

Benefícios**Compacto e Conveniente**

Embora o iKey 2032 seja do tamanho de um pendrive, ele oferece grandes recursos de segurança

Fácil de transportar

devido ao seu tamanho pequeno e estrutura resistente, possibilita que os usuários sempre tenham suas identificações digitais exclusivas à mão

Conectividade USB**Fácil de Implantar**

O iKey 2032 oferece a segurança de um smart card sem a necessidade de uma leitora de smart card. Ele apresenta uma porta USB 1.1/2.0 interna para conexão fácil a praticamente qualquer computador, com indicador luminoso de estado do dispositivo

Para aprimorar os aplicativos de segurança, não é necessário implantar e manter leitoras de smart card de custo elevado ou dispositivos biométricos especiais: o iKey oferece a segurança do smart card sem dores de cabeça

Processamento de Criptografia On-board

Ao contrário de outros sistemas de autenticação de smart card ou baseados em tokens, o iKey 2032 oferece criação de chaves e processamento de criptografia on-board para garantir que as funções e chaves criptografadas estejam sempre protegidas

Certificação Microsoft WHQL (Windows Hardware Quality Labs) para Windows 2000 e XP

Proteção para a chave privada

- Não permite que a chave privada, se gerada no dispositivo, seja exportada, condicionando as transações que utilizam a chave privada a ocorrer dentro deste;
- As rotinas de criptografia manipulam as chaves privadas em memória do tipo non-swappable;
- Sobrescreve com valores fixos imediatamente após o término das funções que utilizaram estas chaves;
- Roda em kernel mode, como parte do núcleo do sistema operacional, no anel 0, também chamado de "supervisor mode"

Gráficos personalizados da marca disponíveis

iKey 2032

Dispositivo USB pessoal de autenticação e criptografia



O iKey 2032 é um dispositivo compacto de autenticação de dois fatores que fornece segurança do cliente para aplicativos de autenticação na rede, criptografia de emails e assinatura digital.

Token definitivo para autenticação

O iKey 2032 da SafeNet é um dispositivo USB de autenticação para certificação digital, que gera e armazena até 10 chaves privadas, incluindo a cadeia de certificados. Extensão da tecnologia de smart card, o iKey 2032 pode ser conectado a qualquer porta USB e fornece autenticação forte (dois fatores) de usuários sem a necessidade de leitoras de cartão. O iKey 2032 foi projetado para ser compatível com uma grande variedade de aplicativos para desktop e sistemas portáteis. Devido ao seu baixo custo, design compacto e interface USB padrão, é mais fácil de implantar e gerenciar do que os smart cards. Seu hardware tem certificação FIPS nível 2 e seus recursos incorporados de criação e armazenamento de chaves criptográficas, assinatura digital e robustez física fornecem segurança inigualável a qualquer software cliente.

Senhas fracas são eliminadas com a autenticação forte

O iKey 2032 fornece autenticação de dois fatores para aplicativos em que a segurança seja um fator crítico. Ao contrário da autenticação de senhas tradicional, que utiliza senhas fracas, que podem ser facilmente descobertas, o iKey 2032, para concluir o processo de autenticação, requer o token físico (o próprio iKey com a chave privada exclusiva do usuário) e o PIN do usuário.

Compatível com milhares de aplicativos de segurança

A SafeNet vem trabalhando com desenvolvedores de segurança para garantir que o iKey ofereça suporte a uma grande variedade de soluções. Hoje, pode-se usar o iKey em aplicações de logon, logon com smart card, single sign-on, autenticação em VPNs, criptografia de emails, assinaturas digitais, acesso a arquivos criptografados, e em muitos aplicativos de certificação dos principais fornecedores no Brasil, como Certisign, Serasa, Serpro, Microsoft, Computer Associates, VeriSign e outros. Inteiramente compatível com a ICP Brasil, o iKey 2032 também opera com PKCS#11 e MS Crypto API para integração com aplicativos mais personalizados.

Mais segurança, com a certificação FIPS 140-1 L2

O iKey 2032 está validado pelo padrão FIPS 140-1, nível 2 com a finalidade de oferecer proteção superior aos aplicativos que requerem alto nível de segurança física, lógica e funcional.



