Tribunal Regional Eleitoral do Estado de São Paulo
ESTUDO TÉCNICO PRELIMINAR

Modelo v. 4.0

SEI nº 0036290-67.2025.6.26.8000

Certificados Digitais

São Paulo, data da assinatura eletrônica

ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO

Este Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de aquisição. Refere-se à aquisição por Dispensa de certificados digitais e-CPF, CERT-JUS Institucional para servidores e magistrados do TRE-SP tipo A3, incluindo o fornecimento de ***TOKEN*** criptográfico USB para armazenamento, de acordo com a demanda do TRE-SP.

1. IDENTIFICAÇÃO

Aquisição de 90 (noventa) certificados digitais para pessoa física, e-CPF, padrão ICP-Brasil tipo A3, CERT-JUS Institucional, incluindo o fornecimento dos respectivos ***TOKENS*** USB para armazenamento com validade de 36 (trinta e seis) meses.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. Identificação das necessidades de negócio

A **Resolução CNJ de Nº 185/2013** (que institui o Sistema Processo Judicial Eletrônico PJe como sistema de processamento de informações e prática de atos processuais) estabelece em seu Art. 27º, §2º: que "*Os sítios eletrônicos do PJe dos Conselhos e dos Tribunais deverão ser acessíveis somente por meio de conexão segura HTTPS, e os servidores de rede* ***deverão possuir certificados digitais Equipamento Servidor da ICP-Brasil*** *adequados para essa finalidade*".

Assim, torna-se necessária a contratação de certificados digitais e-CPF, padrão ICP-Brasil tipo A3, CERT-JUS Institucional, padrão ICP-Brasil tipo A3 com mídia criptográfica do tipo TOKEN, pelo TRE-SP para garantir a segurança das informações trafegadas por meio dos acessos realizados às aplicações e serviços disponibilizados que exijam o uso dessa tecnologia, como por exemplo o Processo Judicial Eletrônico, implantado no TRE-SP em julho de 2017.

2.2. Identificação das necessidades tecnológicas

- **Certificado digital para magistrados e servidores do Poder Judiciário do tipo A3, CERT-JUS Institucional, com mídia criptográfica do tipo TOKEN e validade de 36 (trinta e seis) meses:**
    - Certificado digital do tipo A3, CERT-JUS Institucional, aderente ao padrão ICP-Brasil com prazo de validade de 36 (trinta e seis) meses;
    - Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails, acesso a aplicações, logon de rede, entre outras funções;
    - O presente item engloba o respectivo serviço de autoridade de registro conforme determina a ICP-Brasil;
    - Certificado aderente padrão do Comitê Gestor da ICP Brasil;
    - Garantia de correção e atualização motivadas por falhas técnicas e mudanças originadas de diretrizes oriundas da ICP-Brasil, pelo

período mínimo de 36 (trinta e seis) meses para o certificado, contados a partir da data de emissão do certificado;
- Emissão e gravação compatíveis com qualquer mídia criptográfica homologada pelo ITI – Instituto Nacional de Tecnologia da Informação ou certificada pelo Inmetro;
- Os certificados digitais poderão ser emitidos nos postos de atendimento da CONTRATADA, ou ainda de forma online, a critério do CONTRATANTE;

2.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

A contratação de certificados digitais e-CPF CERT-JUS Institucional, padrão ICP-Brasil tipo A3, com mídia criptográfica do tipo TOKEN, é indispensável para a segurança, autenticidade e integridade das informações e atos praticados no ambiente digital do Tribunal Regional Eleitoral do Estado de São Paulo (TRE-SP). Esses certificados são cruciais para o acesso ou continuidade de acesso dos servidores aos sistemas que exigem tal certificação, como RENAJUD, INFOJUD (da Receita Federal), PJE e Compras.gov.br.

