# PE nº 13/2024

## Pedido de Esclarecimentos 1

**Questionamento 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 da área técnica:**

Sim, conforme legislação em vigor.

**Questionamento 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 da área técnica:**

Sim. Conforme explicitado no subitem 5.2.1. do Edital, a Contratada não será responsável por reparar ou por repor mídias criptográficas perdidas ou danificadas por mau uso pelo usuário. Todavia, as mídias criptográficas bloqueadas por situações como esquecimento de senha deverão ser passíveis de reutilização, por meio de remoção total dos dados armazenados e geração de nova senha de acesso.

**Questionamento 3:**

A Contratante está adquirindo uma quantidade inferior de tokens, considerando o número de certificados solicitados. Neste caso perguntamos a Contratante qual a marca e modelo das mídias já adquiridas?

**Resposta da área técnica:**

Conforme consta no subitem 3.5.17 do Edital, o token e seu gerenciador deverão ser compatíveis com os sistemas utilizados neste Regional. Atualmente o TRT3 utiliza as mídias Giesecke & Devrient StarSing Crypto USB, SAFENET 5110, SAFENET 5100 e ePass2003. O token ePass2003 tem apresentado incompatibilidades com as aplicações Assinatura de Certidão Judicial, ACJ, e com assinatura de despachos de recursos e de agravos de instrumento no programa eRec (eRevista), de maneira que a sua substituição tem sido realizada gradativamente, portanto, esta mídia não será aceita. Caso a proposta contemple mídia de outro modelo, a empresa vencedora deverá fornecer amostra, que será testada pela equipe técnica do Tribunal em até 5 (cinco) dias úteis após o

fornecimento, de modo que um técnico do TRT3 emitirá parecer sobre a aceitabilidade ou não do dispositivo.

**Questionamento 4:**

Informamos que os usuários do Poder Judiciário do Estado de Mato Grosso do Sul aptos a receberem os Certificados Digitais e que possuam CNH, e ainda levando em conta a IN do ITI nº 005/2021 em vigor desde fevereiro/2021 onde é permitido a validação de forma remota (videoconferência), a emissão/validação do certificado digital pode ocorrer nesta modalidade. A emissão dos certificados digitais pode ocorrer por videoconferência (de forma on line) e presencialmente com o cliente se dirigindo a um de nossos pontos de atendimento (ARs). A contratante se utilizará destes 2 meios para emissão? Está correto nosso entendimento?

**Resposta da área técnica:**

Conforme se verifica no subitem 3.6.3.1 do Edital, as emissões de certificados devem seguir as seguintes diretrizes:

a. A validação, emissão e/ou gravação do certificado digital no modelo tradicional (token) ou em nuvem ocorrerá, preferencialmente, de forma remota (on-line ou por videoconferência, nos termos da Instrução Normativa n. 5, de 22 de fevereiro de 2021 do Instituto Nacional de Tecnologia da Informação (ITI) - ou a que vier a substituí-la - e legislação correlata). No entanto, a Contratada deverá possuir posto de atendimento em Belo Horizonte/Minas Gerais para emissão/renovação de certificados para magistrados/servidores que não quiserem ou não puderem emitir seus certificados de forma remota (como exemplo cita-se as pessoas que não possuem carteira de habilitação e nunca emitiram certificado digital – estas, necessariamente, precisam realizar a emissão presencial). No caso de a Contratada disponibilizar infraestrutura em outras localidades, por sua exclusiva liberalidade, estas poderão ser utilizadas pelos(as) magistrados(as)/servidores(as) do TRT3;

b. As emissões/renovações remotas (por videoconferência) e presenciais devem ser realizadas em dia e horário previamente agendados pelo magistrado(a)/servidor(a) por telefone, e-mail ou sistema próprio da Contratada, devendo ocorrer em até 3 (três) dias úteis da solicitação ou conforme acordado entre magistrado(a)/servidor(a) e a empresa Contratada;

c. As emissões/renovações on-line, disponíveis no sítio eletrônico da Contratada, não devem necessitar qualquer tipo de agendamento por parte dos magistrados(as)/servidores(as). Para auxílio aos usuários, a Contratada deverá manter suporte técnico em língua portuguesa (por telefone, chat on-line, whatsApp ou sistema próprio), que deverá estar disponível de segunda a sexta-feira, das 9h às 18h, horário de Brasília (GMT-3), exceto feriados nacionais;

d. A Contratada manterá pasta na nuvem para envio, pelo Contrante, das autorizações de emissão das certificações digitais, de modo que não seja necessário, em regra, o envio de autorizações impressas. Poderá ser adotado outro modelo, a critério do Contratante;

e. A Contratada deve realizar a configuração inicial do token criptográfico (se o caso de emissão tradicional), mesmo que não seja a fornecedora desse dispositivo, incluindo formatação, por meio de remoção total dos dados armazenados e geração de nova senha de acesso diante do emitente do

certificado digital tipo A3 (atualmente o TRT3 utiliza as mídias Giesecke & Devrient StartSing Crypto USB, SAFENET 5110, SAFENET 5100 e ePass2003);

f. O certificado digital será considerado emitido no momento em que o par de chaves for gerado no dispositivo de armazenamento, as cadeias de certificados ICP-Brasil importadas e gerada a evidência, por parte da empresa Contratada, de que o certificado está funcionando corretamente;

g. A emissão de certificados digitais compreende as atividades de inicialização do dispositivo criptográfico com as senhas de administrador e de usuário, validação da documentação, importação do certificado digital e das cadeias de certificado necessárias para sua correta utilização, apresentação das instruções necessárias e solicitadas pelo usuário e coleta da evidência de emissão;

h. A evidência da emissão do certificado digital tipo A3 poderá ser caracterizada pelo envio de e-mail com documento e/ou o próprio e-mail assinado digitalmente;

i. No momento da emissão do certificado digital armazenado em token deverão ser alteradas as senhas PIN e PUK para senhas de escolha do magistrado/servidor;

j. O magistrado/servidor deve ser orientado sobre a importância destas senhas e sobre princípios básicos de segurança na utilização de certificação digital (esta orientação pode ser entregue por escrito em material entregue fisicamente ou por e-mail).