ANEXO II – ESPECIFICAÇÕES TÉCNICAS
Pregão Eletrônico SRP nº ___/2023 – Processo Administrativo nº 0144/2023

1. ESPECIFICAÇÕES DOS ITENS

1.1. ITEM 1: Emissão de Certificado digital para Pessoa Física (e-CPF A3 com Token)

1.1.1. Certificado nível A3 – tipo e-CPF;

1.1.2. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil);

1.1.3. **Validade: 3 (três) anos**, contados da data de emissão do certificado;

1.1.4. Aderente às normas do Comitê Gestor da ICP-Brasil;

1.1.5. O presente item engloba o respectivo serviço de autoridade de registro;

1.1.6. Deverá ser fornecido, acompanhando cada certificado digital emitido, um dispositivo criptográfico de armazenamento do certificado digital (token), que deverá atender, minimamente, às seguintes especificações técnicas:

1.1.6.1. Deverá ser capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil;

1.1.6.2. Totalmente compatível com as especificações do certificado digital do tipo A3;

1.1.6.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 2.0 (ou superior compatível com a versão 2.0);

1.1.6.4. Emitir conexão direta com a porta USB, sem necessidade de interface intermediária para leitura;

1.1.6.5. Seguir as regras estabelecidas para o nível 3 (ou superior) de segurança do padrão FIPS 140-2 e também ser aderente às demais normas do Comitê Gestor da ICP-Brasil;

1.1.6.6. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres;

1.1.6.7. Permitir criação de senhas com caracteres alfanuméricos;

1.1.6.8. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos;

1.1.6.9. Fornecer driver e programa de gerenciamento para o Sistema Operacional Microsoft Windows 10 e versões superiores;

1.1.6.10. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução;

1.1.6.11. Suportar, pelo menos, os seguintes navegadores: *Microsoft Internet Explorer* (versão 7.0 e superiores), *Firefox* (versão 45.0 e superiores) e *Google Chrome* (versão 35 ou superior);

1.1.6.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do Titular do dispositivo;

1.1.6.13. O bloqueio do dispositivo deverá seguir as recomendações das normas do ICP-

Brasil;

1.1.6.14. O *Software* de gerenciamento do dispositivo deverá estar no idioma Português do Brasil.

1.1.6.15. Requisição Mínima: 1 (uma) unidade.

1.2. ITEM 2: Emissão de Certificado digital para Pessoa Física (e-CPF A3 sem Token)

1.2.1. Certificado nível A3 – tipo e-CPF;

1.2.2. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil);

1.2.3. **Validade: 3 (três) anos,** contados da data de emissão do certificado;

1.2.4. Aderente às normas do Comitê Gestor da ICP-Brasil;

1.2.5. O presente item engloba o respectivo serviço de autoridade de registro.

1.2.6. Requisição Mínima: 1 (uma) unidade.

1.3. ITEM 3: Emissão de Certificado digital para Pessoa Jurídica (e-CNPJ A3 com token)

1.3.1. Certificado nível A3 – tipo e-CNPJ;

1.3.2. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil);

1.3.3. **Validade: 3 (três) anos**, contados da data de emissão do certificado;

1.3.4. Aderente às normas do Comitê Gestor da ICP-Brasil;

1.3.5. O presente item engloba o respectivo serviço de autoridade de registro;

1.3.6. Deverá fornecer em conjunto com o certificado digital um dispositivo de armazenamento do certificado digital do tipo token (para cada certificado) totalmente compatível e com as seguintes especificações técnicas mínimas:

a) Deverá ser capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil;

b) Totalmente compatível com as especificações do certificado digital do tipo A3;

c) Possuir conector USB (Universal Serial Bus) tipo A, versão 2.0 (ou superior compatível com a versão 2.0);

d) Emitir conexão direta com a porta USB, sem necessidade de interface intermediária para leitura;

e) Seguir as regras estabelecidas para o nível 3 (ou superior) de segurança do padrão FIPS 140-2 e também ser aderente às demais normas do Comitê Gestor da ICP-Brasil;

f) Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres;

g) Permitir criação de senhas com caracteres alfanuméricos;

h) Permitir geração de chaves, protegidas por *PINs* (*Personal Identification Number*), compostos por caracteres alfanuméricos;