A necessidade do uso de certificados digitais no Poder Judiciário é amplamente respaldada por uma sólida base legal. A Lei nº 14.063/2020 regulamenta o uso de assinaturas eletrônicas em interações com entes públicos. A informatização do processo judicial é regida pela Lei nº 11.419/2006. Normativos do Conselho Nacional de Justiça (CNJ) complementam essa exigência: a Resolução CNJ nº 185/2013 instituiu o Processo Judicial Eletrônico (PJe), enquanto a Resolução CNJ nº 420/2021 trata da adoção e planejamento da digitalização do acervo processual físico. Além disso, a Resolução CNJ nº 522/2023 estabelece o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário. Internamente, a Instrução Normativa nº 14/2022 do TSE já determina a assinatura digital baseada em certificado digital ICP-Brasil.

Priorizando a eficiência e a modernização, a contratação prevê a emissão dos certificados digitais de forma online. De acordo com a Instrução Normativa ITI Nº 05 de 22 de fevereiro de 2021, que permite a emissão de certificados por videoconferência, a empresa contratada deverá, preferencialmente, prover a emissão do e-CPF online. Após a emissão remota, a empresa será responsável pelo envio dos tokens para a residência de cada servidor, sem ônus adicionais para a Administração.

Nos casos em que a emissão *online* não for viável, seja por falta de documentos exigidos pela IN ITI Nº 05, seja por opção da contratante, a validação e emissão dos certificados ocorrerão em escritórios autorizados (AR) indicados pela empresa contratada.

Processos anteriores de aquisição de certificados:
- Instaurado para aquisição em 2020 para a Secretaria: 0002443-50.2020.6.26.8000
- Instaurado para aquisição em 2021 para a Secretaria: 0008665-97.2021.6.26.8000
- Instaurado para aquisição em 2022 / 2023 para a Secretaria e Cartórios: 0038551-44.2021.6.26.8000
- Instaurado para aquisição em 2024 / 2025 para Secretaria e Cartórios (TRE-BA): 0016564-44.2024.6.26.8000 e 0043986-91.2024.6.26.8000

Qualificação técnica

A inclusão das exigências de qualificação técnica (no Termo de Referência) é fundamental e compulsória para garantir a segurança, a conformidade legal e a capacidade operacional da futura contratada, dada a natureza de fé pública e a criticidade dos certificados digitais utilizados na Justiça Eleitoral.

a. Obrigatoriedade Legal e Segurança Institucional

A exigência de que a licitante seja uma Autoridade de Registro (AR) vinculada a uma Autoridade Certificadora (AC) habilitada na cadeia AC-JUS é a principal condição de habilitação e se justifica pela:

- **Determinação do TSE:** O Tribunal Superior Eleitoral (TSE) recomenda que a emissão de novos certificados digitais para os usuários da Justiça Eleitoral seja feita apenas utilizando a cadeia de certificação da AC-JUS.
- **Segurança Comprovada:** A obrigatoriedade se baseia na constatação do ITI/PR de que a AC-JUS, durante seus mais de 18 anos de operação, jamais registrou um evento de segurança relacionado a fraude na emissão de certificados.
- **Conformidade com o Judiciário:** A AC-JUS foi criada pelo Conselho da Justiça Federal (CJF) para definir regras e perfis de certificados específicos para aplicações do Judiciário , sendo a estrutura que viabilizou o advento do Processo Judicial Eletrônico (PJe) com validade legal.
- **Integração do Órgão:** O próprio TSE é membro integrante do Comitê Gestor da AC-JUS, o que torna mandatória a utilização dessa cadeia de confiança.
- **Não Redução da Concorrência:** A exigência não impacta a competição, pois existem seis Autoridades Certificadoras (AC CERTISIGN JUS, AC SAFEWEB JUS, AC SERASA JUS, AC SERPRO JUS, AC SOLUTI JUS e AC VALID JUS) capazes de emitir certificados JUS e que possuem Autoridades de Registro (ARs) em todo o território nacional.

