



TRIBUNAL SUPERIOR ELEITORAL
RESPOSTA A QUESTIONAMENTO/IMPUGNAÇÃO

Referência: Edital de Licitação TSE nº 1/2021, Concorrência, Tipo Técnica e Preço.
2020.00.000007979-5

Assunto: Questionamento 4 - Positivo Tecnologia S.A.

Trata-se de pedido de esclarecimento encaminhado, via mensagem eletrônica, pela empresa Positivo Tecnologia S.A., inscrita no CNPJ sob o nº 81.243.735/0001-48, no uso da faculdade prevista no Capítulo XVII do Edital, interessada em participar da licitação TSE nº 1/2021, Modalidade Concorrência, Tipo Técnica e Preço – Registro de Preços para eventual produção e fornecimento de até 176.000 (cento e setenta e seis mil) urnas eletrônicas (UE2022), de acordo com as especificações, condições e prazos do Edital e seus anexos.

PRELIMINARMENTE

2. O pedido preenche os requisitos legais, pois foi apresentado tempestivamente e nos seguintes termos:

1) No item 125.1.3 da subseção F. Testes de Segurança consta: "125.1.3. Um arquivo de configuração, comum a todas as Licitantes, será fornecido pelo TSE na ocasião da publicação do Edital e deverá fazer parte do Makefile utilizado na compilação do Kernel;". No dia 24/06/2021 foi liberado pelo TSE um arquivo compactado chamado Insumos_para_os_testes_ME. Dentro deste arquivo encontramos o arquivo compactado configuração src_so_kernel_linux-5.4.x.config onde se encontra o arquivo de configuração .config relativo ao item 125.1.3 acima. Utilizando este arquivo constatamos que ele faz inclusões de arquivos específicos não disponibilizados pelo TSE. Entendemos que será permitido alterar as configurações abaixo para não incluir estes arquivos e suas dependências que serão alteradas de forma automática. I - Mudar: CONFIG_SYSTEM_TRUSTED_KEYRING=y Para: # CONFIG_SYSTEM_TRUSTED_KEYRING is not set II - Mudar: CONFIG_SYSTEM_TRUSTED_KEYS="certs/sevin.x509" Para: CONFIG_SYSTEM_TRUSTED_KEYS=" " III - Mudar: CONFIG_MODULE_SIG=y Para: # CONFIG_MODULE_SIG is not set Também, se faz necessário alterar a configuração abaixo, pois é necessário para o systemd funcionar. A ativação desta configuração inclui as dependências para o systemd ser executado corretamente. Mudar: # CONFIG_CGROUPS is not set Para: CONFIG_CGROUPS=y Questionamos: Entendemos que será permitido alterar o arquivo .config conforme descrito acima para a correta realização do teste descrito na subseção F - Teste de Segurança do Anexo Ia. Está correto o nosso entendimento? 2) Na subseção C.2. Testes de Autonomia do Anexo Ia é informado no item 24.2.3 que a CAT fornecerá às licitantes a bobina de papel térmico conforme as especificações exigidas no Anexo II. Solicitamos o fornecimento destas bobinas de papel para testes no Modelo de Engenharia a ser apresentado juntamente com a proposta técnica. 3) Na subseção D.1 Testes de não interferência de bateria descarregada, informação de controle da fonte ao software e de seleção automática de alimentação - do Anexo Ia - é solicitado no subitem item 30.1. - Teste A: "30.1.1. Conectar bateria interna descarregada e utilizada nos testes de autonomia ao ME; 30.1.2. Conectar a fonte externa CC ligada a um multímetro, regular para 12Vcc e ligar o ME; 30.1.3. Imprimir um relatório com leiaute igual ao ilustrado abaixo e coletar uma biometria; 30.1.4. Alterar a tensão da fonte externa para o limiar inferior de 10,5Vcc (aceitável até 11Vcc); 30.1.5. Imprimir um relatório igual ao do item 30.1.3 e coletar uma biometria;". Questionamos: A tecnologia da bateria ofertada considera que quando a bateria estiver com tensão de 10,5Vcc a 12Vcc a mesma se encontrará em estado crítico. Tendo em vista que quando a bateria entrar em estado crítico, a Urna Eletrônica permite operação de apenas 6 a 10 minutos antes de se desligar para evitar danos à bateria, entendemos que este teste deverá ser realizado dentro deste período e, caso não seja possível sua finalização, a licitante poderá reiniciar este teste sem ser penalizada. Está correto o nosso entendimento? Caso não esteja correto favor esclarecer. 4) Na subseção D.1 Testes de não interferência de bateria descarregada, informação de controle da fonte ao software e de seleção automática de alimentação do Anexo Ia é solicitado no subitem 30.7. - Teste G: "30.7.1. Conectar a fonte externa CC ligada a um multímetro e previamente regulada para 12Vcc; 30.7.2. Imprimir um relatório igual ao do item 30.1.3 e coletar uma biometria; 30.7.3. Alterar a tensão da fonte externa para o limiar inferior de 10,5Vcc (aceitável até 11Vcc); 30.7.4. Imprimir um relatório igual ao do item 30.1.3 e coletar uma biometria;". Questionamos: A tecnologia da bateria ofertada considera que quando a bateria estiver com tensão de 10,5Vcc a 12Vcc a mesma se encontrará em estado crítico. Tendo em vista que quando a bateria entra em estado crítico, a Urna Eletrônica permite operação de apenas de 6 a 10 minutos antes de se desligar para evitar danos à bateria, entendemos que este teste deverá ser realizado dentro deste período e, caso não seja possível sua finalização, a licitante poderá reiniciar este teste sem ser penalizada. Está correto o nosso entendimento? 5) Na subseção D.1 Testes de não interferência de bateria descarregada, informação de controle da fonte ao software e de seleção automática de alimentação do Anexo Ia é solicitado no item 30.10. - Teste J: "30.10.1. Alterar a tensão da fonte externa para 12,0Vcc; 30.10.2. Desconectar o ME da rede AC; 30.10.3. Imprimir um relatório igual ao do item 30.1.3 e coletar uma biometria; 30.10.4. Alterar a tensão da fonte externa para o limiar inferior de 10,5Vcc; 30.10.5. Imprimir um relatório igual ao do item 30.1.3 e coletar uma biometria;". Questionamos: A tecnologia da bateria ofertada considera que quando a bateria estiver com tensão de 10,5Vcc a 12Vcc a mesma se encontra em estado crítico. Tendo em vista que quando a bateria entra em estado crítico, a Urna Eletrônica permite operação de apenas de 6 a 10 minutos antes de se desligar para evitar danos à bateria, entendemos que este teste deverá ser realizado dentro deste período e, caso não seja possível sua

