

**Esclarecimento 22/10/2020 11:29:52**

PEDIDO DE ESCLARECIMENTO PE 110/20 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? 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? 3) Considerando o longo período contratual, perguntamos à contratante se mediante comunicado formal, poderá ser fornecido mais de um modelo de mídia criptográfica, compatível com o objeto e devidamente homologada pelo ITI (Instituto de Tecnologia da Informação) e pelo Inmetro? Afirmamos que tal necessidade não impactará no pleno atendimento do contrato. 4) Em relação às validações na Contratante, poderá ser estabelecido junto a Contratada um cronograma para execução do objeto, considerando um volume fixo de validações/dia (10 certificados) para que o tempo seja otimizado? 5) A Contratante disponibilizará a contratada para as emissões dos certificados, impressora, scanner, telefone e internet para que os atendimentos sejam executados com eficiência, considerando que poderá haver intermitência no sinal do 4G, impactando diretamente no tempo do atendimento? 6) Ressaltamos que a configuração inicial dos tokens é 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. 7) Em relação à quantidade de visitas a serem adquiridas pelo contratante, afirmamos que a quantidade diária de emissões é em torno de 10 certificados, considerando a carga horária de 8 horas, com 01 hora de almoço e os procedimentos de validação, verificação e emissão dos certificados. Desta forma, questionamos ao cliente, se o contratante se deslocará aos pontos de atendimento da contratada para efetuar a validação presencial do saldo restante de certificados já que a quantidade de visitas é menor que a quantidade de certificados? 8) Considerando o cenário atual do Brasil a respeito do Coronavírus (COVID-19), questionamos ao Contratante de que forma serão conduzidas as validações presenciais para as emissões dos certificados digitais? 9) Em relação às validações, informamos que os postos das ARs tem uma mudança constante (abrem e fecham), não sendo possível mantermos um controle sobre o fechamento ou abertura das ARs nas cidades. Diante disso perguntamos a Contratante, caso a Contratada não possua posto de atendimento em algumas das cidades, a Contratada poderá realizar as validações na sede da Contratante, sem que isso gere nenhum custo adicional para a Contratante? 10) De acordo com o ITEM 01 – "EMISSÃO DE CERTIFICADO DIGITAL DE PESSOA FÍSICA com fornecimento de dispositivos tokens criptográficos (TIPO A3)". E subitem 1.11 "Os certificados, tokens e drivers fornecidos pela Contratada devem ser compatíveis com os softwares de assinatura utilizados pelo Contratante". Visando garantir a melhor oferta dos serviços, solicitamos gentileza informar quais são os softwares utilizados pela CONTRATANTE? 11) De acordo com o ITEM 9 – "DAS CONDIÇÕES E PRAZOS DE ENTREGA" E subitem 9.3. "Após o início dos serviços, a Contratada terá 02 (dois) dias úteis para atender um pedido do Contratante para emissão de certificado nas capitais de Rio de Janeiro ou Espírito Santo, ou 03 (três) dias úteis nas demais localidades". Considerando o quantitativo a ser entregue e a necessidade de negociação entre CONTRATADA x Parceiros (Rede de atendimento nas localidades indicadas), os prazos indicados no item 9.3 em questão, se tornam insatisfatórios para uma excelência na prestação do serviço. Assim, solicitamos gentileza o acréscimo de pelo ao menos 1 (um) dia útil nas capitais do Rio de Janeiro ou Espírito Santo, totalizando 03 (três) dias uteis e acréscimo de ao menos 02 (dois) dias úteis para demais localidades, totalizando 05 (cinco) dias úteis. Nossa solicitação será acatada?

