ANEXO I

DESCRIÇÃO DO OBJETO DA LICITAÇÃO/ESPECIFICAÇÕES/CONDIÇÕES

1 Objeto

Aquisição de 93.065 (noventa e três mil e sessenta e cinco)unidades de dispositivo (mídia) USB, do tipo Token, para armazenamento de chaves criptográficas.

2 Especificações Técnicas

Requisitos mínimos para as soluções de armazenamento de chaves privadas e certificados digitais que usam dispositivos do tipo token:

2.1 Aderência a Padrões

a) Seguir, no mínimo, as regras estabelecidas para o nível 1 de segurança do padrão FIPS 140-1 ou 2.

b) Seguir, no mínimo, as regras estabelecidas para o nível 2 de segurança do padrão FIPS 140-1 ou 2, para verificação de violação no hardware (Tamper Evidence).

c) Compatível com certificados digitais gerados pelas autoridades certificadoras ICP-Brasil como AC.

d) Ser homologado pela ICP Brasil.

I – Para a comprovação do item "d", acima, deverá ser apresentado certificado de conformidade com os padrões definidos pela ICP.

2.2 Características do dispositivo

2.2.1 Token USB

a) Possuir numeração única para cada dispositivo.

b) Suportar os algoritmos RSA, MD5, SHA2, DES, 3DES e AES.

c) Deverá gerar chaves RSA de até 2048 bits (padrão ICP Brasil A3 e A4).

d) Deverá suportar a geração On-board de par de chaves RSA.

e) Deverá ser compatível com aplicações PKI.

f) Deverá suportar assinatura digital em Hardware.

g) Deverá suportar a geração de números aleatórios em hardware.

h) Deverá suportar gerenciamento através de PIN e PUK.

i) Seguir o padrão ISO 7816 partes 1, 2, 3, 4 e 8.

j) Atender aos requisitos da seção 4.7.2, do padrão FIPS 140-2, para a geração de chaves criptográficas.

k) As mídias destinadas ao armazenamento de certificados de nível de segurança 3 devem implementar a geração de chaves RSA com até 2048 bits.

2.2.2 Características Físicas

a) Deverá possuir no mínimo Hardware com processador de 8 bits e memória de 32 K.

b) Deverá permitir o armazenamento de no mínimo 5 certificados com chaves RSA de tamanho 2048 bits.
c) Deverá ter conectividade compatível com USB 1.1/2.0.
d) Deverá possuir chassi em plástico rígido e resistente a água.

2.3 Características funcionais

2.3.1 Deverá possuir software gerenciamento com as seguintes características:

a) Exibir detalhes do Token USB
I. Nome do token USB;
II. Tamanho máximo do PIN;
III. Tamanho mínimo do PIN.
b) Alteração do PIN.
c) Renomear o Token USB.
d) Alterar o PUK.
e) Destravar o PIN.
f) Formatar o Token USB*
(*) formatar token, após o usuário informar o PUK, significa o apagamento de todo o conteúdo de sua memória. Após este procedimento, o dispositivo volta a ter os mesmos parâmetros de inicialização comparativamente a um token novo entregue ao MP
g) Deverá possuir a opção do idioma Português do Brasil.

2.4 Interoperabilidade com Aplicações

2.4.1 A solução deve ser compatível com as camadas de software definidas, para ambiente Microsoft por:

a) Ambientes Windows 98, 98SE, 2000, XP, Vista, Windows 7 e versões superiores.
b) Suporte nativo para arquiteturas 32 bits e 64 bits para Windows Vista, Windows 7 e versões superiores.
c) Possuir biblioteca implementando a CryptoSPI do Microsoft Cryptographic Service Provider assinada pela Microsoft.
d) Possuir biblioteca implementando o padrão PKCS#11.
e) Deve ser compatível com as bibliotecas NSS.
f) As implementações devem seguir os seguintes padrões:
I. Padrão PC/SC versão 1.0.
II. Padrão CSP - Microsoft Cryptographic Service Provider.
III. Padrão PKCS#11 versão 2.20.
IV. Padrão PKCS#15 versão 1.1.

2.4.2 A solução deve ser compatível com as camadas de software definidas para ambiente Linux por:

a) Ambiente Linux kernel 2.4 e Linux kernel 2.6 versões estáveis.
b) Suporte nativo para arquiteturas 32 bits e 64 bits.
c) Possuir biblioteca implementando o padrão PKCS#11.
d) Deve ser compatível com as bibiotecas OpenSSL e NSS.
e) As implementações devem seguir os seguintes padrões:

I. Padrão PC/SC versão 1.0
II. Padrão PKCS#11 versão 2.20.
III. Padrão PKCS#15 versão 1.1.

2.4.3 A solução deve ser compatível com as camadas de software definidas, para ambiente MacOS X por:

a) Ambiente MacOS X 10.5, 10.6 e superiores.

b) Implementar módulo no padrão TokenD para SmartCard Services.

c) As implementações devem seguir os seguintes padrões:

I. Padrão PKCS#11 versão 2.20.
II. Padrão PKCS#15 versão 1.1.

2.5 Deverá possuir, no mínimo, as seguintes certificações:

a) X.509 versão 3.
b) ISO 7816 Compliant.
c) PKCS#11 versão 2.20.
d) Microsoft CryptoAPI (CAPI) 2.0.
e) PC/SC versão 1.0.
f) SSL versão 3.