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

A presente contratação visa atender à demanda imediata e reprimida por certificados digitais de 192 certificados, assegurando a continuidade das atividades essenciais e o acesso aos sistemas judiciais pelos servidores do TRE-SP.

4. ANÁLISE DE SOLUÇÕES POSSÍVEIS

4.1. IDENTIFICAÇÃO DAS SOLUÇÕES

Dentre as soluções que dispõe de dispositivos criptográficos para armazenamento do certificado digital, temos as 2 (duas) seguintes soluções possíveis:

Id	Descrição da solução (ou cenário)
1	Certificado digital do tipo A3, padrão ICP Brasil, com fornecimento de leitor e cartão criptográfico - ***SMART CARD*** para armazenamento do certificado, com validade por 36 (trinta e seis) meses;
2	Certificado digital do tipo A3, padrão ICP Brasil, com fornecimento de **TOKEN** criptográfico para armazenamento do certificado, com validade por 36 (trinta e seis) meses;

4.2. ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X		
	Solução 2	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X		
	Solução 2	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

A solução proposta envolve a contratação de serviços que incluem a emissão de certificados digitais de tipo A3, CERT-JUS Institucional para servidores e magistrados do TRE-SP. Esta solução deve estar alinhada com os padrões da ICP-Brasil e ter validade de 36 (trinta e seis) meses.

Importante salientar que o presente estudo não considera adquirir os certificados separadamente dos dispositivos físicos, pois seriam necessários dois processos de estudo de viabilidade, o que aumentaria os custos administrativos. Além disso, sincronizar os contratos para os serviços e os dispositivos físicos é essencial para evitar custos adicionais durante a execução.

Outro ponto a ser considerado é que o padrão criptográfico dos certificados digitais pode não ser compatível com todos os dispositivos físicos de armazenamento disponíveis no mercado. Isso poderia inviabilizar o uso desses dispositivos ao longo da vigência do contrato.

Existem diferentes cenários possíveis para oferecer essa solução, incluindo o uso de token criptográfico ou *smart card* como dispositivo de armazenamento. No entanto, a certificação digital em nuvem não é viável para a instituição devido a questões técnicas específicas:

- **Dependência de conectividade constante e estável**

  A utilização de certificados digitais em nuvem exige uma conexão contínua e estável com a internet para qualquer operação que demande a assinatura ou autenticação digital. No contexto deste Tribunal Regional Eleitoral, onde a disponibilidade e a agilidade são cruciais, especialmente em períodos eleitorais ou para o acesso a sistemas judiciais eletrônicos, qualquer interrupção na conexão à internet pode inviabilizar o uso do certificado. Mesmo com a infraestrutura de rede robusta que possuímos, não estamos imunes a falhas de conectividade que poderiam comprometer a continuidade dos trabalhos.

- **Desempenho e latência**

  O desempenho do certificado digital em nuvem é intrinsecamente ligado à latência da conexão. Assinaturas digitais em larga escala ou operações que demandem múltiplas autenticações podem ser impactadas por atrasos, mesmo que mínimos, na comunicação com os servidores da nuvem. Para sistemas críticos e com alto volume de transações, como os utilizados no processo eleitoral ou em tramitações processuais, essa latência pode gerar gargalos e lentidão, prejudicando a eficiência das atividades e a experiência do usuário.

- **Controles de Segurança e Auditoria**

  Embora os provedores de serviços de nuvem ofereçam robustas camadas de segurança, a gestão das chaves privadas em ambiente externo ao controle direto do Tribunal representa um desafio. A rastreabilidade e a auditoria de cada uso do certificado em nuvem podem ser mais complexas de serem integradas aos nossos sistemas de log e monitoramento internos. A necessidade de garantir a integridade e a não-repúdio das assinaturas, em conformidade com as exigências da legislação eleitoral e das normas de segurança da informação, impõe a preferência por soluções em que o controle sobre a chave privada permaneça sob a gestão do TRE-SP, como ocorre com os tokens criptográficos.

