TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS
Avenida Aristeu de Andrade nº 377 - Bairro Farol - CEP 57051-090 - Maceió - AL

Estudos Preliminares

1. Análise de Viabilidade da Contratação (Resolução CNJ nº 182/2013 – Arts.12 e 14)

1.1. Contextualização

A implantação do Processo Judicial Eletrônico - PJE e a crescente exigência de publicação de documentos digitais com valor jurídico elevou consideravelmente a demanda por certificados digitais pelos servidores e magistrados deste Regional.

Essa demanda por um número crescente de certificados tem se mostrado um desafio no que diz respeito à gestão desses certificados, principalmente no que diz respeito aos prazos de validade e eventual revogação por motivo de perda, roubo ou desligamento do titular de suas funções no TRE-AL.

2. 2. Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

2.1. Especificações Técnicas

A solução deve apresentar as seguintes características:

1. Prover assinatura digital segura em documentos eletrônicos no PJE, DJE e documentos no formato PDF;
2. Deverá ser homologada pela ICP-Brasil;
3. Deverá prover alta disponibilidade;
4. Ter capacidade para gerenciar um número mínimo de 800 usuários e suas chaves privadas e públicas;
5. Garantir o uso de certificados digitais ICP-Brasil tipo A1 e A3 de 2048 bits passíveis de derem emitidos pelo TRE-AL por Autoridade Certificadora ICP-Brasil contratada a parte.

3. 3. Soluções Disponíveis no Mercado de TIC (Art. 14, I, a):

Um Módulo de Segurança Criptográfico (MSC), ou Hardware Security Module (HSM) em inglês, é um dispositivo de criptografia baseado em hardware, fisicamente seguro e resistente à violação, que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltadas para utilização em uma Infraestrutura de Chaves Públicas (ICP).

Um MSC gera, armazena e protege chaves criptográficas e geralmente fornece aceleração de hardware para operações criptográficas. Pode se constituir de um dispositivo independente ou apenas de uma placa auxiliar. Nesse último caso, atende unicamente ao servidor em que está instalado. Caso seja um dispositivo independente, um HSM pode atender a diversos servidores, via rede, dependendo de seu modelo e da forma como foi configurado.

A ICP-Brasil admite a utilização de MSC de outros dispositivos criptográficos, como cartões ou tokens, para a geração e guarda de chaves de titulares de certificados do tipo A3, A4, S3 e S4, desde que tais dispositivos estejam homologados na ICP-Brasil.

4. Contratações Públicas Similares (Art. 14, I, b):

- Preção Eletrônico Nº 94/2018

- Pregão Eletônico Nº 1885/2017

5. Outras Soluções Disponíveis (Art. 14, II, a):

Devido à natureza sensível das informações armazenadas, é fundamental o uso de soluções homologadas pela ICP-Brasil. Dentre as soluções homologadas para armazenamento seguro de certificados temos, além do Módulo de Segurança Criptográfico, os Tokens Criptográficos e os Cartões Criptográficos.

6. Portal do Software Público Brasileiro (Art. 14, II, b):

Não se aplica.

7. Alternativa no Mercado de TIC (Art. 14, II, c):

Não há.

8. Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d):

Não se aplica.

9. Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e):

A solução deve ser homologada pelo ICP-Brasil, contanto em sua página de Equipamentos Certificados .

10. Modelo de Requisitos Moreq-Jus (Art. 14, II, f):

Não se aplica.

11. Análise dos Custos Totais da Demanda (Art. 14, III):

Para a implantação da solução MSC/HSM será necessário:

1. Adquirir no mínimo 02 unidades do Módulo de Segurança Criptográfico, homologados pelo ITI, para armazenamento de certificados digitais padrão ICP-Brasil;

2. Contratar treinamento/Capacitação das unidades responsáveis pela sua implantação e operação.

3. Contratar suporte técnico para garantir a correta instalação, configuração e funcinamento do equipamento;

12. Escolha e Justificativa da Solução (Art. 14, IV):

A solução MSC/HSM provê um ambiente centralizado, fisicamente seguro e resistente à violação, para armazenamento de chaves criptográficas ICP-Brasil. Uma das grandes vantagens desta solução é prover um serviço de alta disponibilidade, garantindo que os usuários possam utilizar seus certificados sempre que necessário. Além disso, a solução centralizada reduz a demanda de suporte para gestão de diversos dispositivos e marcas/modelos distintos em diversos computadores.

Outras soluções como tokens e cartões criptográficos, apesar se serem mais econômicas, estão sujeitas a perda e roubo da mídia criptográfica, fazendo com que o titular do certificado fique impossibilitado de utilizar seu certificado para assinatura de documentos até que seu certificado possa ser reemitido, procedimento esse que exige contração de empresa para emissão do novo certificado juntamente com a aquisição de novo token/cartão, podendo levar até algumas semanas para ser concluído. Além disso, o uso de tokens exige a instalação de *drivers*, um para cada modelos/marca, nos computadores do Tribunal e nos dos Magistrados; demandando sempre suporte para garantir o perfeito funcionamento do certificado.

Portanto, a aquisição da solução MSC está pautada na alta disponibilidade e na redução do custo operacional gerado pelo crecente número de certificados digitais adquiridos pelo Regional.

