologies Co., Ltd. 100071 CKE TOKEN PRESE</td><td></td></cartão></cartão></cartão></cartão></cartão></cartão></cartão>	Detalhes do Slot: Campo Valor Descrição FT OCS Fabricante Feitian Flacs ΓΩνΩΩΩΩ ↓ Detalhes do Token:	3 0 Technologies Co., Ltd. 100071 CKE TOKEN PRESE	
Ē-À FT OCS 0 [SUPORTE]	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máx. de sess Número Máx. de sess	Valor SUPORTE Feitian Technologies Co., Lt ePassHD 6062690000207900 [0x0000040D] CKF_RNG 0 0 0	d. CKF_LOGIN_REQUIRED
	Login Atividades do Administrad Alterar PUK	Alterar PIN Or (requer PUK): Destravar PIN	Renomear Token Formatar Token

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

Formatar o Token (Inicializar Setor PKI) 🔀				
Digite o ATUAL PUK do Token:				
10000				
Digite um NOVO PIN (8 a 1000 caracteres):				
Confirme o NOVO PIN do Token:				
Digite um nome para o Token (máx. 32 caract.)				
MGPLATA				
OK Cancelar				

No campo 'Por favor, informe o ATUAL PUK do Token' digite o PUK do seu Token. Nos campos 'Informe um NOVO PIN' e 'Confirme o NOVO PIN', digite um novo PIN para o seu ProToken. 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" e aguarde que a mensagem 'Token formatado com sucesso! Todas as informações que estavam armazenadas no Token foram apagadas!' seja exibida.

6.6 Visualizando dados armazenados no ProToken

Para visualizar os dados armazenados no ProToken, basta dar um clique no botão slot referente ao seu dispositivo e depois dar um novo clique no "Login" do Gerenciador PKI. Uma janela chamada "Login" (figura 7.2) será exibida, nela digite o PIN do seu dispositivo. Se o PIN informado estiver correto, você será redirecionado para a área "Gerenciamento de Dados" (figura 7.21). Nesta área, você poderá visualizar o certificado digital com o par de chaves, importar certificados (vide Tópico 11 Importando um certificado digital a partir de um arquivo), além de outras informações que estejam armazenadas no seu dispositivo.

💦 Gerenciador PKI - ePassNG (Administrador)				
Arquivo(<u>A</u>) Ver(<u>V</u>) Operação(<u>O</u>) Aju	uda(<u>J</u>)			
Uista de Slots ⊡- ॐ FT OCS 0 [ProToken]	Detalhes do Slot: Campo Valor Descrição FT OCS 0 Fabricante Feitian Technologies Co., Ltd. Flags IOV000000021 CKE TOKEN PRESENT LCKE REMOVARIE Detalhes do Token:			
	Campo Valor Nome do Token ProToken Fabricante Feitian Technologies Co., Ltd. Modelo ePassHD Número Serial 77E 910000090006A Flags [0x00080400] CKF_RNG CKF_LOGIN_REQUIRED Número Máx. de sessões 0 Número Máx. de sess 0 Operações permitidas ao Usuário: Login Login Alterar PIN		_td. CKF_LOGIN_REQUIRED ▼ Renomear Token	
	Operações permitidas ao A Alterar PUK	Administrador: Destravar PIN	Inicializar Token	





Figura 7.21

Recomendamos que você tenha muito cuidado com as informações que estão armazenadas no seu dispositivo, pois se elas foram apagadas, NÂO SERÁ POSSÍVEL RESTAURÁ-LAS! Portanto, antes de excluir qualquer objeto na área de Gerenciamento de Dados do Gerenciador PKI, tenha absoluta certeza de que tal objeto não será mais necessário para você.

Se você não estiver certo da importância de um determinado objeto, consulte-nos!

Se você codificou (criptografou) e-mails ou arquivos com dados que estão armazenados no seu Token, **NUNCA** apague qualquer objeto do tipo **chave privada** que lá esteja armazenada, pois ela sempre é utilizada nos processo de codificação e decodificação.
7. Instalando um certificado digital emitido por uma AC Microsoft no ProToken

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-Brasiil, consulte <u>www.fti.gov.br</u>.

Instalar um certificado digital no ProToken é uma tarefa muito simples. Entretanto, é importante ressaltar que o processo deverá ser concluído na mesma máquina onde o processo de solicitação foi iniciado.

Você poderá instalar qualquer certificado digital cujo par de chaves RSA seja de até 2048bits, inclusive 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 ProToken. Com o seu dispositivo conectado, acesse a página web onde será feita a solicitação do certificado digital.

Nosso exemplo fará uso de uma Autoridade Certificadora Microsoft e 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*.

Microsoft Certificate Services - PRONOVA SOLUÇÕES INTELIGENTES	
<u>A</u> rquivo E <u>d</u> itar E <u>x</u> ibir <u>E</u> avoritos F <u>e</u> rramentas Aj <u>u</u> da	
🎯 • 🕥 - 📓 🙆 🏠 🔎 🜟 🧐 🍰 💌 • 🛄 🛍	
Endereço 🗃 https://192.168.0.100/certsrv/certrqma.asp 🔽 💽 Ir	Links 📆 👻
	·
Microsoft Certificate Services PRONOVA	Home
Advanced Certificate Request	
Identifying Information:	
Name: Suporte Técnico Pronova Soluções Inteligentes	
E-Mail: suporte@pronova.com.br	
Company: PRONOVA SOLUÇÕES INTELIGENTES	
Department: SUPORTE	
Country/Region: BR	
Intended Purpose:	
E-Mail Protection Certificate	
Key Options:	
CSP: FEITIAN ePassNG RSA Cryptographic Service Provider	_
Key Usage: O Exchange O Signature O Both	
Key Size: 2048 Min: 512 Max:2048 (common key sizes: 512 1024 2048)	
	•

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".

Verificação do PIN do Usuário					
Olá PROTOKEN! Agora é necessário verificar o seu PIN.					
PIN do Usuário):				
	<u>L</u> ogin	Cancelar			

Se o PIN informado for o correto, o par de chaves será gerado dentro do ProToken e ao término deste processo o usuário é encaminhado para a próxima página.

Microsoft Certificate Services - PRONOVA SOLUÇÕES INTELIGENTES	
<u>A</u> rquivo E <u>d</u> itar E <u>x</u> ibir <u>F</u> avoritos F <u>e</u> rramentas Aj <u>u</u> da	
😋 • 🕥 - 💌 🖻 🏠 🔎 🧙 🏵 🔝 - 🤤 🏭 -	
Endereço 🗃 https://192.168.0.100/certsrv/certfnsh.asp 🔽 🄁 Ir	Links 📆 👻
Microsoft Certificate Services PRONOVA	<u>Home</u>
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
	V
🕲 📔 🖯 🔛 🔁 🖓 🔛 Internet	t //.