- **Conformidade Regulatória e Soberania dos Dados**

  A legislação brasileira, especialmente no âmbito da Justiça Eleitoral, possui requisitos rigorosos quanto à soberania dos dados e à localização do armazenamento de informações sensíveis. Embora os provedores de nuvem possam oferecer datacenters no Brasil, a gestão das chaves criptográficas por terceiros e a interconexão com infraestruturas fora do controle direto do TRE-SP podem levantar questionamentos quanto à plena conformidade com as normas regulatórias e à garantia da independência de acesso e controle. A opção por tokens criptográficos, onde a chave privada está sob o controle físico do usuário no ambiente do Tribunal, oferece uma maior garantia nesse aspecto.

A opção pelo token oferece maior segurança por ser uma mídia criptográfica dedicada, gerando e armazenando as chaves privadas de forma inviolável. Essa segurança é um requisito indispensável para garantir a validade jurídica das assinaturas eletrônicas e a conformidade com as diretrizes da ICP-Brasil.

Em segundo lugar, a escolha atende às necessidades operacionais e de praticidade do Tribunal. Os servidores do TRE-SP já estão familiarizados com o uso de tokens, e o Tribunal já possui a infraestrutura necessária para sua instalação nas máquinas, dispensando adaptações. Além disso, o tamanho reduzido e a facilidade de transporte

do token se mostram mais práticos em comparação ao *smart card*, que exige uma leitora, tornando-o menos portátil.

Esses fatores, somados à sua maior mobilidade, justificam a decisão por essa mídia criptográfica, assegurando uma solução que não apenas atende aos requisitos técnicos e de segurança, mas também se alinha à realidade operacional da instituição.

