

Hardware de Segurança - Net D-Fence

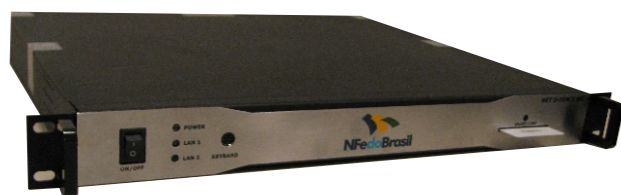
O Net D-Fence é um *appliance* HSM (Hardware Security Module) do tipo *network attached*, ou seja, seus serviços são oferecidos via rede. Sua função principal é ser um repositório seguro para chaves criptográficas. Além disso, é também um provedor de serviços criptográficos, como assinatura digital, geração de chaves e autenticação, entre outras funcionalidades.

Aplicações que necessitam de criptografia normalmente demandam maior processamento, o qual poderia ser usado para a atividade-fim do negócio. Uma grande preocupação dos gestores é o armazenamento das chaves de criptografia, pois uma vez na posse destas chaves toda a informação confidencial que elas protegem pode ser exposta. Nos sistemas baseados em chave pública, muitas vezes o problema não é apenas a confidencialidade, mas a posse, integridade e a autoria das informações. Com a regulamentação da ICP-Brasil (Infra-estrutura de Chaves Públicas Brasileira), documentos assinados digitalmente têm valor legal e não admitem o repúdio por parte do emitente.

O Net D-Fence é um *appliance* desenhado desde o início para oferecer proteção no armazenamento de chaves de acordo com padrões internacionais. É aderente aos padrões de mercado, para garantir interoperabilidade e facilidade de integração. Possui uma arquitetura modular, permitindo ao cliente adquirir apenas os módulos (internos ao Net D-Fence) que serão necessários na sua solução.

O HSM é oferecido em dois modelos com gabinete rack-mount:

1. Net D-Fence NG;
2. Net D-Fence XP.



Hardware de Segurança - Net D-Fence

A NFe do Brasil acompanha atentamente a definição e evolução das várias iniciativas governamentais nas quais há necessidade de criptografia, desta forma oferece um produto adequado as necessidades dos clientes que precisam aderir a estas iniciativas. Entre elas podemos citar o Sistema de Pagamentos Brasileiro e o Projeto Nota Fiscal Eletrônica que utilizam o HSM para guarda segura do certificado digital.

Aplicações em praticamente qualquer sistema operacional podem se beneficiar dos serviços de criptografia do HSM, fazendo do Net D-Fence uma solução única e consistente para cenários multiplataforma.

O mecanismo de balanceamento de carga, transparente para a aplicação, traz confiabilidade e disponibilidade à solução.

A escalabilidade praticamente linear do Net D-Fence permite que novas unidades do HSM possam ser incorporadas à solução conforme a demanda e sem nenhum impacto na aplicação.

Solução premiada

O HSM da NFe do Brasil Net D-Fence recebeu o Prêmio de Melhor Solução e Produtos para Gerenciamento de Risco e Segurança da Informação, o SECAWARD 2006, na categoria Melhor Tecnologia Nacional, durante a Security Week 2006, realizada em São Paulo.

Ainda naquele ano a Souza Cruz e a Ultragaz receberam dois prêmios de inovação oferecidos pela B2B Magazine por utilizarem o HSM Net D-Fence na implantação do projeto NF-e.

Em 2007, o prêmio veio em função da solução de Criptografia em Banco de Dados desenvolvida para a Liberty Seguros. O prêmio foi oferecido pela Revista Executivos Financeiros.

Características Técnicas Net D-Fence XP e NG

NG	XP
Algoritmos	
RSA (até 1024 bits) ECDSA (160, 192, 256, 384 e 521 bits) DES 3DES (128 e 192 bits) MD5 (128 bits) SHA1 (160 bits) SHA2 (256,384 e 512 bits)	RSA (512, 1024, 2048 e 4096 bits) ECDSA (160, 192, 256, 384 e 521 bits) DES 3DES (128 e 192 bits) AES (128, 196 e 256 bits) MD5 (128 bits) SHA1 (160 bits) SHA2 (256,384 e 512 bits)
Application Programming Interface - APIs	
MS Crypto API API Nativa (criptografia e gerência) API Nativa Assinatura XML padrão W3C 1, 5	MS Crypto API API Nativa (criptografia e gerência) API Nativa Assinatura XML padrão W3C 1, 5
Sistemas Operacionais Suportados	
MS Windows Linux Sun Solaris Outras (sob consulta)	MS Windows Linux Sun Solaris Outras (sob consulta)
Conectividade	
Serial RS-232 DB9 Ethernet 10/100 RJ-45 x3	Serial RS-232 DB9 Ethernet 10/100 RJ-45 x3 Ethernet 10/100 RJ-45 x1
Armazenamento de Objetos	
Proteção por chave master (SVMK) em Smart Card Separação de domínios por usuários Diferentes níveis de privilégios Backup criptografado	Proteção por chave master (SVMK) em Smart Card Separação de domínios por usuários Diferentes níveis de privilégios Backup criptografado
Gerência	
Console Local (porta serial) Console remoto (rede)	Console Local (porta serial) Console remoto (rede)
Módulos	
Core Crypto Engine State Manager XML DSing Engine PDF417 Engine Code128 Engine	Core Crypto Engine State Manager XML DSing Engine PDF417 Engine Code128 Engine PIN Management OTP Manager SPB Engine
Autenticação	
Regular (console remoto/API) Smart Card (console local)	Regular (console remoto/API) Smart Card (console local) TFA - Two Factor Authentication (console remoto/API)
Comunicação HSM - Application Host	
Canal aberto (console remoto/API) Canal criptografado - TLS (console remoto/API) Sessões simultâneas não limitadas	Canal aberto (console remoto/API) Canal criptografado - TLS (console remoto/API) Sessões simultâneas não limitadas
Hash Message Authentication (HMAC) Based Host One Time Password (HOTP) 1	
	Geração de Soft Token HOTP Validação de Soft Token HOTP M-HOTP (applet padrão J2ME) F-HOTP (para tabelas de senhas indexadas)
Auditoria	
Registro persistente de eventos (log) Recuperação de registros	Registro persistente de eventos (log) Recuperação de registros
Código de Barras - padrão TIFF	
Linear 128c Bidimensional PDF417	Linear 128c Bidimensional PDF417
Monitoramento	
Eventos CPU, memória e sessões ativas	Eventos CPU, memória e sessões ativas Temperatura do módulo criptográfico Diagnóstico de bateria, memória e controladora
Desempenho	
80 Assinaturas RSA 1024 bits por segundo 12 Assinaturas XML DSIG RSA 1024 bits por segundo	175 Assinaturas RSA 1024 bits por segundo 23 Assinaturas XML DSIG RSA 1024 bits por segundo



Soluções sob medida para NF-e, SPED e CT-e

Solução HSM

Hardware Security Module - Net D-Fence