i) Fornecer *driver* e programa de gerenciamento para o Sistema Operacional *Microsoft Windows* 10 e versões superiores;

j) Armazenar chaves privadas em repositório de dados próprio, controlado pela solução;

k) Suportar, pelo menos, os seguintes navegadores: *Microsoft Internet Explorer* (versão 7.0 e superiores), *Firefox* (versão 45.0 e superiores) e *Google Chrome* (versão 35 ou superior);

l) Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do Titular do dispositivo;

m) O bloqueio do dispositivo deverá seguir as recomendações das normas do ICP-Brasil;

n) O *Software* de gerenciamento do dispositivo deverá estar no idioma Português do Brasil.

1.3.7. Requisição Mínima: 1 (uma) unidade;

1.4. ITEM 4: Emissão de Certificado digital para Pessoa Jurídica (e-CNPJ A1)

1.4.1. Certificado nível A1 – tipo e-CNPJ;

1.4.2. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil);

1.4.3. **Validade: 12 (doze) meses**, contados da data de emissão do certificado;

1.4.4. Aderente às normas do Comitê Gestor da ICP-Brasil;

1.4.5. O presente item engloba o respectivo serviço de autoridade de registro;

1.4.6. O certificado digital deve ser compatível com uso em sistemas operacionais *Linux*.

1.5. ITEM 5: Emissão de Certificado digital do tipo *SSL Wildcard (OV)*

1.5.1. O certificado digital deve ser do tipo *wildcard* (sub-domínios) e permitir a sua utilização em ilimitados sub-domínios do Coren-SP (*.coren-sp.gov.br).

1.5.2. O Certificado deverá permitir uso em ilimitados servidores e serviços.

1.5.3. O Certificado deverá ser compatível com o padrão de segurança TLS versão 1.2 ou superiores.

1.5.4. O certificado digital deve possuir compatibilidade com todos os servidores e equipamentos que suportem SSL/TLS.

1.5.5. O certificado digital deve possuir validade de 12 (doze) meses após a emissão, com possibilidade de reemissão gratuita e ilimitada do certificado digital durante sua validade;

1.5.6. O Certificado deve ser emitido por Autoridade Certificadora Raiz e Intermediárias cujas cadeias de certificação já venham nativamente instaladas e confiadas no Sistema Operacional *Windows*, *Android*, *iOS*, *MacOS* e nos navegadores *Internet Explorer*, *Edge*, *Google Chrome*, *Safari*, *Opera* e *Firefox*, em suas versões *desktop* e também versões móveis. Em outras palavras, o certificado, uma vez instalado nos servidores do Coren-SP deverá permitir a navegação segura de todos os usuários dos sistemas/sites de forma transparente, sem a necessidade de intervenção manual do usuário, considerando que esse utilize um dos principais navegadores de internet (*desktop* ou móvel) citados acima.

1.5.7. O objetivo deste último requisito é facilitar o acesso do público externo aos serviços do Coren-SP, visto que não será necessário realizar instalação de certificado de AC alguma manualmente (nem raiz nem intermediária).

1.5.8. O Certificado deverá seguir os padrões x.509 v3 de acordo com o perfil definido pela RFC 5280 e RFC 3647.

1.5.9. Quando constatada emissão imprópria ou defeituosa de um certificado, o mesmo deverá ser revogado e reemitido sem ônus à Contratante.

1.5.10. Também deverá ser disponibilizada para consulta a Lista de Certificados Revogados (LCR).

1.5.11. A Autoridade Certificadora que emitir os certificados deverá disponibilizar, no regime 24x7, canal de atendimento para que a Contratante solicite, caso necessário, revogação dos certificados emitidos. Neste caso, a revogação deverá ser refletida na LCR no prazo máximo de 72 (setenta e duas) horas corridas.

1.5.12. Em caso de Revogação de certificados a Contratada deverá agir rapidamente para restabelecimento da confiança nas comunicações do Coren-SP através da emissão de novos certificados confiáveis pelos principais navegadores (*Internet Explorer*, *Edge*, *Google Chrome*, *Safari*, *Opera* e *Firefox*), inclusive suas versões móveis.