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

Microsoft Certificate Services - PRONOVA SOLUÇÕES INTELIGENTES	<u>_ ×</u>
<u>A</u> rquivo E <u>d</u> itar E <u>x</u> ibir <u>E</u> avoritos F <u>e</u> rramentas Aj <u>u</u> da	
🕒 • 🕞 · 🖹 🗟 🏠 🔎 🧙 🏵 😒 • 😓 🖬 • 🛄 🛍	
Endereço 💩 https://192.168.0.100/certsrv/certrmpn.asp 💽 💽 Ir	Links 📆 👻
	<u> </u>
Microsoft Certificate Services PRONOVA	Home
Certificate Installed	
Your new certificate has been successfully installed.	
Concluído	t //

Pronto, seu certificado já está armazenado no ProToken!

8. Integrando o Token USB ProToken com o Mozilla Firefox 1.5x

ATENÇÃO: os procedimentos abaixo mencionados neste tópico não precisam ser realizados com o navegador Microsoft Internet Explorer!!!

Para integrar o ProToken ao Mozilla Firefox sigas as seguintes instruções:

a) Execute o Firefox

b) Clique em "Ferramentas" da barra de menu e em seguida clique em "Opções"



c) Na janela opções clique na guia "Segurança" e em seguida no botão "Disp. De Segurança"

Opções						×
1				4	203	
Geral	Privacidade	Conteúdo	Abas	Downloads	Avançado	
Geral At	ualizações Se	guranca				
ocidi j ni						1
- Protoc	olos					
I St	SL <u>2</u> .0		•	SSL <u>3</u> .0		
Π	.S <u>1</u> .0					
Certific	cados					
Quand	lo um site requis	sitar um certifi	cado:			
● <u>S</u> e	elecionar um au	tomaticamente	e 🔿 Pe	rgu <u>n</u> tar quando	necessário	
Certi	ficados <u>R</u> ev	/ogações	<u>V</u> erificaçã	o <u>D</u> isp. de	segurança	
-						
				Ca	ncelar	Ajuda

d) Na janela "Gerenciador de dispositivos de segurança", clique no botão "Carregar"

🍪 Gerenciador de dispositivos de segurança			<u> </u>
Dispositivos e módulos de segurança	Detalhes Módulo Caminho	Valor ePassNG c:\WINDOWS\sy	Logar Deslogar Modificar senha Carregar Descarregar Ativar FIPS
	1		ОК

e) Clique no botão 'Procurar' da janela 'Carregar dispositivo PKCS#11'

😻 Carregar dispositivo PKCS#11	
Forneça a informação para o módulo que você quer adicion	ar.
Nome do módulo: Novo módulo PKCS#11	
Nome de arquivo do módulo:	Procurar
ОК	Cancelar

f) Na janela "Selecione um dispositivo PKCS#11 para carregar", localize no diretório System32 do Windows o arquivo ngp11v211.dll e em seguida clique no botão "Abrir"

Selecione um dis	positivo PKCS#11 para car	regar		? X
E <u>x</u> aminar:	🗀 Mozilla Firefox	•) 🌶 📂 🖽	
Documentos recentes Desktop Desktop Meus documentos Meu computador	 chrome components defaults extensions greprefs plugins res searchplugins uninstall updates autoreg AccessibleMarshal.dll browserconfig.properties firefox.exe install.log install_status.log 	 install_wizard.log js3250.dll ILCENSE nspr4.dll nss3.dll plc4.dll plds4.dll README.txt smime3.dll softokn3.chk softokn3.dll ssl3.dll updater.exe updater.ini xpcom.dll 	Sxpcom_compat.dll xpcom_core.dll xpicleanup.exe xpistub.dll	
Meus locais de rede	Nome do arquivo:)WS\system32\ngp11v211.d		orir
	Arquivos do <u>ti</u> po: Todos os	arquivos	▼ Canc	elar

g) Altere o registro "Novo módulo PKCS#11" no campo "Nome do módulo" para ePassNG. Uma vez que você informou o arquivo ngp11v211.dll, clique no botão "OK" da janela "Carregar dispositivo PKCS#11"

Carregar dispositivo	PKCS#11	
Forneça a informação para o r	módulo que você quer adici	onar.
Nome do módulo: Novo mód	lulo PKCS#11	
Nome de arquivo do módulo:	C:\WINDOWS\system32	Arquivo
OK Cancelar		

h) Uma janela chamada "Confirmar" irá surgir. Clique no botão "OK" para continuar



i) Novos itens serão adicionados à janela "Gerenciador de dispositivos de segurança". Clique no botão "OK" desta janela para continuar



j) Para continuar, clique no botão "OK" da janela "Opções" para fechar esta janela.

9. Utilizando o Mozilla Firefox 1.5 para alterar o PIN do Usuário do ProToken

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"

Opções						×
1		$\langle \langle \rangle$		<u> </u>	E Contraction	
Geral	Privacidade	Conteúdo	Abas	Downloads	Avançado	
Geral At	tualizações Se	gurança				
Protoc	colos					
S:	SL <u>2</u> .0		V	SSL <u>3</u> .0		
Π 🖸 🛛	LS <u>1</u> .0					
⊂ Certifi	cados					
Ouand	to um site reauis	itar um certifi	cado:			
• s	elecionar um au	tomaticamente	e O Per	rountar quando	necessário	
				3-7		
Certi	ficados Rev	/ogações	Verificação	Disp. de	seguranca	
					ncolor	Aiuda
						Ajuua

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

😺 Gerenciador de dispositivos de segurança			
Dispositivos e módulos de segurança	Detalhes Status Descrição Fabricante HW Version FW Version Label Fabricante Número de série HW Version FW Version	Valor Logado FT OCS 0 Feitian Technolo 1.0 1.0 PROTOKEN Feitian Technolo 77E9100000900 1.0 1.0	Logar Deslogar Modificar senha Carregar Descarregar Ativar FIPS
			ОК

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

Modificar a senha mestra		×
Dispositivo de segurança:	PROTOKEN	
Senha mestra atual:	******	ן ן
Nova senha:	******	
Confirmar a nova senha:	*******	
Medidor de qualidade da se	enha	ך ר
		J
	OK Cancelar	

