ANEXO I AO DECRETO Nº 1.031, DE 29 DE MAIO DE 2015

PREFEITURA MUNICIPAL DE PALMAS **Data: 13/02/2019** **Nº 002**

Secretaria de Transparência e Controle Interno

SETCI
Fls. 03

SOLICITAÇÃO DE COMPRAS DE BENS E SERVIÇOS / TERMO DE REFERÊNCIA – ANEXO I
(art. 14 da Lei nº 8666/93)

1 – Unidade orçamentária demandante.

Secretaria de Transparência e Controle Interno – SETCI, Secretário: **Edmilson Vieira das Virgens**, fone: (63) 2111-2218.

2 – Objeto:

O presente Termo de Referência tem por objeto a contratação de empresa especializada na emissão de Certificado Digital para atender demandas do SETCI

3 – Origens dos Recursos:

Recursos próprios destinados a outras funções

4 – Justificativa Da Aquisição Ou Contratação.

O presente objeto trata da à contratação de empresa especializada na emissão de Certificado Digital para atender demandas do SETCI.

A utilização da certificação digital atualmente é uma ferramenta importante para assegurar a inviolabilidade das transações eletrônicas sobretudo nas instituições governamentais, onde as mesmas, devem garantir que as informações que trafegam pela sua rede são seguras e que as informações armazenadas em seus bancos de dados não serão furtadas nem violadas.

Tal solicitação se faz necessária para transmissão de arquivos e informações necessárias ao Tribunal como o SICAP-AP, SICAP- LO, SICAP CONTÁBIL, CADUN, e órgãos federais fiscalizadores para transmissão e emissão de dados e documentos como: GFIP,RAIS, DCTF, DIRF, e DIF.

E ainda, visto a mudança de presidência, diretores e outros servidores desta secretaria torna-se necessária para a mudança de identificação dos responsáveis (CPF) dos mesmos.

5 – QUANTIFICAÇÃO E ESPECIFICAÇÕES TÉCNICAS

Item	Quant.	Unid.	Especificações	Valor Unitário Estimado	V. Total Estimado
01	02	Srv.	Certificado Digital tipo E-CNPJ A3 – para armazenamento de assinatura digital com validade de 03 (três) anos, tipo token USB.	100,00	200,00
02	06	Srv.	Certificado Digital tipo E-CPF A3 – para armazenamento de assinatura digital com validade de 03 (três) anos, tipo token USB.	100,00	600,00
03	02	Srv.	Certificado Digital tipo E-CNPJ sem mídia para token USB.	300,00	600,00

04	06	Srv.	Certificado Digital tipo E-CPF sem mídia para token USB.	200,00	Fls 04	1.200,00

VALOR TOTAL **2.600,00**

6 – PREVISÃO ORÇAMENTÁRIA E CLASSIFICAÇÃO DA DESPESA:

Funcional Programática – Nome da ação	Natureza da Despesa - Subitem	Fonte	Ficha	Valor
04.122.1175.4501 - Manutenção dos serviços administrativos	33.90.39 - 5700	001000103	20190129	

7 – Valor Total por extenso:

R$ 2.600,00 (dois mil seiscentos reais)

8 – Prazo Para a Entrega / Execução:

O contrato terá vigência pelo período de 12 (doze) meses podendo ser prorrogado nas hipóteses do artigo 57, da Lei Federal nº 8.666/93;
O prazo de entrega será de imediato, logo após a solicitação, requisição expedida pela Diretoria de Finanças, conforme a necessidade do Instituto.

9 – Local De Entrega / Realização / Instalação: A entrega do token será na sede da **Secretaria de Transparência e Controle Interno** localizado no endereço 502 Sul, Av. NS-02, Conj. 1, Ed. Buriti – 3º Piso - CEP: 77.021-658

A emissão do certificado, a geração de senha e a biometria será realizada na sede da certificadora em até 12 horas após a solicitação do token.

10 – Condições Gerais:

10.1 – Emissão de certificado de assinatura digital

10.1.1 Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP Brasil.

10.1.2Nível: A3.

10.1.3 Validade: 3 (três) anos, contados a partir da data do aceite definitivo do certificado.

10.2 – Dispositivo do tipo *token* de armazenamento de certificado digital

10.2.1 Totalmente compatível com as especificações do certificado digital constante do Item 10.1.

10.2.2 Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior.

