



Segunda-feira, 03 de maio de 2021 às 13:56, Florianópolis - SC

PUBLICAÇÃO

Nº 3017156: ATO DE DISPENSA Nº 08/2021

ENTIDADE

CIGA - Consórcio de Informática na Gestão Pública Municipal



<https://www.diariomunicipal.sc.gov.br/site/?q=id:3017156>

CIGA - Consórcio de Informática na Gestão Pública Municipal
Rua Gen. Liberato Bittencourt, n.º 1885 - Sala 102, Canto - CEP 88070-800 - Florianópolis / SC
<https://www.diariomunicipal.sc.gov.br>

ATO DE DISPENSA Nº 08/2021
PROCESSO ADMINISTRATIVO Nº 94/2021

OBJETO: Contratação dos serviços de licença de uso, renovável e permanente, de componente de hardware em nuvem do tipo IaaS (Infrastructure As A Service), denominado HSM (Hardware Security Module), para o fornecimento de segurança extra para o armazenamento de 2 (duas), podendo chegar até 10 (dez), chaves criptográficas de 2048 bits e que permita a implementação Autoridade Certificadora (AC) Raiz armazenando de forma segura, durante todo o ciclo de vida os certificados principais de uma Autoridade Certificadora de Cadeia Própria, para que a partir destas chaves, seja possível a emissão de certificados ilimitados aos entes usuários dos sistemas que permitam assinatura digital fornecidos por este consórcio.

PREVISÃO LEGAL: Art. 24, inciso II, da Lei nº 8.666/93.

JUSTIFICATIVA:

1. Identificação do Problema: os certificados eletrônicos padrão ICP-Brasil (Medida Provisória Nº 2.200-2, De 24 De Agosto De 2001) possuem ampla utilização como operações de assinatura eletrônica, porém o custo de emissão e manutenção do certificado digital torna-se inviável para uso massivo a todos os servidores da administração pública.

A Lei nº 14.063, de 23 de setembro de 2020, dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, normatiza a utilização de assinatura eletrônica avançada (certificados não emitidos pela cadeia ICP-Brasil), no caso, utiliza certificação por cadeia própria. A emissão dos certificados digitais, a implementação de Autoridades Certificadoras e a administração das emissões e revogações dos certificados de cadeia própria são um desafio para o ente público.

A situação a ser solucionada é: Garantir a guarda segura de chaves criptográficas assimétricas de 2048 bits de uma autoridade certificadora, em uma camada de hardware através de um módulo de segurança em nuvem aumentando o nível de segurança necessário para que as emissões e revogações de certificados digitais de cadeia própria para usuários dos sistemas desenvolvidos e ofertados pelo CIGA e para servidores das Prefeituras consorciadas ao CIGA, totalizando, no momento, 322 Prefeituras. Esta solução deverá comportar a escala do consórcio de forma econômica e confiável.

2. Identificação da Necessidade: A segurança da informação dos documentos se baseia em quatro pilares: Integridade, autenticidade, não repúdio e Irretroatividade:

Integridade: a integridade visa assegurar que um documento não teve seu conteúdo alterado após ter sido assinado. Para isso, o sistema é capaz de detectar alterações não autorizadas no conteúdo. O objetivo é que o destinatário verifique que os dados não foram modificados indevidamente.

Autenticidade: visa estabelecer a validade da transmissão, da mensagem e do seu remetente. O objetivo é que o destinatário possa comprovar a origem e autoria de um determinado documento.

Não repúdio: visa garantir que o autor não negue ter criado e assinado o documento.

Irretroatividade: visa garantir que o sistema não permita a geração de documentos de forma retroativa no tempo.

A Lei 14.063/2020 classifica as assinaturas eletrônicas em três categorias: assinatura eletrônica simples, assinatura eletrônica avançada e assinatura eletrônica qualificada. A utilização da assinatura eletrônica avançada é autorizada por Lei e encaixa-se nos quatro pilares da segurança da informação de documentos.

O CIGA necessita mudar os fluxos de utilização das assinaturas eletrônica simples (login e senha) para assinaturas eletrônicas avançadas (certificado digital de cadeia própria). Assim irá aumentar a segurança da informação de seus serviços e aumentará as possibilidades de novas funcionalidades.

A solução deve não só emitir o certificado digital, mas ter a garantia da guarda segura e o controle rígido de todo o ciclo de vida do certificado, emissão, validade, revogação. Além do gerenciamento a ferramenta deve ser integrada ao sistema de assinatura de documentos e ser possível automatizar processos de gerenciamento.

3. Requisitos: A guarda segura com camada de segurança em hardware do tipo nCipher validados por FIPS 140-2 Nível 2, de chaves assimétricas RSA de 2048 bits que constituem os certificados raiz da cadeia da Autoridade Certificadora do Ciga, a serem disponibilizados em nuvem

4. Solução Escolhida: Diante da solução escolhida pelo Ciga para a integração com os sistemas disponibilizados permitindo a geração de certificados e seu gerenciamento, o Lacuna AMPLIA, faz-se necessária a contratação do serviço de HSM disponibilizado em nuvem pelo Microsoft, através de seu serviço Azure Key Vault® por ser este o único com integração desenvolvida com o serviço desejado, e não havendo num curto período de tempo a expectativa de desenvolvimento pela fornecedora da solução do desenvolvimento de integrações com outros fornecedores de HSM em nuvem.

DOTAÇÃO ORÇAMENTÁRIA: Atividade nº 2.001 - Administração e Manutenção do Consórcio; Elemento de despesa 3.3.90.40.99 (Outros serviços de tecnologia da informação).

CONTRATADA: TELTEC SOLUTIONS LTDA

CNPJ: 04.892.991/0001-15

VALOR: R\$ 616,00 (seiscentos e dezesseis reais)

Florianópolis, 03 de maio de 2021.

GILSONI LUNARDI ALBINO

Diretor Executivo do CIGA



Assinado digitalmente por:

GILSONI
LUNARDI
ALBINOn912.833.
619-49
Data: 03/05/2021
13:34:56 -03:00