finalização, a licitante poderá reiniciar este teste sem ser penalizada. Está correto o nosso entendimento? 6) Em relação à subseção F.7. Tempo para assinatura de blocos de dados do Anexo Ia é descrito o procedimento: “167.1. Para a realização deste teste, o ME-UE2022 deverá utilizar a placa-mãe sem o chip que contém o processador principal da placa-mãe (item 127.1); 167.2. Para efeito de aferição, o MSE deverá executar o algoritmo E-521 que faz parte da libe521 fornecida, em seu modo determinístico, conforme versão indicada no Anexo IV; 167.3. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo e521 da biblioteca libe521, conforme comando do item 132.1; 167.4. A equipe do TSE gerará um bloco de valores aleatórios de 1024 bytes; 167.5. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item 129) para que, usando um computador (item 130), implante, em memória não-volátil do microcontrolador do MSE, a parte privada do par de chaves gerado pelo TSE no passo 167.3 e o bloco de valores aleatórios gerados no passo 167.4. A equipe da Licitante definirá a posição de memória onde será inicialmente alocado o referido bloco; 167.6. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE; 167.7. A equipe da Licitante reiniciará o ME-UE2022 e o firmware do MSE deverá executar 1.000 (hum mil) iterações, em um procedimento iterativo de assinaturas digitais EdDSA com a chave implantada no passo 167.5, do bloco de valores aleatórios implantados no mesmo passo; 167.8. A cada iteração, o bloco de valores aleatórios deverá ser alterado de forma que os 10 (dez) primeiros bytes da assinatura obtida ocupem, na mesma ordem, os 10 (dez) primeiros bytes do bloco de valores aleatórios. 167.8.1. O resultado da assinatura do bloco de valores aleatórios (modificado conforme item 167.8) deverá ser exibido no display do MSE, a cada 25 (vinte e cinco) iterações, incluindo a exibição da primeira iteração, conforme formato e regras definidas no item 133; 167.8.2. A cada uma das 1000 (hum mil) iterações, o ME da licitante deverá anexar a respectiva assinatura gerada em formato RAW, sem qualquer estrutura, em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 129), com o auxílio de um computador (item 130); 167.9. Após o final do teste, o espaço de memória utilizado para armazenamento das informações geradas no item 167.8.2 deverá ser gravado em um arquivo no computador (item 130), com a utilização do equipamento leitor/gravador no MSE (item 129) 167.9.1. Se necessário o ME poderá ser reiniciado; 167.9.2. O arquivo deverá conter as informações geradas no item 167.8.2, referentes a todas as iterações e na mesma ordem em que foram geradas; 167.10. Para registrar o tempo total, deverá ser utilizada uma câmera de vídeo para registrar o display do MSE ao lado de um cronômetro. O resultado desse teste é o tempo médio da assinatura do bloco de dados, ou seja, o tempo total obtido com o método descrito, a partir da exibição da primeira iteração, até a 1000ª iteração; 167.10.1. O tempo total apurado será dividido por 999 (novecentos e noventa e nove); 167.10.2. A câmera de vídeo iniciará a gravação antes do passo 167.7; 167.11. O TSE irá analisar o vídeo, para verificar a correspondência entre as partes das assinaturas exibidas no display do MSE, relativas às iterações registradas em vídeo, e as respectivas assinaturas geradas e recuperadas no arquivo do item 167.9; 167.12. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.”. Questionamos: No item 167.7. consta que será executado um procedimento iterativo de assinaturas digitais EdDSA. Entendemos que para este teste, a assinatura do bloco de 1024 bytes será feita sem o uso de algoritmo de hash (SHA512) externo à função de assinatura EdDSA. Está correto o nosso entendimento?

