TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Av. Paulista, 1842 - Bairro Bela Vista - CEP 01310-936 - São Paulo - SP - www.trf3.jus.br

ANÁLISE DA PROPOSTA Nº - CONSULTECH/2022

EMPRESA: CONSULTECH – CONSULTORIA TÉCNICA LTDA.

CNPJ: 13.102.563/0001-32

PROPOSTA : Doc. 9338328

DILIGÊNCIA: Doc. 9359330

PREGÃO ELETRÔNICO Nº 023/2022

ITEM 1		**ATENDIMENTO**	
TERMO DE REFERÊNCIA	**ESPECIFICAÇÃO**	**SIM**	**NÃO**
4 **4.1**	**REQUISITOS TÉCNICOS** **Subitem 1.1 - Certificado Digital para pessoa física do tipo A3 e-CPF**		
4.1.1	Certificado digital do tipo A3 para pessoa física, padrão ICP-Brasil, compatível com a AC-JUS, com validade de 03(três) anos;	X	

4.1.2	Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails, acesso a aplicações, logon de rede, entre outras destinações;	X	
4.1.3	Certificado aderente padrão do Comitê Gestor da ICP Brasil;	X	
4.1.4	Ser emitido em Token Criptográfico constante da lista de equipamentos certificados pelo Instituto Nacional de Tecnologia da Informação – ITI.	X	
4.2	**Subitem 1.2 – Certificado Digital em nuvem para Pessoa Física A3-e-CPF**		
4.2.1	Certificado digital do tipo A3 em nuvem para pessoa física, padrão ICP-Brasil, compatível com a AC-JUS, com prazo de validade de 3 (três) anos;	X	
4.2.2	Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails, acesso a aplicações, logon de rede, entre outras destinações;	X	
4.2.3	Gerar apenas um certificado e permitir a utilização em múltiplos dispositivos móveis a escolha do usuário;	X	
4.2.4	Mostrar histórico completo de uso, possibilitando rastrear todos os acessos feitos com o certificado;	X	
4.2.5	Validade de 3 anos com possibilidade de renovação automática, sem a necessidade de passar por todo o fluxo de autorização presencial novamente;	X	
4.2.6	Permite gerenciar os dispositivos autorizados e assinar digitalmente documentos por meio de celular ou tablet, com praticidade e mobilidade;	X	
4.2.7	Caso seja necessário qualquer aplicativo ou recurso para instalação e uso do certificado em dispositivo móvel, este deverá ser fornecido sem ônus para a Contratante.	X	

4.3	**Subitem 1.3 – Certificado Digital para Pessoa Jurídica A3 e-CNPJ**		
4.3.1	Certificado digital do tipo A3 para pessoa jurídica, emitido por autoridade certificadora credenciada pela ICP-Brasil;	X	
4.3.2	Deve ter prazo de validade de 3 (três) anos contados da emissão do certificado;	X	
4.3.3	Deve ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública no processo de certificação digital brasileira;	X	
4.3.4	Deve possuir compatibilidade com os navegadores web;	X	
4.3.5	Deve ser instalado em Token Criptográfico constante da lista de equipamentos certificados pelo Instituto Nacional de Tecnologia da Informação – ITI.	X	
4.4	**Subitem 1.4 - Certificado digital A1 e-CPF (1 ano) sem token criptográfico**		
4.4.1	Certificado digital do tipo A1 para pessoa física, padrão ICP Brasil;	X	
4.4.2	Validade de 1(um) ano contado a partir da data de sua emissão;	X	
4.4.3	A Contratada deverá ser uma Autoridade de Registro vinculada à Autoridade Certificadora, ou ela mesma ser uma Autoridade Certificadora;	X	
4.4.4	Deverá permitir a utilização para assinatura de documentos eletrônicos, e-mails, acesso a aplicações, logon de rede, entre outras destinações;	X	

4.4.5	Deverá ser gerado e armazenado diretamente no computador do usuário e permitir a exportação das chaves;	X	
4.4.6	Deverá estar em plena conformidade com os requisitos estabelecidos pelo padrão ICP-Brasil.	X	
4.5	**Subitem 1.5 - Certificado digital A1 e-CNPJ (1 ano) sem token criptográfico**		
4.5.1	Certificado Digital A1 e-CNPJ, padrão ICP-Brasil, com validade de 1(um) ano;	X	
4.5.2	Certificado A1 com chave armazenada em um PKCS#12 (.p12), emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil;	X	
4.5.3	Possuir validade de 1 ano a partir da data de emissão do certificado;	X	
4.5.4	Deverá permitir a realização de assinatura digital utilizando um subconjunto do padrão de assinatura XML, definido pelo padrão contido em http://www.w3.org/TR/xmldsig-core;	X	
4.5.5	Deverá permitir a validação correta da assinatura digital, através da canonicalização do XML enviado, soba as transformações Enveloped e C14N, conforme documentações disponíveis nos links http://www.w3.org/2000/09/xmldsig#enveloped-signature e http://www.w3.org/TR/2001/REC-xml-c14n-20010315, respectivamente;	X	
4.5.6	Utilizar chaves criptográficas assimétricas RSA de, no mínimo, 2048 bits;	X	
4.5.7	Utilizar, no mínimo, função de Message Digest SHA-256;	X	

