RESPOSTAS AO PEDIDO DE ESCLARECIMENTOS Nº 01 REFERENTE AO PREGÃO ELETRÔNICO Nº 15/2019 - PAE nº 246/2019

Prezados(as) licitantes:

Abaixo transcrevo Pedido de Esclarecimentos e respectivas respostas:

1) Conforme determinação das normas fiscais em vigor, a Certisign está obrigada a emitir notas fiscais distintas para produtos (mídias criptográfica), certificados digitais e validações presenciais. Lembramos ao contratante que as distinções das notas fiscais seguem a regulamentação de ISS e ICMS. A contratante concorda com essas condições?

Resposta: Deste que devidamente amparada pela legislação específica, não observamos qualquer óbice para a forma de faturamento informada. Acreditamos, inclusive, ser a melhor maneira.

2) Caso ocorra a invalidação, revogação em decorrência da utilização indevida do certificado e mau uso dos hardwares (tokens, smart card e leitoras), se por ventura o usuário danificar (por exemplo: quebrar, perder, molhar, etc) a mídia que armazena o certificado, ou no caso do usuário apagar o seu certificado da mídia, bloqueá-la por esquecimento de senha, (PIN e PUK), as despesas de nova emissão de certificado digital e troca dos hardwares será de responsabilidade da Contratante?

Resposta: Neste caso, a responsabilidade será do Tribunal, respondendo a empresa apenas no caso de defeito no *token* em garantia (quando for a fornecedora do *token*) ou de falhas no processo de certificação que provoquem a invalidação do certificado.

3) Considerando a resolução 130 e suas exigências, atualmente o tempo médio de validação, verificação e emissão dos certificados é de 50 minutos, sendo possível realizar o volume máximo de 07 certificados/dia. A Contratante compreende o atual cenário e concorda com o cronograma sugerido?

Resposta: Não. Este Tribunal vem realizando certificação digital de pessoal, pelo menos, nos últimos cinco anos. Portanto, devem ser observados os quantitativos solicitados no Termo de Referência. Outra opção é o encaminhamento de mais de um profissional de certificação (a critério da empresa).

4) Nos casos em que as autoridades ou servidores não comparecerem para realizar a emissão dos certificados digitais nas dependências da Contratante, entendemos que os colaboradores se deslocarão posteriormente para um ponto de atendimento da Contratada mediante agendamento para a realização da emissão. Será aceito esse modelo de atendimento?

Resposta: Sim. Consoante também a previsão constante no Termo de Referência (item 13.1.4).

5) Ressaltamos que a configuração inicial será feita de acordo com a normativa do ITI (Instituto de Tecnologia da Informação) órgão que regula a certificação digital no Brasil por motivos de segurança, onde exige no DOC ICP-10, no MCT3- vol II, pag. 51 e 54 que: "2.2.10.2 Bloqueio do PIN REQUISITO I.56: Por questões de segurança (contra ataques de adivinhação do PIN por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PIN do papel de acesso usuário após, no máximo, 5 tentativas mal sucedidas". 2.2.10.6 Bloqueio do PUK REQUISITO I.62: Por

questões de segurança (contra ataques de adivinhação do PUK por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PUK após, no máximo, 5 tentativas mal sucedidas.

Resposta: Sim. A empresa contratada, na condição de licitante deverá ofertar os serviços de acordo com as melhores práticas e com a legislação vigente.

6) Em relação à entrega das mídias criptográficas (Tokens/smart cards e leitoras), perguntamos ao Contratante qual será a forma de entrega. Poderão ser entregues em um único lote para o endereço sede, indicado no edital?

Resposta: Sim. E serão faturadas de forma independente.

7) Considerando a Resolução nº 130 de 19 de setembro de 2017 publicadas pelo ITI que institui uma quantidade limitada de atendimentos externos para emissão de certificados digitais, o órgão tem ciência que as validações de certificados previstas para ocorrerem na sede do órgão ou nos endereços por ele definidos (conforme consta no termo de referência) estarão sujeitas ao limite mensal estipulado pelo ITI e que caso este número exceda o limite mensal da AR, as validações excedentes deverão ser feitas nas dependências da contratada?

Resposta: Quanto a pergunta quanto a ciência dos quantitativos disciplinados pela Resolução em apreço, se referindo-se ao Art. 14, item 3.1.1.2, subitem VI, v.g.:

> *VI. Outras pessoas não citadas anteriormente, mediante solicitação expressa de validação externa pelo titular do certificado, limitado a 15% (quinze por cento) do total de certificados emitidos pela AR no mês imediatamente anterior.*

Sim. O cronograma de execução dos trabalhos (vide Termo de Referência, item 5.2.1, e) deverá levar em conta o volume. Entretanto, caberá a empresa licitante observar sua capacidade de atender o volume inicialmente previsto (287 certificados, quadro do lote 02, item 2.8 do TR), no prazo de 90 (noventa) dias (item 5.2.3).

8) De acordo com o subitem 2.5.2 "*Garantia de reposição do certificado digital ou correção, em caso de constatação de erro técnico no Certificate Signing Request (CSR), no prazo de 3 (três) dias após sua emissão*". Informamos a Contratante que a garantia de reposição do certificado digital ou correção, considera-se como reposição ou correção o reenvio das mesmas chaves geradas, exceto no prazo de 30 (trinta) dias contados da emissão, em que é possível a correção de determinados dados. A geração de novas chaves e emissão de um novo certificado para essas chaves é um serviço adicional, não contemplado nesta garantia.

Resposta – por analogia, já que não parece configurar uma pergunta:

As providências necessárias para correção do erro serão de responsabilidade de empresa, cabendo a ela, em obediência ao prazo estipulado, encontrar a melhor alternativa.