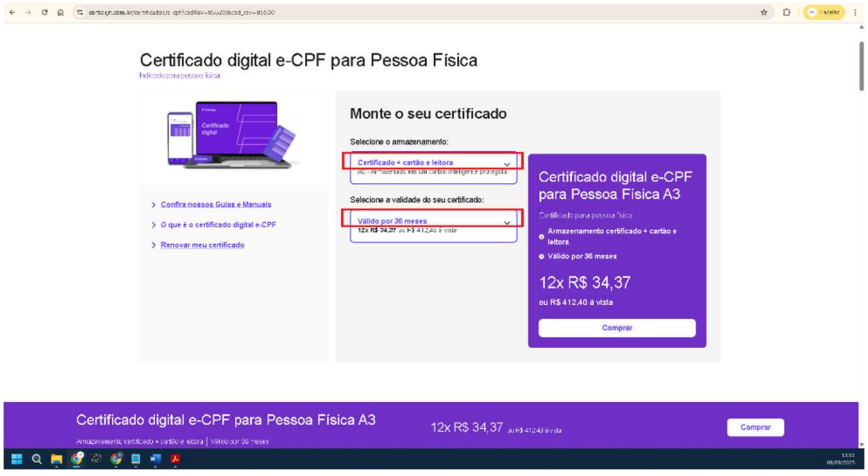
4.3. PESQUISA DE PREÇOS DE MERCADO

4.3.1. eCPF

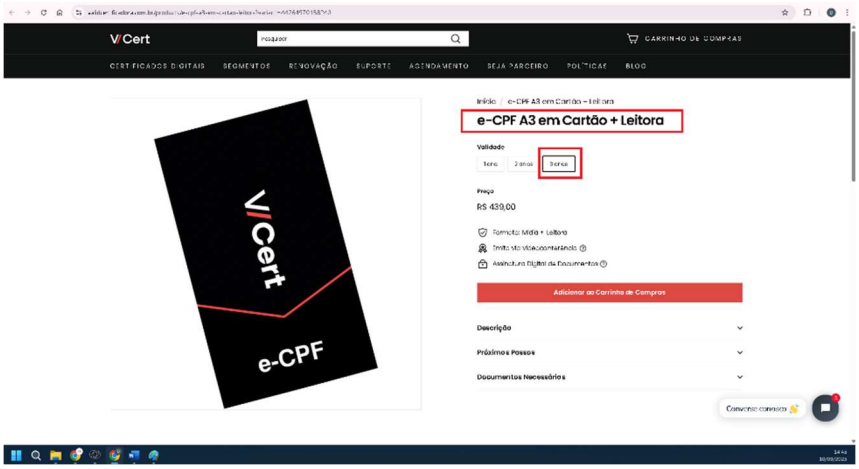
- Certificado Digital e-CPF (pessoa física) com dispositivo criptográfico tipo ***Token*** (A3), com validade de 36 (trinta e seis) meses;
- Certificado Digital e-CPF (pessoa física) com dispositivo criptográfico tipo ***SMART CARD + Leitor*** (A3), com validade de 36 (trinta e seis) meses;

Id	Descrição da solução (ou cenário)	Custo Unitário R$
1	Certificado Digital – tipo A3 com mídia criptográfica do tipo ***SMART CARD*** + **Leitor** – com validade de 36 meses – **Certisign**	412,40
2	Certificado Digital – tipo A3 com mídia criptográfica do tipo ***TOKEN*** – com validade de 36 meses – **Certisign**	412,40
3	Certificado Digital – tipo A3 com mídia criptográfica do tipo ***SMART CARD + Leitor*** – com validade de 36 meses – **VALID**	439,00
4	Certificado Digital – tipo A3 com mídia criptográfica do tipo ***TOKEN*** – com validade de 36 meses – **VALID**	439,00
	Valor médio	**R$ 425,70**

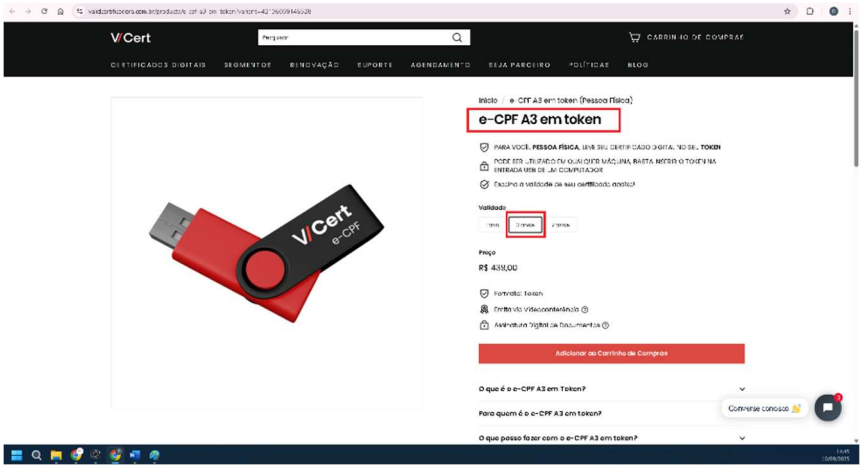
Quadro 1: Pesquisa de preços das 2 soluções viáveis de diferentes fornecedores na internet



https://certisign.com.br/certificados/e-cpf



https://validcertificadora.com.br/products/e-cpf-a3-em-cartao-leitora



https://validcertificadora.com.br/products/e-cpf-a3-em-token?variant=42136009146528

Quadro 2: Pesquisa de preços das 2 soluções viáveis de diferentes fornecedores na internet

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

a. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução Viável 1

Custo Total de Propriedade – Memória de Cálculo

Quantidade	Item	Custo médio unitário	Custo médio total
90	Certificados digitais do tipo A3 de **Pessoa Física** com dispositivo criptográfico - **TOKEN** para armazenamento.	R$ 425,70	R$ 38.313,00
Total			**R$ 38.313,00**

b. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 2026	Ano 2027	Ano 2028	
Solução viável	**R$ 38.313,00**	R$ 0	R$ 0	R$ 38.313,00