**Fechar**

**Resposta 22/10/2020 11:29:52**

RESPOSTA PEDIDO DE ESCLARECIMENTO PE 110/20 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? Cabe ao Contratante providenciar o pagamento dos serviços prestados à vista dos documentos fiscais apresentados. Cabe a cada empresa atentar para a legislação fiscal que rege a emissão de suas notas fiscais. 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? A Contratada não é responsável nessas situações 3) Considerando o longo período contratual, perguntamos à contratante se mediante comunicado formal, poderá ser fornecido mais de um modelo de mídia criptográfica, compatível com o objeto e devidamente homologada pelo ITI (Instituto de Tecnologia da Informação) e pelo Inmetro? Afirmamos que tal necessidade não impactará no pleno atendimento do contrato. Está correto o entendimento, desde que respeitado o item 1.9 do Anexo I-A do Termo de Referência 4) Em relação às validações na Contratante, poderá ser estabelecido junto a Contratada um cronograma para execução do objeto, considerando um volume fixo de validações/dia (10 certificados) para que o tempo seja otimizado? Tendo em vista a quantidade de visitas técnicas previstas no futuro contrato não é possível garantir um mínimo de validações/dia, devendo a Contratada se planejar conforme previsto no item 4 do Anexo I-A do Termo de Referência 5) A Contratante disponibilizará a contratada para as emissões dos certificados, impressora, scanner, telefone e internet para que os atendimentos sejam executados com eficiência, considerando que poderá haver intermitência no sinal do 4G, impactando diretamente no tempo do atendimento? A Contratada deverá utilizar seu próprio material/equipamento conforme previsto no item 4.6 do Anexo I-A do Termo de Referência 6) Ressaltamos que a configuração inicial dos tokens é 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. A Contratante está ciente 7) Em relação à quantidade de visitas a serem adquiridas pelo contratante, afirmamos que a quantidade diária de emissões é em torno de 10 certificados, considerando a carga horária de 8 horas, com 01 hora de almoço e os procedimentos de validação, verificação e emissão dos certificados. Desta forma, questionamos ao cliente, se o contratante se deslocará aos pontos de atendimento da contratada para efetuar a validação presencial do saldo restante de certificados já que a quantidade de visitas é menor que a quantidade de certificados? Está correto o entendimento. 8) Considerando o cenário atual do Brasil a respeito do Coronavírus (COVID-19), questionamos ao Contratante de que forma serão conduzidas as validações presenciais para as emissões dos certificados digitais? O atendimento nas validações presenciais deverá ser feito de acordo com o item 17.7 do Edital e item 4.1.12 do futuro contrato. 9) Em relação às validações, informamos que os postos das ARs tem uma mudança constante (abrem e fecham), não sendo possível mantermos um controle sobre o fechamento ou abertura das ARs nas cidades. Diante disso perguntamos a Contratante, caso a Contratada não possua posto de atendimento em algumas das cidades, a Contratada poderá realizar as validações na sede da Contratante, sem que isso gere nenhum custo adicional para a Contratante? Está correto o entendimento, ressaltando que, neste caso, não será contabilizada uma visita técnica (item 2.2.4) e que a Contratada deverá dispor, no mínimo, de postos de atendimento nas capitais dos estados do Rio de Janeiro e Espírito Santo, conforme previsto no Edital 10) De acordo com o ITEM 01 – "EMISSÃO DE CERTIFICADO DIGITAL DE PESSOA FÍSICA com fornecimento de dispositivos tokens criptográficos (TIPO A3)". E subitem 1.11 "Os certificados, tokens e drivers fornecidos pela Contratada devem ser compatíveis com os softwares de assinatura utilizados pelo Contratante". Visando garantir a melhor oferta dos serviços, solicitamos gentileza informar quais são os softwares utilizados pela CONTRATANTE? O software de assinatura é o Assijus (desenvolvimento internamente) sendo também utilizada a assinatura de emails através do Microsoft Outlook 11) De acordo com o ITEM 9 – "DAS CONDIÇÕES E PRAZOS DE ENTREGA" E subitem 9.3. "Após o início dos serviços, a Contratada terá 02 (dois) dias úteis para atender um pedido do Contratante para emissão de certificado nas capitais de Rio de Janeiro ou Espírito Santo, ou 03 (três) dias úteis nas demais localidades". Considerando o quantitativo a ser entregue e a necessidade de negociação entre CONTRATADA x Parceiros (Rede de atendimento nas localidades indicadas), os prazos indicados no item 9.3 em questão, se tornam insatisfatórios para uma excelência na prestação do serviço. Assim, solicitamos gentileza o acréscimo de pelo ao menos 1 (um) dia útil nas capitais do Rio de Janeiro ou Espírito Santo, totalizando 03 (três) dias uteis e acréscimo de ao menos 02 (dois) dias úteis para demais localidades, totalizando 05 (cinco) dias úteis. Nossa solicitação será acatada? O Contratante considera razoáveis e exequíveis os prazos fixados no item 9.3, principalmente considerando que nas capitais a Contratada sempre deverá dispor de postos de atendimento. Ainda assim, após a assinatura do Contrato, a Contratada poderá em conjunto com o Contratante trabalhar num planejamento prévio das necessidades de certificados e localidades, visando se organizar com antecedência para as prováveis emissões. Ass. Rubens Ferraz – Pregoeiro Substituto

**Fechar**