4.5.8	Permitir estabelecimento de sessões SSL (Security Socket Layer) e TLS (Transport Layer Security);	X	
4.5.9	A cadeia de certificação precisa ser EndCertOnly, onde estará incluso na assinatura apenas o certificado do usuário final;	X	
4.5.10	Permitir a geração de CMS (PKCS#7) assinado com ao menos algoritmos sha1withRSA e sha256withRSA.	X	
4.6	**Subitem 1.6 - Certificado digital para equipamento de rede (wildcard)**		
4.6.1	Certificado digital para servidor, do tipo SSL, com prazo de validade de 1 (um) ano;	X	
4.6.2	Emissão do certificado em até 3 dias úteis a contar da data de solicitação;	X	
4.6.3	Certificado digital para equipamento servidor, do tipo SSL WildCard, permitindo sua utilização em ilimitados subdomínios, um nível, do domínio para o qual foi emitido;	X	
4.6.4	Permitir criptografia de no mínimo 256 bits;	X	
4.6.5	Possuir chave RSA de no mínimo 2048 bits;	X	
4.6.6	Deverá ser baseado em SSL/TLS (Secure Sockets Layer/Transport Layer Security) e possibilitar a instalação em ilimitados servidores sem custo adicional;	X	
4.6.7	Após receber a Ordem de Serviço para a emissão de certificados digitais, a Contratada deverá informar o rol de	X	

	documentos necessários para a emissão;		
4.6.8	A Contratada deverá entrar em contato com o representante do Contratante para concluir a emissão do certificado ou solicitar complementação documental, se for o caso, quando não for possível a emissão imediata da identidade digital;	X	
4.6.9	A Contratada deverá disponibilizar suporte remoto via chat, e-mail ou website para prestação de esclarecimentos e dúvidas técnicas e cadastrais;	X	
4.6.10	O representante técnico do Contratante autorizado previamente a solicitar o certificado atestará a emissão do certificado na Ordem de Serviço;	X	
4.6.11	A emissão do Certificado Digital SSL Wildcard ocorrerá na Av. Paulista, 1.842, Torre Norte - 19º andar - Bela Vista - São Paulo/SP;	X	
4.6.12	O presente item engloba o respectivo serviço de autoridade de registro.	X	
4.7	**Token criptográfico**		
4.7.1	Token criptográfico USB capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil;	X	
4.7.2	Fazer parte da lista de equipamentos certificados pelo Instituto Nacional de Tecnologia da Informação – ITI; http://www.inmetro.gov.br/prodcert/certificados/lista.asp: Equipamentos de certificação digital padrão ICP-Brasil - PT INMETRO N° 8/2013;	X	
4.7.3	Total compatibilidade com os certificados digitais A3;	X	

4.7.4	Possuir conector USB (Universal Serial Bus) tipo A versão 2.0 (ou superior compatível com 2.0);	X	
4.7.5	Permitir conexão direta na porta USB, sem necessidade de interface intermediária para leitura;	X	
4.7.6	Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 64 KBytes;	X	
4.7.7	Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 2048 bits;	X	
4.7.8	Possuir carcaça resistente à água e à violação;	X	
4.7.9	Compatibilidade e disponibilização de drivers para pleno uso nas plataformas Microsoft Windows 10 e superior, Linux e Mac OS;	X	
4.7.10	Permitir a criação de senha de acesso ao dispositivo obrigatoriamente com 06 (seis) caracteres, no mínimo, ou de acordo com os critérios da JF3R;	X	
4.7.11	Permitir criação de senhas com caracteres alfanuméricos;	X	
4.7.12	Permitir a geração de chaves, protegidas por PINs (Personal Identification Number);	X	
4.7.13	Permitir a inicialização e reinicialização do token mediante a utilização de PUK (Pin Unlock Key);	X	
4.7.14	Suporte aos principais navegadores de mercado, entre os quais: Internet Explorer, Microsoft Edge, Mozilla Firefox e Google Chrome;	X	

4.7.15	O software de gerenciamento do dispositivo deverá estar no idioma português do Brasil e deve permitir;	X	
4.7.15.1	Gerenciamento do dispositivo;	X	
4.7.15.2	Exportação de certificados armazenados no dispositivo;	X	
4.7.15.3	Importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;	X	
4.7.15.4	Importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;		
4.7.15.5	Visualização de certificados armazenados no dispositivo;	X	
4.7.15.6	Remoção de chaves e outros dados contidos no dispositivo após autenticação do titular;	X	
4.7.15.7	Reutilização de dispositivos bloqueados, por meio de remoção total dos dados armazenados e geração de nova senha de acesso;	X	
4.7.16	Possuir memória mínima de 72k.	X	
7.28.2.1 do Edital	Deverão ser atendidos também os subitens 6.2.2.1 e 6.2.3 do Termo de Referência (Anexo I deste Edital).		
6.2.2.1	Documento(s) contendo a(s) especificação(ões) técnica(s) detalhada(s) do(s) certificado(s) cotado(s), em língua portuguesa.		

6.2.3	Todas as características técnicas obrigatórias deverão ser comprovadas por meio de folders, ou catálogos, ou manuais, ou impressão de páginas do fornecedor na Internet.		

PARECER: Após análise do Registro de Diligência 1 - Consultech verificamos que não há informação a respeito do item 4.7.15.4 para comprovar se atende ao solicitado. Solicitamos que seja feita nova diligência.

Documento assinado eletronicamente por **Ines De Fatima Figueiredo Lopes**, **Diretora de Atendimento a Usuários**, em 16/12/2022, às 18:56, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Flavio de Souza Oliveira**, **Diretor da Divisão de Aquisições e Acompanhamentos de Contratos**, em 17/12/2022, às 11:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antonio Augusto Bueno Costa**, **Técnico Judiciário**, em 19/12/2022, às 10:05, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **9359350** e o código CRC **A15AD7DD**.