6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Apesar de 2 (duas) soluções se mostrarem viáveis, tanto do ponto de vista tecnológico quanto econômico, a escolha da solução que fornece o **TOKEN criptográfico** para armazenamento do certificado justifica-se por 2 (dois) aspectos mais relevantes que trazem vantagens do ponto de vista operacional: os servidores do TRE-SP já estão habituados a utilizar o TOKEN e o TRE-SP já conta com a infraestrutura necessária ao seu funcionamento disponível para instalação nas máquinas, sem a necessidade de adaptação; outro aspecto considerado como favorável diz respeito ao ponto de vista da praticidade, o TOKEN tem um tamanho reduzido e bastante fácil de guardar em qualquer lugar, já o cartão – SMART CARD necessita sempre estar associado à leitora, que é grande e pouco prática para transportar.

Para a presente contratação, não há indicação direta de marcas ou modelos específicos de Autoridades Certificadoras (ACs) ou de dispositivos criptográficos (tokens).

No entanto, a fim de garantir a segurança, a interoperabilidade e a conformidade legal necessárias às operações do Tribunal Regional Eleitoral do Estado de São Paulo, são indispensáveis as seguintes especificações técnicas mínimas, que, por sua natureza, direcionam a solução para padrões de mercado reconhecidos e homologados pelos órgãos reguladores:

Certificado Digital:

- **Padrão ICP-Brasil:** O certificado digital deve ser emitido por Autoridade Certificadora devidamente credenciada na ICP-Brasil, em conformidade com a Medida Provisória nº 2.200-2/2001 e suas regulamentações.
- **Tipo A3:** Exige-se que o certificado seja do tipo A3 (com chaves armazenadas em dispositivo criptográfico inviolável).
- **Perfil CERT-JUS Institucional (e-CPF):** O certificado deve possuir o perfil e-CPF, com o atributo específico "CERT-JUS Institucional", conforme as normas da ICP-Brasil para a Justiça, garantindo a interoperabilidade com os sistemas do Poder Judiciário.
- **Validade:** O certificado deve possuir validade mínima de 36 (trinta e seis) meses.

Mídia Criptográfica (Token):

- **Padrão:** O token criptográfico deve ser compatível com as especificações da ICP-Brasil para certificados A3.
- **Hardware Criptográfico:** Deve possuir hardware criptográfico dedicado, capaz de gerar e armazenar as chaves privadas de forma segura e inviolável, atendendo aos requisitos da ISO/IEC 15408 (Common Criteria) EAL4+ ou superior.
- **Drivers e Compatibilidade:** Deve ser compatível com os sistemas operacionais e navegadores de internet amplamente utilizados no TRE-SP (Windows 10/11, navegadores Chrome, Firefox, Edge) e com os principais softwares de assinatura e sistemas eletrônicos do Poder Judiciário (PJe, SEI, etc.), com drivers disponíveis e de fácil instalação.
- **Padrão PKCS#11 e CSP/KSP:** Deve ser compatível com os padrões PKCS#11 e interfaces de provedor de serviços criptográficos (CSP/KSP) do Windows, garantindo a interoperabilidade com as aplicações.

A adoção dessas especificações técnicas é justificada pela necessidade imperativa de garantir a segurança da informação, a validade jurídica das assinaturas eletrônicas, a interoperabilidade com os sistemas do Poder Judiciário e a conformidade com as diretrizes da ICP-Brasil e da legislação pertinente. Tais requisitos não buscam restringir a competitividade, mas sim assegurar que a solução contratada atenda plenamente às necessidades críticas e aos padrões regulatórios do Tribunal Regional Eleitoral do Estado de São Paulo.