1.5.13. Requisitos de Criptografia e Chaves:

a) O referido Certificado Digital deverá possuir criptografia SHA 256bits.

b) O tamanho da chave dos Certificados deverá ser de 2048 bits se for RSA e 256bits caso seja ECC.

c) As chaves privadas do Coren-SP não poderão ser armazenadas pela Contratada, devendo essas serem de conhecimento e posse exclusiva da Contratante.

1.5.14. Requisição Mínima: 1 (uma) unidade.

1.6. ITEM 6 - Emissão de Certificado digital do tipo *SSL DV*.

1.6.1. O certificado digital deve ser do tipo *SSL DV* e permitir a sua utilização em um único domínio do Coren-SP.

1.6.2. O Certificado deverá permitir uso em ilimitados servidores e serviços.

1.6.3. Possuir alto nível de segurança e confiança, com 2048 *bits* de criptografia e 256 *bits* de assinatura ou superior;

1.6.4. O certificado digital deve possuir compatibilidade com certificado SSL.

1.6.5. O certificado digital deve possuir validade de 12 (doze) meses;

1.6.6. O Certificado deve ser emitido por Autoridade Certificadora Raiz e Intermediárias cujas cadeias de certificação já venham nativamente instaladas e confiadas no Sistema Operacional *Windows*, *Android*, *iOS*, *MacOS* e nos navegadores *Internet Explorer*, *Edge*, *Google Chrome*, *Safari*, *Opera* e *Firefox*, em suas versões *desktop* e também versões móveis. Em outras palavras, o certificado, uma vez instalado nos servidores do Coren-SP deverá permitir a navegação segura de todos os usuários dos sistemas/sites de forma transparente, sem a necessidade de intervenção manual do usuário, considerando que esse utilize um dos principais navegadores de internet (*desktop* ou móvel) citados acima.

1.6.7. O objetivo deste último requisito é facilitar o acesso do público externo aos serviços do Coren-SP, visto que não será necessário realizar instalação de certificado de AC alguma manualmente (nem raiz nem intermediária).

1.6.8. Quando constatada emissão imprópria ou defeituosa de um certificado, o mesmo deverá ser revogado e reemitido sem ônus à Contratante.

1.6.9. Também deverá ser disponibilizada para consulta a Lista de Certificados Revogados (LCR).

1.6.10. A Autoridade Certificadora que emitir os certificados deverá disponibilizar, no regime 24x7, canal de atendimento para que a Contratante solicite, caso necessário, revogação dos certificados emitidos. Neste caso, a revogação deverá ser refletida na LCR no prazo máximo de 72 (setenta e duas) horas corridas.

1.6.11. Em caso de Revogação de certificados a Contratada deverá agir rapidamente para restabelecimento da confiança nas comunicações do Coren-SP através da emissão de novos certificados confiáveis pelos principais navegadores (*Internet Explorer*, *Edge*, *Google Chrome*, *Safari*, *Opera* e *Firefox*), inclusive suas versões móveis.

1.6.12. As chaves privadas do Coren-SP não poderão ser armazenadas pela Contratada, devendo essas serem de conhecimento e posse exclusiva da Contratante.

1.6.13. Requisição Mínima: 1 (uma) unidade

2. REQUISITOS DE GARANTIA – TOKENS (itens 1 e 2)

2.1. Os *tokens* fornecidos (itens 1 e 3) deverão ser novos e de "primeiro uso", não podendo ser recondicionados.

2.2. Será exigida garantia de correção e atualização motivadas por falhas técnicas e mudanças originadas de diretrizes oriundas da ICP-Brasil, pelo período mínimo de 3 (três) anos para o certificado de pessoa física ou jurídica contados a partir da data de emissão do certificado.

2.3. Para o *token* fornecido, será exigida garantia mínima de 1 (um) ano contado do recebimento definitivo da peça.

2.4. Não estão contemplados nessa garantia os casos de roubo, perda do dispositivo e mau uso do usuário.

2.5. Caso o *token* necessite ser substituído ou apresente erro que comprometa o funcionamento do certificado ali armazenado, um novo *token* e uma nova emissão de certificado deverá ser realizada, no prazo de até 5 (cinco) dias úteis, contados da data da notificação feita pelo Coren-SP à Contratada.