9) De acordo com subitem 2.4 "*Item 4 - Até 27 (vinte e sete): Certificado Digital SSL padrão AC-JUS ICP – Brasil*". Informamos a Contratante que o Certificado Digital SSL padrão AC-JUS ICP-Brasil, alertamos que, a Microsoft efetuou uma atualização tecnológica em seus navegadores e sistemas operacionais, que passaram a não confiar no certificado raiz da ICP-Brasil – V5 para emissão de certificados SSL. Os certificados da AC-JUS são emitidos sobre esta hierarquia, com isso, pode ocorrer alerta ou mensagens de segurança ao acessar sites contendo este certificado. É aceitável a emissão deste certificado sob outra hierarquia – AC Certisign Múltipla. Perguntados a Contratante se ela está ciente dessa alteração e se ela aceita a substituição?

Resposta: A princípio não. A entrega deverá corresponder ao que descreve o Termo de Referência, podendo, eventualmente, este Tribunal optar por alternativa mais vantajosa no momento da entrega (se o for ofertado, se realmente mais vantajosa e a exclusivo critério desta Corte).

10) De acordo com os subitens 17.2.22.2 "*Será responsabilidade da Contratada a configuração inicial do token criptográfico, mesmo que não seja ela a fornecedora desse dispositivo ou que não seja de primeiro uso, incluindo formatação e colhimento da senha de administração diante do emitente do certificado digital tipo A3*". E subitem 17.2.22.3 "*Caberá à empresa contratada providenciar toda a infraestrutura necessária para emissão dos certificados*". Informamos a Contratante que atualmente o Instituto de Tecnologia da Informação (ITI) homologou mais de 04 (quatro) modelos de mídias criptográficas conforme link a seguir https://www.iti.gov.br/homologacao/64-homologacao/212-equipamentos-homologados, Caso as mídias não sejam homologadas, a emissão será de responsabilidade do cliente. A Contratante está de acordo?

Resposta: Sim. A responsabilidade pelas mídias que não forem fornecidas pela empresa será do Tribunal, que acionará a empresa fornecedora ser for o caso.

11) De acordo com o subitem 2.4.3 "Emissão do certificado em até 72 (setenta e duas) horas". Informamos que a aprovação do pedido é realizada no momento da validação do certificado e que o processo de emissão é feito pelo cliente. A Contratante está de acordo?

Resposta: Não. Acreditamos estar claro que o termo "emissão" foi empregado em sentido amplo, considerando evidentemente as ações da empresa a partir do recebimento do pedido e culminando com a entrega do certificado ao solicitante, até porque, de outra forma, tratar-se-ia de processo instantâneo.

12) De acordo com o subitem 13.1.2 "*Para atendimento, as visitas técnicas para validação e emissão de certificados digitais, serão realizadas conforme agendamento de data e horário pelo Tribunal, e encaminhado junto à Central de Serviços da contratada, por meio de Ordem de Serviço, com antecedência mínima de 01 (um) dia*". Perguntamos a Contratante se é possível prorrogar esse para no mínimo 05 (cinco) dias uteis?

Resposta: O prazo de um dia, contido no item 13.1.2 diz respeito a apenas ao comunicado quanto aos horários.

O prazo de atendimento, conforme item 13.1.2, já é de 5 (cinco) dias úteis.

13) Com relação às validações, perguntamos a Contratante se ela irá até um posto de atendimento da Contratada?

Resposta: O termo de referência deixa claro que durante as visitas técnicas deverão ser realizadas todas as atividades necessárias para a entrega dos certificados digitais ao pessoal a ser indicado pelo Tribunal e explicita os casos onde poderá encaminhar servidores para serem atendidos nos postos da empresa a ser contratada. Não há qualquer ou previsão de deslocamento de pessoal do Tribunal.

14) De acordo com os subitens 3.1 "*O Tribunal possui cerca de trezentos tokens adquiridos a partir de 2015*" e subitem 3.2 "*Sempre que em bom estado de conservação, o Tribunal reaproveitará os tokens adquiridos em licitações anteriores no processo de certificação, fincando a empresa a ser contratada responsável pela inicialização deles*". Perguntamos a Contratante qual a marca e modelo já adquirido?

Resposta: Parte SafeNet (empresa Soluti) e parte SafeNet (empresa Certisign).

15) Com relação ao subitem "*2.5.4. Reemissão gratuita e ilimitada do certificado durante seu período de validade*". Considerando que para solicitar um Certificado Digital é necessário gerar um par de chaves (chave publica e chave privativa), a onde a chave pública (CSR) é enviada a Autoridade Certificadora para atestar que esta chave publica pertence ao titular da chave privativa correspondente. A chave privativa deve ser guardada de forma segura pelo seu titular e não deve ser distribuída, pois sem ela a chave pública certificada não funcionará corretamente.
A reemissão de um certificado consiste em disponibilizar o mesmo certificado digital validado anteriormente pela Autoridade Certificado. Caso o titular do certificado não possua a chave privativa correspondente ao certificado emitido, o mesmo não funcionará corretamente. Neste caso será necessário à emissão de um novo certificado (geração de um novo par de chaves), o que acarretará novo custo para a contratante. A contratante compreende o cenário e concorda com o exposto?

Resposta: Tecnicamente não se reemite um certificado digital, na prática, se emitiria um novo (outras chaves). Isso dito, a substituição gratuita de que trata o item deve ser considerada à luz das responsabilidades objetivas da empresa, sendo ela obrigada a realizar novas emissões (reemissão) apenas nos casos de sua responsabilidade (durante o prazo de validade do primeiro), de outra forma estar-se-ia a adquirir objeto não limitado e infinito já que não se previu a revogação dos anteriores.

Atenciosamente,

Adriana das Graças Faverão
Pregoeira Oficial
TRE – MT