Utilizado por vários aplicativos de segurança no mundo inteiro

O iKey 2032 foi integrado com vários aplicativos, inclusive no logon com smart card e single sign-on, autenticação em VPNs, criptografia de e-mails, assinaturas digitais e em muitos aplicativos para certificação digital dos principais fornecedores, como Certisign, Serasa, Serpro, Microsoft, Computer Associates, VeriSign e outros. O iKey 2032 é compatível com o PKCS#11 e a Microsoft CryptoAPI para uma melhor integração com aplicativos personalizados.

Software de gerenciamento em português brasileiro

Interface gráfica permite exportação de certificados armazenados no dispositivo; importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo de acordo com a RFC 2315; importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; visualização de certificados armazenados no dispositivo; apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; reutilização de dispositivos bloqueados através de apagamento total dos dados armazenados e geração de nova senha de acesso.

Com mais de 5.000 clientes em todo o mundo, a SafeNet está presente em 100 países, com escritórios próprios e canais de distribuição. Alguns de seus principais clientes são: Serpro, Banco Itaú, Caixa Econômica Federal, Certisign, Serasa, Imprensa Oficial do Estado de São Paulo, Bradesco, Microsoft, Bank of America, Citibank, Cisco Systems, Departamento de Defesa dos EUA, Deutsche Bank, Banco Ibi, Samsung, Texas Instruments, Receita Federal Americana, VIVO, Telefonica, Brasil Telecom, Embratel.

<http://br.safenet-inc.com>



SafeNet Brasil

Alameda Tocantins, 280
06455-020 - Barueri - São Paulo
TEL FAX: +55(11)4208-7700
<http://br.safenet-inc.com>

SafeNet Brasil© - Todos os direitos reservados. As informações constantes neste folheto podem ser alteradas sem aviso prévio. A SafeNet não assume responsabilidade por quaisquer erros que eventualmente possam ser identificados neste folheto.

Compacto e conveniente

Embora o iKey 2032 seja do tamanho de um pendrive, ele oferece grandes recursos de segurança. Fácil de transportar, devido ao seu tamanho pequeno e estrutura resistente, possibilita que os usuários sempre tenham suas identidades digitais exclusivas à mão.

Máxima Segurança

- Uso das chaves privadas só após autenticação da identidade do titular do dispositivo;
- Mecanismo de autenticação tipo challenge-response;
- Força a troca da senha padrão no primeiro acesso;
- Utilização do dispositivo é bloqueada após 5 tentativas de autenticação com códigos inválidos;
- Titular do dispositivo é avisado a cada vez que uma função que utilize sua chave privada é ativada, e deve se autenticar para liberar a utilização pretendida;



Especificações Técnicas

Integração de certificados armazenados no dispositivo com ambiente Windows 98/SE, ME, 2000, 2003 e XP e Linux com Kernel 2.4 ou superior

APIs de Criptografia

- PKCS#11 v 2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC

Validação de Hardware de Criptografia

- Certificado no padrão FIPS 140-1 nível 2 - certificado nº 161

Funções de Criptografia

- Criação assimétrica de pares de chaves (RSA)
- Criação simétrica de chaves (DES, 3DES (k1,k2,k3), RC2, AES)
- Armazenamento e gerenciamento de chaves protegidos por hardware
- Assinatura digital incorporada
- Desempenho da Criptografia
- Operações de chaves RSA de 1024 e 2048 bits
- Criação de chaves: menos de 90 segundos com verificação da chave
- Assinatura digital: menos de 1 segundo

Algoritmos de Criptografia

Criptografia Assimétrica de Chaves

- RSA de 1024 bits, RSA de 2048 bits
- #### Algoritmos Simétricos de Chaves
- DES, 3DES (k1,k2,k3), RC2, AES
- #### Assinatura Digital
- RSA de 1024 bits, RSA de 2048 bits
- #### Algoritmos de Hash
- SHA-1, MD5

Middleware para Windows e Linux

Integração dos certificados armazenados no dispositivo com o NSS (Network Security Services), do ambiente Linux kernel 2.4 e versões superiores estáveis

Suporte a algoritmos adicionais disponível

Características Físicas Hardware

- Processador de 8 bits
- Memória de 32 K

Conectividade

- Compatível com USB 1.1/2.0
- Transferência de 1,5 Mbits por segundo

Dimensões

- 15,875 mm x 57,15 mm x 7,9375 mm

Normas Reguladoras

- FCC Parte 15 - classe B CE
- Compatível com RFC 2459
- Compatível com padrão ITU X.509
- Compatível com padrão ISO 7816-3/4