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



	😻 Gerenciador de dispositivos de segurança					_ 🗆 ×
l	Dispositivos e módulos de segurança	ĺ	Detalhes	Valor	ĺ	Logar
l	NSS Internal PKCS #11 Module	1	Status	Não logado	1	
l	Serviços criptográficos gerais		Descrição	FT HID VSCR 4		Deslogar
l	Dispositivo de segurança (softw		Fabricante	Feitian Technolo		Modificar senha
l	 Builtin Roots Module 		HW Version	1.0		
l	Builtin Object Token		FW Version	1.0		Carregar
l	ePassNG		Label	ePass2000FT11		Descarregar
l	FT HID VSCR 0		Fabricante	Feitian Technolo		
l	FT HID VSCR 1		Número de série	0687212509311		Ativar FIPS
l	FT HID VSCR 2		HW Version	1.0		
l	FT HID VSCR 3		FW Version	1.0		
l	···ePass2000FT11					
l	FT HID VSCR 5					
l	ePass2000					
l						
l						
l						
l						
			l			
						ОК

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

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

Opções						×
				<u> </u>	No.	
Geral	Privacidade	Conteúdo	Abas	Downloads	Avançado	
Geral At	tualizações Se	gurança]
🔽 🔽 S	SL <u>2</u> .0			SSL <u>3</u> .0		
🛛 🗖 π	LS <u>1</u> .0					
L						
Certifi	cados ———					
Quand	lo um site requis	itar um certif	icado:			
• <u>S</u> e	elecionar um aut	tomaticament	e 🔿 Pe	rgu <u>n</u> tar quando	necessário	
<u>C</u> erti	ficados <u>R</u> ev	/ogações	<u>V</u> erificaçã	o <u>D</u> isp. de	segurança	
			C	ж Ca	ncelar	Ajuda

10. Importando um certificado digital para o ProToken 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 ProToken é necessário que você possua a senha deste seu arquivo. De posse deste arquivo e da senha do mesmo, siga os seguintes passos:

(ب	Evenute o	Caropolador	DIL de Dreteken	a partir do ata	albo origido po aru	na INICIAD da Mindaw
a	i execute o	Geleliciddol		a parili ao aic	ano chado no giu	

à Gerenciador PKI ePassNG (Admin	nistrador)		
Arquivo (A) Ver (V) Operação (O) A	.juda (J)		
Arquivo (A) Ver (V) Operação (Q) A FT SCR2000 0 < Token não enc FT SCR2000 1 < Token não enc FT SCR2000A 0 < Token não enc FT SCR2000A 0 < Token não er FT SCR2000A 1 < Token não er FT SCR2000C 0 < Token não er FT SCR2000C 1 < Token não er FT SCR2000C 1 < Token não er FT OCS 0 [PROTOKEN]	juda (1) Informações dos Slots: Descrição FT SCR2000 0 FT SCR2000 1 FT SCR2000A 0 FT SCR2000C 0 FT SCR2000C 1 FT OCS 0	Status do Dispositivo <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> <token encontrado="" não=""> Token não encontrado> Token presente e pronto p</token></token></token></token></token>	Fabricante Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co Feitian Technologies Co

Clique no slot referente ao seu ProToken para que as opções de operação sejam exibidas

凝 Gerenciador PKI - ePassNG (Adn	ninistrador)		
Arquivo(A) Ver(V) Operação(O) Aju	uda(<u>)</u>		
 Lista de Slots FT SCR2000 0 <cartão en<="" li="" não=""> FT SCR2000 1 <cartão en<="" li="" não=""> FT SCR2000A 0 <cartão e<="" li="" não=""> FT SCR2000C 0 <cartão e<="" li="" não=""> FT SCR2000C 1 <cartão e<="" li="" não=""> FT SCR2000C 1 <cartão e<="" li="" não=""> FT SCR2000C 2 <cartão e<="" li="" não=""> FT SCR2000C 2 <cartão e<="" li="" não=""> </cartão></cartão></cartão></cartão></cartão></cartão></cartão></cartão>	Detalhes do Slot: Campo Valor Descrição FT OCS Fabricante Feitian Flans Invn∩n ◀ Detalhes do Token:	5 0 Technologies Co., Ltd. INNN71 CKF TOKEN PRESE	
FOCS 0 [MGPLATA] Gerenciamento de Dados	Campo Nome do Token Fabricante Modelo Número Serial Flags Número Máx. de sess Número Máx. de sess	Valor MGPLATA Feitian Technologies Co., Lt ePassHD 6062690000207900 (0x0008040D) CKF_RNG 0 0 0	d. CKF_LOGIN_REQUIRED
<u>↓</u>	Atividades permitidas ao L Login Atividades do Administrad Alterar PUK	Isuário: Alterar PIN or (requer PUK): Destravar PIN	Renomear Token Formatar Token

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

Gerenciador	de Certificados - Lo	gin X	
PIN:			
	Login	Cancelar	



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.

Importar certificado	×
Caminho do certificado:	\frown
Senha do certificado:	\sim
OK	Cancelar

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

Importar certificado	×
Caminho do certificado:	
C:\Documents and Settings\NX9005\Meus d	
Senha do certificado:	
OK Cancel	ar

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



11. Configurando o Microsoft Outlook para usar um certificado armazenado no ProToken

Siga os passos apresentados neste tópico para que seja possível fazer uso de um certificado digital armazenado no ProToken.

- 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"