DA ANÁLISE DO PEDIDO DE ESCLARECIMENTO

3. Em resposta ao pedido de esclarecimento e com fundamento no Parecer da Comissão de Assessoramento Técnico, documento acostado nos autos sob nº 1736136, consigno, a seguir, as respostas. **Resposta 1** - Sim, o entendimento está correto. Tais alterações não causam impacto no desempenho do *kernel* compilado. Destaca-se que todas as licitantes deverão utilizar, após as referidas adaptações, o mesmo arquivo de configuração, conforme indicado no item 125.1.3 do Anexo Ia. **Resposta 2** - Esta CAT disponibilizou bobinas à CPL para fornecimento às licitantes interessadas. Contudo, não foi especificada a quantidade pela licitante. Assim, esta CAT sugere um quantitativo máximo de 02 (duas) unidades por licitante interessada. **Resposta 3** - Sim, o entendimento está correto. **Resposta 4** - Sim, o entendimento está correto. **Resposta 5** - Sim, o entendimento está correto. **Resposta 6** - Sim, o entendimento está correto.

ENCAMINHAMENTO

À **Senhora Secretária de Administração**, para ciência e, se entender pertinente, ao **Senhor Diretor-Geral** com a mesma finalidade.

É a informação.

NATHALIA DOS SANTOS COSTA
PRESIDENTE DA COMISSÃO PERMANENTE DE LICITAÇÃO



Documento assinado eletronicamente em **02/08/2021, às 13:05**, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1737855&crc=C14C7068, informando, caso não preenchido, o código verificador **1737855** e o código CRC **C14C7068**.