ESTUDO TÉCNICO PRELIMINAR

Contratação de empresa especializada na prestação de serviços de solução de plataforma de assinatura e validação de assinatura digital com serviços de manutenção, suporte e atualização tecnológica a serem realizados no curso de tempo definido em contrato.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

PORTARIA N° 156/2026

INTEGRANTE	UNIDADE	NOME	MATRÍCULA
Requisitante	DTI	Wellington Glass da Silva	516015
Lider Técnico	DTI	Leonardo Luiz Cruz Bucher	526860
Técnico	DTI	Luciano Drosda Marques dos Santos	526770
Técnico	DTI	Pedro Emanuel Costa Vaz	515639
Administrativo	DA/SLC	Gustavo Ribeiro Dortas	521175

SUMÁRIO

1 INTRODUÇÃO 5
1.1 Objetivo do Estudo Técnico Preliminar e contextualização do objeto. 5
2 DESCRIÇÃO DA NECESSIDADE 5
2.1 Caracterização do problema a ser resolvido sob a perspectiva do interesse público. 5
2.2 Como o TCE-PR vai alcançar maior eficiência com a solução demandada. 6
3 RESULTADOS A SEREM ALCANÇADOS 7
3.1 Demonstração dos benefícios esperados, ganhos de eficiência, continuidade, qualidade ou economicidade. 7
4 ALINHAMENTO ESTRATÉGICO 8
5 ANÁLISE DA SITUAÇÃO ATUAL 9
6 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO E REQUISITOS 9
6.1 Requisitos de Negócio 9
6.1.1 Assinatura Digital de Documentos 10
6.1.2 Validação de Documentos Digitais 10
6.1.3 Assinatura Individual e em Lote de Documentos 10
6.1.4 Integração com os Sistemas Corporativos do Tribunal 10
6.1.5 Manutenção, Suporte e Atualização Tecnológica 11
6.1.6 Evolução Funcional da Solução 11
6.2 Requisitos Técnicos 11
6.3 Requisitos operacionais e de implantação 12
6.4 Monitoramento 14
6.5 Qualidade, Metodologias e Padrões 14
6.6 Pagamento 14
6.7 Implantação 15
6.8 Componentes Tecnológicos 15
6.9 Legais, de Segurança e Privacidade 16
6.10 Propriedade Intelectual 17
6.11 Sociais, Ambientais e Culturais 17
7 IDENTIFICAÇÃO E ANÁLISE DE SOLUÇÕES 18
7.1 Introdução 18
8 LEVANTAMENTO DE ALTERNATIVAS 19
8.1 Cenário A1: Desenvolvimento de software assinador de documentos digitais pelo TCE-PR: 19
8.2 Cenário A2: Aquisição de Solução de Assinatura Implantada e Operada no Ambiente do TCE PR: 20
8.3 Cenário A3: Aquisição de Solução de Assinatura Implantada e Operada em Ambiente Externo 20
9 ESTIMATIVA DAS QUANTIDADES 21
10 ESTIMATIVA PRELIMINAR DE PREÇOS 23
11 JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA 25
12 BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO 26
12.1 Bens e serviços que compõe a solução 26
12.2 Vigência do contrato 27
12.3 Qualificação técnica do fornecedor 27
12.4 Parcelamento do Objeto 29
12.5 Da Aceitação ou Não de Consórcio e Cooperativas 29
12.6 Subcontratação e Alteração Subjetiva 30
13 INSTRUMENTO DE MEDIÇÃO DE RESULTADO (IMR) E NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) 30