Preferência	s	Entrega de correio	Format	o de mensagen	n Ortografia
Seg	jurança		Outro	1	Fax
orreio eletrô	inico segu	iro			
Da 🗆	Criptogra	afar conteúdo e an	exos de m <u>e</u> nsag	iens sendo envi	adas
	Adicionar	assinatura <u>d</u> igital	a mensagens en	viadas	
Г	Enviar me	ensagem assinada	em <u>t</u> exto não cr	iptografado ao	enviar mens, assina
onfigurações	padrão:			-	Configurações
anguraçoc.					
orteúdo sec	uro		Mu		
onteúdo seg	juro	seguranca permite	m personalizar s	e os scripts e o	conteúdo ativo
orteúdo seg	juro zonas de lerão ser	segurança permite executados em me	em personalizar s ensagens HTML.	e os scripts e o Selecione a zor	conteúdo ativo na de segurança
orteúdo seg As poc do	juro zonas de lerão ser Microsoft	segurança permite executados em me Internet Explorer	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecion <mark>e</mark> a zor	conteúdo ativo na de segurança
orteúdo seg orteúdo seg poc do Zor	guro zonas de derão ser Microsoft na:	segurança permite executados em me Internet Explorer Sites restritos	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configurad	conteúdo ativo na de segurança
orteúdo seg As poc do <u>Z</u> or	guro zonas de derão ser Microsoft na:	segurança permite executados em me Internet Explorer Sites restritos	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç	conteúdo ativo na de segurança jões de zo <u>n</u> as
onteúdo seg As poc do <u>Z</u> or	guro zonas de derão ser Microsoft na:	segurança permite executados em me Internet Explorer Sites restritos	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç	conteúdo ativo na de segurança jões de zo <u>n</u> as
onteúdo seg orteúdo seg poc do Zor dentificacõe	guro zonas de lerão ser Microsoft na:	segurança permite executados em me Internet Explorer Sites restritos (Certificados)	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç	conteúdo ativo na de segurança jões de zo <u>n</u> as
onteúdo seg orteúdo seg poc do Zor dentificaçõe	guro zonas de s lerão ser Microsoft na: es digitas	segurança permite executados emme Internet Explorer Sites restritos (Certificados)	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç	conteúdo ativo na de segurança jões de zo <u>n</u> as
dentificaçõe	juro zonas de Jerão ser Microsoft na: es digitas ntificaçõe ntidade er	segurança permite executados em me Internet Explorer Sites restritos (Certificados) es digitais, ou certif m transações eletr	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç umentos que pe	conteúdo ativo na de segurança jões de zo <u>n</u> as
onteúdo seg orteúdo seg poc do Zor dentificaçõe iden	juro zonas de Jerão ser Microsoft na: es digitas ntificaçõe ntidade er	segurança permite executados em me Internet Explorer Sites restritos (Certificados) es digitais, ou certif m transações eletr	em personalizar s ensagens HTML. a ser usada.	e os scripts e o Selecione a zor Configuraç umentos que pe	conteúdo ativo na de segurança jões de zo <u>n</u> as
dentificaçõe	guro zonas de derão ser Microsoft na: es digitas ntificaçõe ntidade er	segurança permite executados em me Internet Explorer Sites restritos (Certificados) es digitais, ou certif m transações eletro <u>I</u> mportar/e	em personalizar s ensagens HTML. a ser usada. ficados, são docu ônicas. exportar	e os scripts e o Selecione a zor Configuraç umentos que pe <u>O</u> hter uma ide	conteúdo ativo na de segurança jões de zo <u>n</u> as ermitem provar a

 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";

elecione o certif	icado que deseja	a usar.		
Emitido para	Emitido por	Finalidades	Nome amig	Data de va.
mauricio	GlobalSign	<todas></todas>	Nenhum	31/3/2005
MAURICI	Autoridade	Autenticaç	Nenhum	29/5/2005
e		Ш		

- 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.

12. Configurando o Outlook Express para usar um certificado armazenado no ProToken

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..."

Ferramentas	Mensagem	Ajuda	
Enviar e rec	eber		•
Sincronizar	tudo		
Catálogo de	endereços	C	Ctrl+Shift+B
Adicionar re	metente ao C	atálogo de endereços	
Regras para	a mensagens		۲
Contas			
Opções			

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

	de mauricio@pronova.com.br 👘 💽 🔀					
Geral Servidores	Conexto Segurança Abançado					
Conta de email						
Digite o nome que você deseja dar aos servidores. Por exemplo, 'Trabalho' ou 'Servidor de email da Microsoft'.						
mauricio@prono	ova.com.br					
Informações sobre	o usuário					
No <u>m</u> e:	Mauricio Plata					
<u>O</u> rganização:	Pronova Soluções Inteligentes					
Emai <u>l</u> :	mauricio@pronova.com.br					
En <u>d</u> ereço para resposta:						
Incluir esta con	ta ao receber ou sincronizar emails					
	OK Cancelar Aplicar					

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

Propriedades	de mauri	cio@pronov	va.com.br 🛛 😢
Geral Servidores	Conexão	Segurança	Avançado
Certificado de auto Selecione o cer determinar a ide com esta conta	enticação tificado de a entificação dig	utenticação al gital usada par	paixo. Isso vai ra assinar mensagens
<u>C</u> ertificado:			Selecionar
Preferências de cr	iptografia —		
Selecione o cer incluídos nas m outras pessoas você com essa: Certificado:	tificado e o a ensagens qu possam envi s configuraçã	Igoritmo de cri le você assina ar mensagens íes.	iptografia. Eles serão ar digitalmente para que s criptografadas para
Co <u>r</u> inodao.			
Algoritmo:	3DES		▼
	ОК	Car	ncelar Aplicar

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

=	e ant	et bl. i	1	
Emitido para	Emitido por	Finalidades	Nome amig	Data de va
mauricio	GlobalSign	<lodas></lodas>	Nenhum	31/3/2005

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"

Propriedade:	s de mauri	cio@pronov	va.com.br	? 🗙
Geral Servidore	s Conexão	Segurança	Avançado	
Certificado de aut Selecione o ce determinar a ide com esta conta	enticação — rtificado de a entificação di a.	utenticação al gital usada pa	paixo. Isso vai ra assinar mensi	agens
<u>C</u> ertificado:	mauricio@p	pronova.com.b	or <u>S</u> elecio	nar
Preferências de c Selecione o ce incluídos nas n outras pessoas você com essa Ce <u>r</u> tificado:	riptografia	Ilgoritmo de cri le você assina ar mensagens ées.	iptografia. Eles s ar digitalmente p s criptografadas	serão ara que para nar
Algoritmo:	3DES		~	
	ОК	Car	ncelar /	Aplicar

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

	ncauo que ueseja	a usar.		
Emitido para	Emitido por	Finalidades	Nome amig	Data de va
mauricio	GlobalSign	<todas></todas>	Nenhum	31/3/2005

