Aline Matos Saraiva [alinesaraiva] - Terça 21/01/2020

Minhas Preferências Sugestões Ajuda

30% (314 MB/1.0 GB)

EXPRESSO MAIL

Nova Mensagem
Atualizar
Ferramentas ...
Minhas pastas
Caixa de entrada
Rascunhos
Enviados
Spam
Lixeira [5]
Antigos
Pastas compartilhadas
licitacao [1188] [833]
Para acompanhamento

licitacao [1188 / 1315] | PEDIDO DE ESCLARECIMEN

daniela.oliveir..., 20/01/2020

Enviado por: "Daniela Andrade de Oliveira Santos" <daniela.oliveira@certisign.com.br>
De: daniela.oliveira@certisign.com.br
Para: "licitacao@mpam.mp.br" <licitacao@mpam.mp.br>
Data: 20/01/2020 16:28
Assunto: PEDIDO DE ESCLARECIMENTO - MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS - Pregão Eletrônico 4.003/2020
Anexos: 8 arquivos :: Baixar todos de uma vez Remover anexos
image001.png (3 KB)
image002.png (213 B)
image003.png (253 B)
image004.png (314 B)
image005.png (274 B)
image006.png (338 B)
Pedidos de Esclarecimentos_ Procuradoria Geral da Justiça Amozonas.docx (35 KB)
smime.p7s (6 KB)

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS

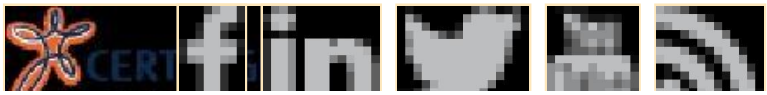
**A/C Sr.(a) Pregoeiro(a).**
**Ref:** Pedido de esclarecimentos
Pregão Eletrônico 4.003/2020-CPL/MP/PGJ-SRP
Abertura: 28/01/2020 – 10h00min
licitacao@mpam.mp.br

A empresa CERTISIGN CERTIFICADORA DIGITAL S.A CNPJ: 01.554.285/0001-75, vem pela presente solicitar esclarecimentos

CERTISIGN
A sua identidade na rede

Daniela Oliveira | Analista de Licitações
Certisign | daniela.oliveira@certisign.com.br
+55 11 4501.1865

8 anexos na mensagem :: Baixar todos de uma vez
**Dica:** Para salvar rapidamente, clique sobre a imagem com o *botão direito* do mouse.



Excluir Mover Imprimir Exportar Importar | Marcar como Spam

**MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS**

**A/C Sr.(a) Pregoeiro(a).**
**Ref:** Pedido de esclarecimentos
Pregão Eletrônico 4.003/2020-CPL/MP/PGJ-SRP
Abertura: 28/01/2020 – 10h00min
licitacao@mpam.mp.br

A empresa CERTISIGN CERTIFICADORA DIGITAL S.A CNPJ: 01.554.285/0001-75, vem pela presente solicitar esclarecimentos sobre a licitação conforme abaixo:

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) A contratante pode disponibilizar os valores unitários estimados para o objeto desta licitação?

9) Em relação às mídias, notamos que a quantidade de certificado é maior que a quantidade de mídias solicitadas. Perguntamos a Contratante se ela já possui as mídias? Em caso positivo por favor informar marca e modelo das mídias já adquiridas.

10) Em relação às validações, perguntamos a Contratante se todas as validações serão realizadas no endereço "*Av. Coronel Teixeira, n.º 7.995 – Nova Esperança II (Ponta Negra), CEP. 69037-473 / Manaus-AM*".

11) De acordo com o subitem 2.3 Item 3. "*Certificado digital SSL WILDCARD para sistemas web*". Trata-se de certificado WildCard de raiz INTERNACIONAL, correto?

12) De acordo com o subitem 2.3.5 "*Emissão do certificado em até 72 (setenta e duas) horas*". Considerando que deve haver o processo de validação, às 72 horas se iniciam após esse processo, correto?

13) De acordo com o subitem 2.3.6 "*A CONTRATANTE poderá solicitar à CONTRATADA, num período de 7 (sete) dias após a emissão inicial de um certificado, a sua re-emissão ou a substituição quantas vezes forem necessárias*". Informamos a Contratante que a re-emisão pode ser solicitada inúmeras vezes, mas a substituição, que conceitualmente se trata da TROCA DOS DADOS DO PRODUTO, possui custo adicional. Desta forma, no período de 07 (sete) dias é garantida apenas a re-emissão. Podemos seguir com este entendimento?

14) De acordo com o subitem 4.2.1 "*A CONTRATADA deverá prover garantia de correção e atualização motivadas por falhas técnicas, pelo período mínimo de 24 (vinte e quatro) meses para o certificado SSL WILDCARD, contados a partir da data de emissão do mesmo*". Entende-se por falha técnica qualquer falha no certificado por culpa da autoridade certificadora. Podemos seguir com este entendimento?

Agradecemos a oportunidade e aproveitamos para reiterar nossos protestos da mais alta estima.

Atenciosamente,
Certisign Certificadora Digital S.A
(11) 4501-2173/1865
E-mail: editais@certisign.com.br