10.2.3 Permitir conexão direta na porta USB, sem necessidade de interface intermediária para leitura.

10.2.4 Ser aderente às normas do Comitê Gestor da ICP-Brasil.

10.2.5 Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

10.2.6 Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.

10.2.7 Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas.

10.2.8 Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3).

10.2.9 Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas.

10.2.10 Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.

10.2.11 Ter suporte à tecnologia de chaves pública/privada (PKI), com geração *on-board* do par de chaves RSA de, no mínimo, 1024bits.

10.2.12 Possuir carcaça resistente à água e à violação.

10.2.13 Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).

10.2.14 Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).

10.2.15 Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da Microsoft (Windows 2000 e versões superiores).

10.2.16 Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente.

10.2.17 Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia

com a biblioteca PKCS#11 nativa do *token*, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE;

SETCI
Fls 05

10.2.18 Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.

10.2.19 Possuir indicador luminoso de estado do dispositivo.

10.2.20 Assinar dados digitalmente em até 10 (dez) segundos.

10.2.21 Funcionalidades:

10.2.22 permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.

10.2.23 permitir personalização eletrônica através de parâmetro identificador interno (label).

10.2.24 permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.

10.2.25 permitir criação de senhas com caracteres alfanuméricos.

10.2.26 permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.

10.2.27 permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459.

10.2.28 armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo, sendo que no caso de certificados emitidos para pessoas jurídicas, o titular é a pessoa física responsável pela empresa.

10.2.29 permitir inicialização e reinicialização do *token* mediante a utilização de PUK (Pin Unlock Key).

10.2.30 ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista e 7) e Linux (kernel 2.4, 2.6 e superiores).

10.2.31 suportar os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome.

10.2.32 possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores).

10.2.33 possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo.

10.2.34 implementar mecanismo de autenticação tipo challenge-response.

10.2.35 forçar a troca da senha padrão no primeiro acesso.

10.2.36 bloquear o dispositivo, após 15 (quinze) tentativas de autenticação com códigos inválidos.

10.2.37 avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida.

10.2.38 bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do *token*.

10.3 Software

10.3.1 Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:

10.3.2 gerenciamento do dispositivo;

10.3.3 exportação de certificados armazenados no dispositivo;

10.3.4 importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;

10.3.5 importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;

10.3.6 visualização de certificados armazenados no dispositivo;

10.3.7 apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;

10.3.8 reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.

10.3.9 Garantia de 1 (um) ano, contado a partir do aceite definitivo dos produtos;

10.3.10 caso o *token* necessite ser substituído ou apresente erro que comprometa o funcionamento do certificado ali armazenado, um novo *token* deverá ser fornecido, no prazo de até 15 (quinze) dias, contados da data da notificação.

10.4 - Do Pagamento:

10.4.1 O pagamento será efetuado em moeda nacional, por meio de ordem bancaria na conta corrente da empresa

fornecedora, efetuado em até 05 (cinco) dias uteis, através de nota fiscal devidamente atestado pelo fiscal do contrato, devendo a referida empresa comprovar que mantém todas as condições de habilitação exigida.

11 – Responsável pela consolidação desta solicitação de compras e do Termo de Referência: Data 07/03/2019 _____ Marineide Santana Pereira Gerente de Gestão e Finanças - SETCI Matrícula 14.160-1 Carimbo e assinatura	**12 – Validação Orçamentária - Financeira** SETCI Fls 06 Data 07/03/2019 _____ Marineide Santana Pereira Gerente de Gestão e Finanças - SETCI Matrícula 14.160-1 Carimbo e assinatura
13 – Setor Solicitante: Data 07/03/2019 Mat. 307483 Carimbo e assinatura	**14 – Validação da Assessoria de Planejamento ou equivalente:** Data 08/03/19 _____ Carimbo e assinatura

15 - Ordenador de despesas:

Declaro, como Ordenador de Despesas, para os fins do art. 16, inciso II da LC nº. 101, de 4/5/2000, que a presente despesa tem adequação orçamentária, financeira e está compatível com o Plano Plurianual 2018-2021 e a Lei de Diretrizes Orçamentárias 2021.

Data: 07/03/2019

_____
Carimbo e assinatura do solicitante

Edmilson Vieira das Virgens
Secretário de Transparência
e Controle Interno
Matrícula: 413032535