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"

ieral Servidon	es Conexão	Segurança	Avan	çado
Certificado de au	tenticação —			
Selecone o c deterninar a io com esta cont	ertificado de au dentificação dig ta.	utenticação al gita usada par	baixo, l ra assin	sso vai nar mensagens
<u>C</u> ertificado:	mauricio@p	oronova.com.b	or [Selecionar
Preferências de	criptografia —			
Selecione o c	ertificado e o al	lgoitmo de cri	ptograf	ia. Eles serão
Selecone o c incluídos nas outras pessoa	ertificado e o al mensagens que s possam envia	lgoitmo de cri e você assina ar mensagens	iptograf ar digita s cripto	ia. Eles serão Imente para qu grafadas para
Selecone o c incluídos nas outras pessoa você com ess	ertificado e o al mensagens qui is possam envia as configuraçõ	lgoîtmo de cri e você assina ar mensagens es.	iptograf ar digita s cripto	ia. Eles serão Imente para qu grafadas para
Selecone o c incluídos nas outras pessoa você com ess Ce <u>t</u> ificado:	ertificado e o al mensagens qui s possam envia as configuraçõ mauricio@p	Igoîtmo de cri e você assina ar mensagens es. pronova.com.t	ptograf ar digita s cripto	ia. Eles serão Imente para qu grafadas para S <u>e</u> lecionar
Selecone o c incluídos nas outras pessoa você com ess Ce <u>r</u> tificado: Algoritmo:	ertificado e o al mensagens qui s possam envia as configuraçõ mauricio@p 3DES	Igoitmo de cri e você assina ar mensagens es. pronova.com.t	ptograf ar digita s cripto	ia. Eles serão Imente para qu grafadas para <u>Se</u> lecionar
Selecone o c incluídos nas outras pessoa você com ess Certificado: Algoritmo:	ertificado e o al mensagens qui s possam envia as configuraçõ mauricio@p 3DES	Igoitmo de cri e você assina ar mensagens es. pronova.com.b	ptograf ar digita s cripto or	ia. Eles serão Imente para qu grafadas para <u>Se</u> lecionar
Selecone o c incluídos nas outras pessoa você com ess Certificado: Algoritmo:	ertificado e o al mensagens qui is possam envia as configuraçõ mauricio@p 3DES	Igoitmo de cri e você assina ar mensagens es. pronova.com.t	iptograf ar digita s cripto or	ia. Eles serão Imente para qu grafadas para <u>Se</u> lecionar
Selecone o c incluídos nas outras pessoa você com ess Certificado: Algoritmo:	ertificado e o al mensagens qui s possam enviz as configuraçõ mauricio@p 3DES	Igoitmo de cri e você assina ar mensagens es. pronova.com.t	ptograf ar digita s cripto or	ia. Eles serão Imente para qu grafadas para <u>Se</u> lecionar

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

Ferramentas	Mensagem	Ajuda		
Enviar e rec	eber			•
Sincronizar	tudo			
Catálogo de	endereços		Ctrl+Shift+B	i.
Adicionar re	metente ao C	atálogo de endereço:	1	
Regras para	a mensagens			•
Contas				
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"

) Opçõe	25		?
Geral	Ler Confirmações	Envio Redag	ção Assinaturas
Verific	car ortografia Segurança	Conexão	Manutenção
Proteçã	io contra vírus		
	Selecione a zona de segurança o	lo Internet Explorer a	ser usada:
S	Zona da Internet (menos :	segura, porém mais fu	incional)
-	 Zona de sites restritos (ma 	is segura)	
	Agisar quando outro aplicativo	tentar enviar email o	como se fosse eu.
	Não permitir que sejam salvos conter vírus.	nem abertos anexos	que possam
Fazer D	lownload de Imagens		
	Bloquear imagens e outros co	nteúdos externos em	emails em HTML.
Email se	eguro		
0.	Identificações digitais (também chi	amadas de	Informações
7	certricados) são documentos espe sua identidade em transações elet	rônicas	
_	Para assinar mensagens digitalmer	te ou receber	I <u>D</u> s digitais
	mensagens criptografadas, você p identidade diotal.	recisa de uma	Qbter ID digital
Cript	tografar conteúdo e anexos de toda	s as mensagens d <u>e</u> s	aida
🖌 Agsi	nar digitalmente todas as mensager	s de saída	
			Avançado
		OK Cano	elar Aplicar

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

🕒 Mensag	em Ass	inada						
Arquivo	Editar	Exibir	Inserir	Formatar	Eerramentas	Mensagem	Ajuda	- 🥂
Enviar		Recortar		Copiar	Colar	Lesfazer	Selecionar	»
Para:	Suporte	Pronova						(2)
Assunto:	Mensag	em Assina	10 🗸	n j	I § A.	Ξ Ξ €	:∉ ≞ :	E 11
Esta é ur armazena	na men ado em	um ePa	que sei ss	á assinada	com um cer	tificado digit	al	<
								Y

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

I) 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

🖂 Mensager	m Assinada					
<u>Arquivo</u>	ditar E <u>x</u> ibir	<u>F</u> erramentas	<u>M</u> ensagem	Aj <u>u</u> da		2
Sev Responder	Responde	9 Encaminhar	Imprimir	X Excluir	Anterior	»
De: Data: Para: Assunto: Segurança:	Mauricio Plata terça-feira, 1 Suporte Pron Mensagem As Digitalmente a	a de março de 20 ova sinada assinado e verifi	05 20:11 cado			(Ձ)
Esta é uma armazenad	Segurança: Digitalmente assinado e verificado Esta é uma mensagem que será assinada com um certificado digital armazenado em um ePass					

13. Integrando o ProToken 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 ProToken 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 ProToken será apresentado
- j) Clique no botão "OK" da janela "Gerenciador de dispositivos de segurança"

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

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

- 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"
- f) Antes de concluir, recomendamos que você habilite a opção "Assinar mensagens digitalmente (por padrão)"
- g) Ainda na janela "Configurar contas", clique no botão "Certificados" da área "Gerenciamento"
- h) 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"
- i) Localize o certificado da sua Autoridade Certificadora e clique no botão "Abrir"
- j) Na janela "Efetuando o donwload do certificado" habilite as finalidades e clique no botão "OK"
- k) De volta a janela "Gerenciador de certificados", clique no botão "OK" para continuar
- I) Para concluir clique no botão "OK" da janela "Configurar contas"

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

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

Para que seja possível a troca de e-mails criptografados, 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..."

eral Detalhes Segu	rança	
Assinatura digital ——		
Assinado digitalmente por:	mauricio@pronova.com.br	<u></u>
Conteúdo não alterado	D:	Sim
Assinatura confiável:		Sim
Solicitada confirmação	o de retorno de segurança:	Não
Revogação de identifi	cação digital verificada:	Não
Status da revogação:	Você desativou a verificação de revogação.	< >
Rótulo de segurança:		~
Criptografia		~
Conteúdo e anexos cr	iptografados:	Não
Criptografado(s) com:		N/C
Exibir certificados	Mais informações	