Critérios de Sustentabilidade

Considerando a natureza digital dos certificados não foram encontrados critérios de sustentabilidade aplicáveis à contratação em pauta.

6.1. ANÁLISE DE PARCELAMENTO OU NÃO DO OBJETO

Em conformidade com o disposto no artigo 40, § 3º,"I", da Lei nº 14.133/2021, que estabelece a excepcionalidade do julgamento por grupo de itens, e considerando a intrínseca relação entre a emissão do certificado digital (e-CPF) e o fornecimento do dispositivo criptográfico (token USB), este Estudo Técnico Preliminar fundamenta a não viabilidade do parcelamento do objeto. A contratação em item único é a abordagem mais vantajosa para o TRE-SP, uma vez que garante a padronização tecnológica dos certificados e dos tokens, a interoperabilidade plena com os sistemas eletrônicos do Poder Judiciário (como o PJe e o SEI), e a responsabilidade única pelo ciclo completo de vida do certificado – desde a emissão e entrega do hardware até o suporte e a garantia. O parcelamento em itens distintos se torna inviável técnica e economicamente, pois resultaria em múltiplos fornecedores, com riscos de incompatibilidade entre certificados e tokens de diferentes fabricantes, diluição da responsabilidade pela funcionalidade integrada da solução, fragmentação do suporte técnico, e custos de gestão contratual mais elevados, o que comprometeria a eficiência operacional e a segurança da informação deste Tribunal. A unificação do objeto visa, portanto, a otimização técnica, econômica e administrativa da contratação.

6.2. SUPORTE TÉCNICO E GARANTIA

A CONTRATADA será responsável por prover suporte técnico especializado para os certificados digitais e os tokens criptográficos durante todo o período de validade do certificado. O suporte deve cobrir questões relacionadas à instalação, configuração, uso e resolução de problemas técnicos.
Além disso, a contratada deverá oferecer garantia de 36 (trinta e seis) meses para os certificados e dispositivos criptográficos. A garantia deve incluir a correção de falhas técnicas e a atualização motivada por mudanças nas diretrizes oriundas da ICP-Brasil, contadas a partir da data de emissão de cada certificado. Durante o período de garantia a contratada deverá realizar a substituição sem ônus adicionais para o TRE-SP, caso o certificado ou o token apresentem defeitos ou falhas, que não se enquadrem em mau uso, roubo ou furto.

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Estima-se:

Quantidade	Serviço	Custo médio unitário	Custo médio total
90	Certificados digitais do tipo A3 de Pessoa Física com dispositivo criptográfico do tipo "TOKEN" para armazenamento.	R$ 425,70	R$ 38.313,00
Total			R$ 38.313,00

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declaramos que a contratação da solução Certificados digitais do tipo A3, CERT-JUS Institucional de Pessoa Física com Token criptográfico para armazenamento, validade por 36 (trinta e seis) meses é viável, tendo sido escolhida por se adequar às necessidades já utilizadas por este Tribunal, bem como por se mostrar mais prática, trazendo os seguintes benefícios:

- Possibilidade de acesso aos sistemas do Governo Federal;
- Aumento na segurança da informação.

9. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pelo Documento de Oficialização da Demanda (doc. nº) de de de 2025.

INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO	INTEGRANTE ADMINISTRATIVO
Daniele de Macedo Braga **Matrícula: 13.565-8**	Aline Cristina Gomes dos Santos Gadret **Matrícula:** xxxxxx	**Matrícula:** xxxxxx

São Paulo, data da assinatura eletrônica	São Paulo, data da assinatura eletrônica	São Paulo, data da assinatura eletrônica

SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO, representando o CETIC
_____ Daniel Forlivesi **Matrícula:xxxxxx** São Paulo, data da assinatura eletrônica

ÁREA DEMANDANTE
_____ Alessander Augusto Cristino Costa **Matrícula: xxxxxx** São Paulo, data da assinatura eletrônica