13. Descrição da Solução (Art. 14, IV, a):

Uma solução MSC/HSM (Módulo de Segurança Criptográfica/Hardware Security Module) é um dispositivo de criptografia baseado em hardware, fisicamente seguro e resistete à violação, que fornece a geração e armazenamento de chaves criptográficas simétricas e assimétricas voltadas para utilização em uma Infraestrutura de Chaves Públicas (ICP).

Para procer segurança às chaves criptográficas e parâmetros crítitos nele armazenados, um MSC mantém conformidade com padrões de construção de hardware, levando em consideração os mais diversos ataques conhecidos.

A ICP-Brasil admite a utilização de MSCs para a geração e guarda de chaves de titulares de certificados do tipo A3, A4, S3 e S4, desde que tais dispositivos estejam homologados na ICP-Brasil.

14. Alinhamento da Solução (Art. 14, IV, b):

A aquisição deste equipamento terá impacto nos seguintes itens do PE para o período de 2016-2021:

- Tramitar eletronicamente os processos administrativos.
- Informatizar o processo judicial na Justiça Eleitoral de Alagoas.
- Assegurar a integração, a padronização e a usabilidade das soluções de TI.

15. Benefícios Esperados (Art. 14, IV, c):

1. Permitir a assinatura digital de documentos eletrônicos sem a necessidade do uso de tokens ou smartcards;
2. Garantir alta disponibilidade de certificados digitais;
3. Reduzir a demanda de suporte para diversas marcas e modelos de tokens no parque de computadores do Regional e dos Magistrados;
4. Permitir auditoria nas operações realizadas com os certificados digitais.

16. Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d):

Está prevista a demanda de 02 MSCs, juntamente com o treinamento para aquisição imediata para que o serviço esteja disponível para armazenamentos de novos certificados emitidos.

17. Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f):

Não se vislumbra necessidade de adequação para instalação do equipamento nos data centers do Regional.

18. Orçamento Estimado (Art. 14, II, g):

A ser efetuado por Unidade competente.

19. Sustentação do Contrato (Art.15)

19.1. Recursos Materiais e Humanos (Art. 15, I):

Não se aplica.

19.2. Descontinuidade do Fornecimento (Art. 15, II):

Não se aplica.

19.3. Transição Contratual (Art. 15, III, a, b, c, d, e):

Não se aplica.

19.4. Estratégia de Independência Tecnológica (Art. 15, IV, a, b):

Requerer que a solução suporte protocolos e APIs abertos minimiza a dependencia de fabricantes ou implementações específicas.

20. Estratégia para Contratação (Art.16)

20.1. Natureza do Objeto (Art. 16, I):

A solução contratada inclui tanto o fornecimento de equipamento quanto contrato de suporte por tempo limitado e treinamento/capacitação necessários para manter o serviço de gestão de certificados operacional de forma a garantir alta disponibilidade para os usuários. Não entendemos, s.m.j, como serviçoi de prestação continuada.

20.2. Parcelamento do Objeto (Art. 16, II):

Não haverá parcelamento do objeto, pois os serviços a serem contratados possuem uma interdependência, ou seja, as atividades executadas em um serviço afetam diretamente as atividades do outro, impossibilitando a separação em mais de um fornecedor, o que prejudicará a ação do fiscal para manter a qualidade das atividades contratuais.

20.3. Adjudicação do Objeto (Art. 16, III):

Adjudicação por fornecedor. Devido a interdependência dos serviços, ou seja, as atividades executadas em um serviço afetam diretamente as atividades do outro, impossibilitando a separação em mais de um fornecedor, o que prejudicará a ação do fiscal para manter a qualidade das atividades contratuais.

20.4. Modalidade e Tipo de Licitação (Art. 16, IV):

A aquisição pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

20.5. Classificação e Indicação Orçamentária (Art. 16, V):

Crédito suplementar nos termos do processo SEI nº 0001591-29.2019.6.02.8000

20.6. Vigência da Prestação de Serviço (Art. 16, VI)

Não se aplica.

20.7. Equipe de Apoio à Contratação (Art. 16, VII):

Integrante Demandante: Luiz Batista de Araujo Neto
Integrante Técnico: Alex Henrique Monte Nunes
Integrante Administrativo: Neilton Souza Silva Júnior

20.8. Equipe de Gestão da Contratação (Art. 16, VIII):

A ser designada pela SAD

21. Análise de Riscos:

Risco	Probabilidade	Dano	Impacto	Mitigação e Contigência	Responsável
Falta de recursos orçamentários para a aquisição	Média	Ausência da solução	Gestão desentralizada de certificados	Utilização de recursos destinados a outras aquisições para contemplar esta necessidade;	STI/SAD
Atraso na entrega do equipamento	Média	Impossibilidade de instalação do equipamento	Suspensão da emissão de certificados digitais	Aceleração dos trâmites internos	STI/SAD

Lista de Potenciais Fornecedores

- Dinamo Networks
- Kryptus
- SafeNet

Maceió, 07 de junho de 2019.

Documento assinado eletronicamente por **ALEX HENRIQUE MONTE NUNES**, **Técnico Judiciário**, em 15/07/2019, às 17:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0553036** e o código CRC **A53E1AAE**.

0003335-59.2019.6.02.8000 0553036v39