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

Exibir certificados	? 🔀
Assinatura	
Clique em 'Certificado de autenticação' para exibir o certificado usado para assinar essa mensagem.	Certificado de autenticação
Criptografia	
A mensagem não foi criptografada.	Certificado de criptografia
Preferências do remetente	
Algoritmo de criptografia recomendado:	3DES
Clique em 'Certificado do remetente' para exibir o certificado recomendado para criptografar mensagens para o remetente.	Certificado do remetente
Clique em 'Adicionar ao Catálogo de endereços' para salvar as preferências de criptografia no 'Catálogo de endereços'.	Adicionar ao Catálogo de end
	OK Cancelar

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

Outlook	Express
i	A identificação digital do remetente foi adicionada a todos os contatos do 'Catálogo de endereços' que correspondiam a seu endereço de email ou foi criado um novo contato.
	СК

16. 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"

Arquivo	Editar	Exibir	Inserir	Formatar	Ferramentas	Mensagem	Ajuda	
		V		E-h	Verificar ort	ografia		F7
Enviar		Recortar	¢	9 Iopiar	Solicitar con Verificar nor Selecionar c	firmação de le mes lestinatários	eitura	Ctrl+K
Cc:	-				Catálogo de	endereços	8	Ctrl+Shift+B
ssunto:					Criptografa	ť		
Arial		~	10 🗸	∏≣, IN	 Assinar digit Solicitar con 	talmente firmação de se	egurança	
					The second se			

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"

- davo	<u>E</u> ditar	E <u>x</u> ibir	Inserir	Formatar	Eerramentas	Mensagem	Aj <u>u</u> da
Enviar		Recortar	(Copiar	Colar	Desfazer	Selecionar
Para: Mauricio Girão Plata							
Cc:	[
unto:	Mensag	gem Assina	da e Crip	otografada		_	
		11.000	Contract Inc.	72 84	T E A	1 400 200 200	
		1.56	10 V	E PI	1 2 12	1 ST 17 HE	
al		×	10 ~	_ <u>1</u> -, N	1 5 17	3= 1= 1F	
al sta é un erá cript estinatái	na mer ografac rio.	nsagem (da, pois j	que ser á existe	á assinada e a relação	com um cer de confiança	tificado digit a entre o ren	al e que também natente e o
al sta é un erá cript estinatái	na mer ografac rio.	nsagem (da, pois j	que ser á existe	á assinada e a relação	сот um cer de confiança	tificado digit a entre o ren	al e que também natente e o

 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. Digite-o no campo "PIN do Usuário" e depois clique no botão "Login"

Verificação do PIN do Usuário					
Olá Ag	Olá PROTOKEN! Agora é necessário verificar o seu PIN.				
PIN do Usuário: ******					
		<u>L</u> ogin	Cancelar		

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.

🛆 Mensager	n Assinada e	e Criptografa	ada				
<u>Arquivo</u>	ditar E <u>x</u> ibir	<u>F</u> erramentas	<u>M</u> ensagem	Aj <u>u</u> da			
Sev Responder	Responde	S Encaminhar	Imprimir	X Excluir	Anterior	Avançar X	
De: Data: Para: Assunto: Segurança	De: Mauricio Plata Data: terça-feira, 1 de março de 2005 20:17 Para: Mauricio Girão Plata Assunto: Mensagem Assinada e Criptografada Segurança: Digitalmente assinado e verificado; Criptografado						
Esta é uma será criptog destinatário	a mensagem grafada, pois).	que será ass já existe a re	sinada com u elação de co	ım certificad nfiança entre	o digital e que e o remetente	e também e o	

 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 3DES

Conteúdo e anexos criptografados:		Sim
Criptografado(s) com:	3DES	
Evibir certificados	Mais informações	

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"

Geral	Ler	Confirmações	Envio Redaçã	ăo Assinaturas
Verifi	car ortografia	Segurança	Conexão	Manutenção
Proteç	ão contra vírus Selecione a :	zona de segurança do	o Internet Explorer a s	er usada:
~	Zona	de sites restritos (mai	s segura)	
	Avisar qu	ando outro aplicativo	tentar enviar email co	ono se fosse eu.
	✓ Não perm conter v í	itir que sejam salvos r us.	nem abertos anexos o	que possam
Fazer [Download de Im	agens imagens e outros con	teúdos externos em e	enails em HTML.
Email s	eguro Identificações certificados) s	digitais (também cha ão documentos espec	madas de ciais que provam	Informações
-	Para assinar m	e em transações elem rensagens digitalment	e ou receber	I <u>D</u> s digitais
	mensagens cr identidade dio	iptografadas, você pri ital.	ecisa de uma	Obter ID digital
Crip	otografar conteú	do e anexos de todas	as mensagens d <u>e</u> sa	aída
Ass Ass	sinar digitalmente	e todas as mensagens	de saída	<u>A</u> vançado

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

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

a) Abra uma mensagem que tenha uma identificação digital anexada

Arquivo Editar	Exibir Inserir Format	tar Ferra <u>m</u> entas	Ações Aj	<u>u</u> da			
Ø ₽ <u>R</u> esponder	Responder a todos	Section Encaminhar	<i>a</i> 🗗	BX	• •	🔹 • 🌋	2
O Você respond	leu em 2/3/2005 11:33. C	Clique aqui para loc	alizar toda:	s as mens	agens rel	acionadas.	
De: Maurici Para: Suport Cc: Assunto: Mensa	o Plata [mauricio@pronov e Pronova nem Assinada	va.com.br]	Env	viada em:	ter 1/3/2	005 20:12	
Assunto, Mensu	geni Assinada						
Segurança: Ass	inada						8
Segurança: Ass Esta é uma r um ePass	inada nensagem que será a	assinada com u	ım certific	ado <mark>d</mark> igi	tal arma	azenado e	R em

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

🖂 Mensagem A	ssinada - Mensagen	n (HTML)					
<u>Arquivo</u> <u>E</u> ditar	E <u>x</u> ibir <u>I</u> nserir <u>F</u> ormata	r Ferramentas	Ações Aj	<u>u</u> da			
<u>Ø</u> ₽ <u>R</u> esponder	Responder a <u>t</u> odos	S Encamin <u>h</u> ar	6 Pa	$\mathbb{B} \times$	* • * •	Å	2.
O Você responder	u em 2/3/2005 11:33. Cli	que aqui para loc	alizar todas	as mensa	gens relacionad	das.	
De: Maurico	F Propriedades	[1	Env	iada em: t	er 1/3/2005 20	:12	
Para: Suporte	P Adicionar a 'Contato)s'					
Cc:	Pesquisar contato						
Assunto: Mensage	Recortar						_
Segurança: Assin	a Copiar						8
	Colar						~
Esta é uma me	Limpar	a com u	a com um certificado digital armazenado em				
um ePass	Selecionar tudo						
							×