2.6 Plataformas suportadas (Sistemas Operacionais)

a) Possuir driver disponíveis para o sistema operacional Linux kernel 2.4 e Linux kernel 2.6 versões estáveis.

b) Possuir driver disponíveis para o sistema operacional Microsoft Windows 98, 98SE, 2000, XP, Vista 32 e 64 bits, Windows 7 32 e 64 bits e versões superiores.

c) Possuir driver para o sistema operacional MacOS X versões 10.5, 10.6 e superiores.

2.7 Outras características

2.7.1 Instalação:

a) Em ambiente Microsoft Windows (98, 98SE, 2000, XP, Vista, Windows 7 e superiores):

I. Permitir a instalação – através de execução de serviço com privilégios de LocalSystem – da solução, driver, CSP, biblioteca PKCS#11 e software gerenciador, de forma assistida e desassistida, através de linha de comando e que forneça código de retorno com informações dos resultados das operações.

II. A documentação do produto deve abranger, inclusive, todas as rotinas e ações efetuadas pelo programa instalador, independentemente do sistema operacional.

b) Ambiente Linux:

I. Fornecer todos os pacotes necessários à instalação da solução, em formato binário:

a) Pacote em formato "rpm" para OpenSuse.
b) Pacote em formato "deb" para Ubuntu.
c) Pacote em formato "deb" para Debian.
d) Pacote em formato "rpm" para Fedora.

e) Pacote em formato "tar.gz" para instalação em outras distribuições.

II. Fornecer os fontes necessários à geração dos pacotes, sem ônus adicional pelo suporte:

a) Para os pacotes "deb" prover "tar.gz" com todos os arquivos utilizados pelo comando "dpkg-deb" para geração do pacote.

b) Para os pacotes "rpm" prover pacote “source rpm”.

c) Em todos os casos prover o “tar.gz” para compilação e adequação às necessidades do MP.

d) A empresa deve informar quais versões específicas de cada distribuição foram utilizadas na criação de pacotes.

III. O(s) empacotamento(s) não deve(m) conter outros pacotes/programas open-source que sejam fornecidos pela(s) distribuição(ões) Linux.

IV. As alterações em aplicativos da comunidade de software livre, se forem feitas, deverão ser submetidas e aceitas pelos respectivos autores. Exemplos:

a) Alterações no pacote pcsc-lite devem ser submetidas e aceitas pelo autor: Ludovic Rousseau <rousseau@debian.org> (projeto http://alioth.debian.org/projects/pcsclite/).

b) Alterações nos pacotes opensc/openct, que tratam das leitoras e das bibliotecas de cartões smartcard devem ser submetidas e aceitas pelo projeto www.opensc-project.org/ e/ou www.musclecard.com/ (conforme o caso).

c) Ambiente MacOS:

I. Fornecer todos os pacotes necessários à instalação da solução no formato “pkg”.

II. As alterações em aplicativos da comunidade de software livre, se forem feitas, deverão ser submetidas e aceitas pelos respectivos autores. Exemplos:

a) Alterações no pacote pcsc-lite devem ser submetidas e aceitas pelo autor: Ludovic Rousseau <rousseau@debian.org> (projeto http://alioth.debian.org/projects/pcsclite/).

b) Alterações nos pacotes opensc/openct, que tratam das leitoras e das bibliotecas de cartões smartcard devem ser submetidas e aceitas pelo projeto www.opensc-project.org/ e/ou www.musclecard.com/ (conforme o caso).

2.7.2 Documentação e suporte:

a) Manuais das interfaces de programação (APIs) e bibliotecas de desenvolvimento;

b) Manual de utilização do token USB em português.

c) PIN padrão, formato permitido para construção de PIN.

d) Deve ser fornecida documentação específica para cada plataforma (Mac, Linux e Windows) bem como suporte técnico.
e) Deve ser fornecida correções de segurança e correção de bugs, pelo período mínimo de 3 anos, sem ônus adicional.

2.8 Homologação

2.8.1 A empresa fornecedora da solução deverá disponibilizar todas as informações (manuais), software e dispositivos necessários à homologação do produto pelo MP.

2.8.2 Somente será considerada apta a EMPRESA que atender todos os requisitos desta especificação.

2.9 Mídia de armazenamento de softwares

2.9.1 Os softwares necessários para o funcionamento do dispositivo token em todos os sistemas operacionais requisitados devem ser armazenados no próprio dispositivo, em memória específica para esta finalidade. Os arquivos devem estar em uma estrutura organizada de diretórios, indicando o sistema operacional, versão e agrupados por finalidade (ex. aplicações, arquivos de configuração, bibliotecas, arquivos de manuais, etc).

2.9.2 A empresa fornecedora do dispositivo deve disponibilizar ao MP endereço Internet, no qual os usuários possam fazer download dos softwares necessários, inclusive updates. O sítio de download deverá ser disponibilizado pelo período mínimo de 03 anos.

2.9.3 O MP, ao seu critério, poderá disponibilizar os softwares necessários ao uso do dispositivo token por meio de link para download pelos seus clientes usuários do token, sem custos adicionais de qualquer natureza.

2.10 Na proposta deverá ser informado: marca, modelo, país de procedência do produto, unidade fabril e ano de fabricação.

2.11 Somente será considerada apta a EMPRESA que atender todos os requisitos desta especificação.