14 INTERDEPENDÊNCIA COM OUTRAS CONTRATAÇÕES 31
14.1 Relação com o Contrato n.º 07/2026 (Desenvolvimento de Software): 31
14.2 Relação com o Contrato n.º 02/2026 (Certificados Digitais): 31
14.3 Relação com o Contrato n.º 36/2024 (Novo Trâmite): 31
14.4 Relação com o Contrato n.º 15/2024 (Sustentação de Software): 32
15 NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL 32
16 ESTRATÉGIA DE CONTINUIDADE EM CASO DE INTERRUPÇÃO CONTRATUAL 33
17 IMPACTOS AMBIENTAIS E MEDIDAS MITIGADORAS 34
18 DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO 35
19 APÊNDICE A - DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA SOLUÇÃO 35
19.1 REQUISITOS TÉCNICOS 35
19.2 Requisitos genéricos da solução 36
19.3 FADD – Requisitos da Funcionalidade de Assinatura Digital de Documentos 37
19.4 FVAAD – Requisitos da Funcionalidade de Validação E VERIFICAÇÃO de Assinatura Digital de Documentos 40
19.5 FVCD – Requisitos da Funcionalidade de Validação E VERIFICAÇÃO DE CERTIFICADO DIGITAL 42
19.6 FGLCR – Requisitos da Funcionalidade de Gerenciamento de Lista de Certificados Revogados 43
19.7 FCT – Requisitos da Funcionalidade de Carimbo de Tempo 44
19.8 FLAPI – Requisitos da APIs para a Execução dos Serviços Descritos nos Requisitos 4.2.1 a 4.2.6 44
19.9 FLSAW – Requisitos da Licença de Software para Execução de Assinaturas Digitais Via Navegadores Web (plugin) 46
19.10 FLSA1 – Requisitos da Licença de Componente para Execução, no Servidor de Aplicações, de Assinaturas Digitais com Suporte a Certificados A1 48
19.11 Requisitos temporais 48
19.12 Requisitos de capacitação e transferência de conhecimento 48
19.13 Requisitos de segurança 49
19.14 Requisitos de monitoramento 49
19.15 Requisitos de sustentabilidade 50
19.16 Requisitos de qualidade 50
19.17 Requisitos de implantação 51
20 APÊNDICE B - ESPECIFICAÇÃO DO SERVIÇO DE ADAPTAÇÃO PARA INTEGRAÇÃO DAS APLICAÇÕES DO TCE-PR 53
20.1 Introdução 53
20.2 Interfaces Do Assinador 53
20.3 Fluxo da assinatura 55
20.4 Fluxo da Coassinatura 57
20.5 Fluxo de assinatura com certificado em nuvem 58
20.6 Fluxo da validação de assinatura 59
20.7 Fluxo da assinatura no servidor 60
20.8 Dicionário de Dados 61
Requisito 8, Etapa 1: Gerar Hash para assinatura 61
Requisito 8, Etapa 3: FinalizarAssinatura 63
Validar Assinatura 65
20.9 Exemplo de Estrutura de Dados 75

1 INTRODUÇÃO

1.1 Objetivo do Estudo Técnico Preliminar e contextualização do objeto.

O presente Estudo Técnico Preliminar (ETP) tem por objetivo subsidiar o planejamento da contratação de solução de plataforma de assinatura digital, a ser utilizada pelo Tribunal de Contas do Estado do Paraná (TCE-PR) no suporte às suas atividades institucionais e administrativas, especialmente aquelas relacionadas ao processo eletrônico, à formalização de atos, documentos e manifestações com validade jurídica.

A solução de assinatura digital constitui elemento essencial da infraestrutura tecnológica do Tribunal, sendo amplamente utilizada por diversos sistemas corporativos para garantir os requisitos de autenticidade, integridade, não repúdio e temporalidade dos documentos eletrônicos produzidos ou tramitados no âmbito do TCE-PR. Trata-se, portanto, de serviço crítico, cuja indisponibilidade ou inadequação impacta diretamente a continuidade das atividades finalísticas da Corte de Contas.

O TCE-PR possui, atualmente, solução de assinatura digital contratada, cujo prazo de vigência é improrrogável, o que impõe a necessidade de planejamento antecipado para a realização de nova contratação, de modo a assegurar a continuidade dos serviços, mitigar riscos operacionais e evitar descontinuidade dos serviços.

Além da necessidade de substituição contratual, verifica-se que o cenário tecnológico e normativo relacionado à assinatura digital evoluiu significativamente nos últimos anos, com o amadurecimento de soluções baseadas em "*Application Programming Interfaces*" (APIs), maior demanda por interoperabilidade entre sistemas, ampliação de padrões de assinatura (como assinaturas em documentos PDF) e o surgimento de novos modelos, como a utilização de certificados digitais armazenados em nuvem, desde que em conformidade com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Nesse contexto, o presente ETP busca:

- analisar a necessidade de contratação sob a ótica do interesse público;
- contextualizar o objeto a ser contratado à luz da solução atualmente utilizada e das demandas futuras do Tribunal;
- fornecer subsídios técnicos e institucionais para a definição dos requisitos da nova contratação, assegurando a competitividade do certame e a aderência às boas práticas de governança, planejamento e contratação pública.
- avaliar a viabilidade técnica e econômica da contratação;
- identificar e comparar alternativas de solução disponíveis no mercado ou no próprio órgão;
- justificar a escolha da solução considerada mais adequada;
- identificar riscos associados à contratação e possíveis medidas de mitigação;
- subsidiar a elaboração dos artefatos de planejamento da contratação, como o Termo de Referência ou Projeto Básico.

2 DESCRIÇÃO DA NECESSIDADE

2.1 Caracterização do problema a ser resolvido sob a perspectiva do interesse público.

O Tribunal de Contas do Estado do Paraná (TCE-PR) depende, de forma contínua e estrutural, de serviços de assinatura digital e verificação de assinaturas digitais para a execução de suas atividades institucionais, especialmente

aquelas relacionadas ao processo eletrônico, à formalização de atos administrativos e ao exercício das competências constitucionais de controle externo.