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"

Contat	to d	luplicado detectado
G	O pa	nome ou endereço de correio eletrônico deste contato já existe nesta ista: Contatos
	Vo	ocê gostaria de:
	C	Adicionar este como <u>n</u> ovo contato assim mesmo
	0	Atualizar novas informações deste contato para o já existente:
		Plata, Mauricio Girão Mauricio Plata
		Obs.: Uma cópia de backup do contato existente será inserida em pasta 'Itens excluídos'.
		Abrir <u>contato existente</u> OK Cancelar

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"

	Nome	Residência	Comercial	Pessoal
Outras		NetMeeting	Identificaçã	ies digitais
Adicione	, remova e exib	a identificações digitais	para o contato.	
"				
ecione um ender	eço de email:			
auricio@pronova	.com.br		•	
entificações digit	ais associadas ac	o endereço de email sel	lecionado:	
/ mauricio@pr	ronova.com.br	(Padrão)		Propriedades
				Remover
			_	
			2	ennir como pad
				Importar
			_	Importar

18. 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".

19. 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"

Opções de mensagem	? 🔀
Configurações de mensagem Segurança Prioridade: Normal ✓ Sensibilidade: Normal ✓	igem sendo enviada
Opções de entrega	Selecionar nomes
Salvar mensagem e <u>n</u> viada em: Itens enviados	Proc <u>u</u> rar
□ Não entregar antes de:	
Expirar dep <u>o</u> is de:	
Enviar mensagem usando: mauricio@pronova.com.br 💌	
Opções de controle	
🖉 🔲 Solicitar confi <u>r</u> mação de leitura para esta mensagem	
Contatos	
Categorias	
	Fechar

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".

20. Como assinar um documento do Microsoft Word 2003 usando um certificado digital ICP-Brasil armazenado no ProToken?

- a) Verifique se o seu ProToken está conectado em uma porta USB e usando o Gerenciador de Certificados certifique-se de que nele existe um certificado digital
- b) Execute o Microsoft Word 2003 e abra o arquivo que você deseja assinar com o seu certificado digital;
- c) Uma vez que o documento que será assinado estiver carregado, clique em "Ferramentas" da barra de menu e depois em "Opções..."
- d) Na janela "Opções", clique na aba "Segurança" e em seguida no botão "
- e) Uma janela chamada "Assinatura digital" será exibida, clique no botão "Adicionar" desta janela;

ŀ	ssinatura digital		×				
	Assinaturas						
	A assinatura digital gerada pelo Office não deverá constituir uma assinatura de vinculação legal. Para obter mais informações, leia sobre assinaturas digitais na 'Ajuda'.						
	Os seguintes usuários	assinaram digitalmente este o	documento:				
	Signatário	Identificação digital emit	Data				
	•		•				
	🗹 Anexar certificado	s às assin atures a dicionadas i	recentemente				
	Exibir certificado	<u>A</u> dicionar	<u>R</u> emover				
	Aj <u>u</u> da						
		ОК	Cancelar				

 f) Na janela "Selecionar certificado", selecione o certificado que está armazenado no seu ePass2000 e clique no botão "OK" para continuar;

S	elecionar certificado			<u>? ×</u>			
Selecione o certificado que deseja usar.							
	Emitido para	Emitido por	Data de validade				
	PRONOVA	PRONOVA	01/01/2012				
	PRONOVA CONSUL	Autoridade Certificado	23/07/2009				
	8949017200002703	8949017200002703301	09/03/2025				
	•						
	[OK Cancelar	Exibir certifica	do			

g) Uma janela de diálogo será exibida, nela digite o PIN do seu ePass2000 e clique no botão "Login" para continuar

Verificação do PIN do Usuário 🔀						
Olá PRONOVA! Agora é necessário verificar o seu PIN.						
PIN do Usuário: *********						
Login Cancelar						

h) Se o PIN informado estiver correto, você irá voltar para a janela "Assinatura digital"; do contrário você receberá uma mensagem informando que o PIN informado não está correto. Ao retornar para a janela "Assinatura digital" você poderá observar que o certificado utilizado será exibido conforme a imagem abaixo. Para continuar clique no botão "OK" desta janela e também no botão "OK" da janela "Opções"

Assinatura digital	×						
Assinaturas							
A assinatura digital gerada pelo Office não deverá constituir uma assinatura de vinculação legal. Para obter mais informações, leia sobre assinaturas digitais na 'Ajuda'.							
Os seguintes usuários assinaram digitalmente este documento:							
Signatário Identificação digital emit Data							
PRONOVA CO Autoridade Certificador 05/09/2006							
 ✓ ✓ Anexar certificados às assinaturas adicionadas recentemente 							
Exibir certificado Adicionar Remover							
Ajuda							
OK Cancelar							

i) De volta a tela de edição do Microsoft Word 2003, observe que um novo ícone será inserido na barra de status, conforme ilustramos na imagem abaixo:

27 - 1 - 28 - 1 - 25		٩	_				_
≡ ਯ 🗉 🗇 邱 🖣							
🕴 Desenhar 👻 🔓 🛛 Auto	oFormas 🔹 🔨 🔌		4 3	🚨 🖂 🛛 🖄 🕶 🚄	<u>- A</u> - =	≣ ≩ ∎	
Pág 3 Seção 1	3/3 Em	n 24,3 cm Lin	16 Col	1 GRA ALT	EST SE Por	rtuguês (🛛 📴	K 🔒

Nota: qualquer modificação que foi feita e que for salva o Microsoft Word 2003 informará que todas as assinaturas digitais serão removidas. Para continuar clique no botão "Sim" e depois repita o procedimento de assinatura digital do arquivo.

Microsoft Office Word						
1	Salvar removerá todas as assinaturas digitais do documento. Deseja continuar?					
	<u>Sim</u> <u>N</u> ão					

21. Removendo o software do ProToken

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

22. O Gerenciador Web PKI do ProToken

Se você deseja disponibilizar para seus usuários uma versão HTML do Gerenciador PKI, utilize o modelo disponibilizado no CD-ROM que acompanha o equipamento. Você poderá usar este modelo para usar em sua Intranet e permitir que seus usuários possam realizar algumas tarefas de gerenciamento do dispositivo sem usar a versão padrão do Gerenciador PKI que é instalada pelo runtime do ProToken.

23. Instalando o Token USB ProToken no Sistema Operacional Linux

Localize no CD-ROM que acompanha o equipamento um diretório chamado Linux, dentro deste identifique a distribuição que você utiliza e faça, então, uso do pacote EnterSafe lá disponibilizado. Fique atento para as mensagens de erro que indicarão quais são os prérequisitos necessários para proceder a instalação do software do ProToken, bem como a sua posterior utilização.

Caso o CD-ROM não possua o pacote para a sua distribuição Linux, entre em contato com a Pronova Soluções Inteligentes e solicite já um pacote de instalação, todavia necessitamos das seguintes informações para o desenvolvimento:

Fabricante	Versão	Versão do	Versão do	Já foi	Onde obteve o	Possui arquivo
Linux	Linux	Kernel	Gcc	atualizado?	Kernel?	Config anexado
Redhat	FC5	kernel-2.6.15- 1.2054_FC5	4.1.0 20060304	Νᾶο	A partir de um repositório do fabricante (RedHat)	Sim. No diretório /boot vmlinuz-2.6.15- 1.2054_FC5

As informações em vermelho são um exemplo

24. Ferramentas de Teste

Caso você deseje fazer testes de geração do par de chaves RSA com 1024bits ou 2048bits, utilize as ferramentas disponibilizadas no CD-ROM de instalação do ProToken. No CD-ROM, existe um diretório chamado "Ferramentas de Teste" que oferece duas ferramentas a saber: PKCSDemo.exe e EnumObj.exe. As instruções sobre como utilizar estas ferramentas, estão descritas no arquivo PDF "Suplemento" que está no mesmo diretório destas aplicações.

25. 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 inicializar o ProToken, <u>é necessário informar o atual PUK</u> no campo *Por favor, informe o PUK* da janela "Inicializar Token".

Nota: se você não possui o PUK do seu dispositivo, entre em contato com o Administrador de Sistemas da sua empresa. Lembramos que existe um número prédeterminado de tentativas de acerto do PUK. Se estas forem excedidas o seu dispositivo será bloqueado e todo o conteúdo do dispositivo ficará indisponível e para poder voltar a utilizar o dispositivo será necessário reinicializar o mesmo, todavia, esta ação irá apagar todas as informações que estão armazenadas no chip criptográfico do ProToken.

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

R: Verifique os valores digitados nos campos "Informe PIN" e "Confirme 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.

d) Ao conectar o meu dispositivo na porta USB, ele não é reconhecido. O que pode estar errado?

R: Certamente o software do ProToken não está instalado, execute o arquivo ProToken_runtime.exe que está na raiz do CD-ROM e siga as instruções do instalador. Maiores detalhes poderão ser encontrados no Tópico 4 "Instalando o software do ProToken".

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

e) O ProToken suporta mecanismo de desafio resposta (challenge response)?

R: Sim, o ProToken suporta mecanismo de desafio resposta. Através de uma chave 3DES pré-definida (chave compartilhada) que é armazenada no servidor (host) e no ProToken, podemos fazer a verificação da identidade de um usuário. Quando realizamos a verificação da identidade do usuário através de uma rede, a máquina do cliente (com o ProToken conectado) envia para o servidor uma requisição; o servidor (host) gera um número aleatório, o qual é devolvido ao cliente, ou seja, o desafio.

Assim que a máquina do cliente recebe este número aleatório, ele é enviado para o ProToken através da porta USB do computador. Ao receber este valor o ProToken irá realizar a codificação deste número aleatório usando o algoritmo 3DES mais a chave compartilhada. O resultado desta operação matemática será devolvida para o computador do cliente.

Este resultado será enviado para o servidor que fará a verificação desta resposta. A
verificação no servidor é feita da mesma forma que no ProToken, ou seja, ele irá codificar o número aleatório com o algoritmo 3DES mais a chave compartilhada. O resultado desta operação será comparado com o que foi enviado pelo computador do cliente. Se os valores forem idênticos, podemos garantir que temos um usuário válido o qual terá seu acesso garantido. Do contrário, o acesso será negado.

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?

VPN-1 SecureClient	
⚠	Token Login: Failed to retrieve KeyHolder.
	ОК

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

R: Certamente o software do ProToken não está instalado, execute o arquivo PortugueseBR_Runtime.exe que está na raiz do CD-ROM e siga as instruções do instalador. Maiores detalhes poderão ser encontrados no Tópico 4 "Instalando o software do ProToken".

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

h) Travei o PUK do meu ProToken, perdi o meu dispositivo?

R: Não, você não perdeu o seu dispositivo. Todavia, para reativar o acesso ao seu ProToken, será necessário reinicializar o seu equipamento para as condições originais de fábrica. Em outras palavras, ao usar a ferramenta ng_init.exe que está no diretório "InitTool", todas as informações que estiverem armazenadas no seu ProToken serão apagadas. Maiores instruções sobre a utilização desta ferramenta poderão ser encontradas no documento ePassNG_Init.pdf que está no mesmo diretório desta ferramenta.

i) Posso instalar mais de um certificado no meu ProToken?

R: Sim, você poderá instalar mais de um certificado no seu ProToken, mas tenha em mente que existe uma limitação que é a quantidade de memória do seu dispositivo. 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 ProToken não pode ser exportada, recomendamos que não sejam armazenados no mesmo ProToken, 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 ProToken.

j) O ProToken pode ser utilizado em outros sistemas operacionais?

R: Sim, o ProToken poderá ser utilizado também no sistema operacional Linux. O software necessário para instalar o ProToken neste sistema operacional poderá ser encontrado no diretório Linux do CD-ROM de instalação .

k) Instalei o software do ProToken no Windows XP, conectei o na porta USB e ele não é reconhecido pelo Monitor de Certificados. O que pode estar errado?

R: Devido ao fato do Windows XP ter um driver do ProToken antigo, ao conectar o ProToken no seu computador, o Windows XP instala o driver antigo ao invés de instalar o driver atual que é instalado pelo runtime. Para resolver este problema, consulte o BT070216.PDF que está no CD-ROM de instalação do ProToken.

26. 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.

27. Contatos:

Pronova Soluções Inteligentes (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 do middleware e alguns Componentes Eletrônicos)

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 <u>www.FTsafe.com</u>

Oberthur Card Systems (Fabricante do Chip Criptográfico)

Endereço	4250 Pleasant Valley Road - Chantilly, VA 20151-1221 USA
Telefone	+1 (703) 263-0100
Fax	+1 (703) 263-0100
Site	www.oberthur.com