Atualmente, a infraestrutura tecnológica do Tribunal conta com solução de assinatura digital contratada, a qual atende aos sistemas corporativos e aplicações internas responsáveis pela tramitação e validação de documentos eletrônicos. Contudo, o contrato vigente possui prazo de vigência improrrogável, o que impõe a necessidade de planejamento e realização de nova contratação, sob pena de descontinuidade de serviço essencial.

A eventual interrupção ou indisponibilidade dos serviços de assinatura digital comprometeria diretamente:

- a formalização de atos administrativos;
- a tramitação regular de processos eletrônicos;
- a produção de documentos com validade jurídica;
- a segurança, integridade e rastreabilidade das informações institucionais.

Sob a ótica do interesse público, tal cenário representa risco significativo à continuidade dos serviços prestados pelo Tribunal, podendo afetar a eficiência administrativa, a segurança jurídica dos atos praticados e o cumprimento tempestivo de suas atribuições constitucionais.

Além do aspecto contratual, observa-se que a solução de assinatura digital constitui uma necessidade permanente e transversal, utilizada por diversos sistemas e unidades organizacionais do TCE-PR, não se tratando de demanda pontual ou circunstancial. Trata-se, portanto, de serviço de natureza contínua, cuja contratação deve ser planejada de forma a assegurar estabilidade, previsibilidade e evolução tecnológica, conforme já reconhecido em estudos técnicos anteriores do próprio Tribunal.

Adicionalmente, o contexto tecnológico e normativo relacionado à assinatura digital tem apresentado evolução relevante, com ampliação de padrões, formatos documentais e modelos de uso, o que reforça a necessidade de que a nova contratação preserve a continuidade operacional, mantenha aderência aos padrões da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), permita a interoperabilidade com os sistemas internos do Tribunal e viabilize a evolução controlada da solução ao longo da vigência contratual.

Dessa forma, o problema a ser enfrentado não se limita à substituição formal de um contrato, mas à necessidade de assegurar a continuidade, a confiabilidade e a adequação tecnológica de serviço essencial à atuação do TCE-PR, em consonância com o interesse público, a eficiência administrativa e a segurança jurídica dos atos praticados.

2.2 Como o TCE-PR vai alcançar maior eficiência com a solução demandada.

A eficiência a ser alcançada pelo Tribunal de Contas do Estado do Paraná com a contratação da solução de plataforma de assinatura digital decorre, primordialmente, da continuidade e da evolução controlada de um serviço essencial, amplamente integrado aos sistemas corporativos e aos fluxos de trabalho institucionais.

A adoção de uma solução corporativa de assinatura digital, provida como serviço e integrada por meio de interfaces padronizadas, permite ao TCE-PR manter e ampliar a automação dos processos administrativos e finalísticos, reduzindo a dependência de procedimentos manuais, eliminando etapas redundantes e assegurando maior celeridade na formalização de atos e documentos eletrônicos.

A eficiência institucional também é alcançada pela centralização da funcionalidade de assinatura digital, evitando a proliferação de soluções isoladas, heterogêneas ou específicas por sistema. Esse modelo contribui para a padronização dos procedimentos, para a simplificação da manutenção tecnológica e para a racionalização do uso de recursos de tecnologia da informação, com reflexos positivos na gestão orçamentária e operacional.

Adicionalmente, a solução demandada possibilita maior eficiência ao preservar a integração com os sistemas internos existentes, de modo que eventuais evoluções tecnológicas, atualizações ou substituições do fornecedor da plataforma de assinatura digital não exijam reescrita ou reestruturação das aplicações corporativas do Tribunal. Essa

abordagem reduz o esforço de adaptação, mitiga riscos de indisponibilidade e assegura maior previsibilidade na gestão do ciclo de vida da solução.

Outro fator relevante para o ganho de eficiência está relacionado à segurança jurídica e à confiabilidade dos documentos eletrônicos, asseguradas por meio da conformidade com os padrões da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). A utilização de mecanismos robustos de assinatura e validação reduz retrabalho, questionamentos formais e a necessidade de reelaboração de atos administrativos, contribuindo para maior fluidez e estabilidade dos processos.

Por fim, a contratação de solução de assinatura digital com capacidade de evolução tecnológica ao longo da vigência contratual, acompanhando mudanças normativas e avanços do mercado, permite ao TCE-PR manter seus processos alinhados às melhores práticas, sem a necessidade de contratações fragmentadas ou emergenciais. Essa característica reforça a eficiência administrativa, ao permitir planejamento, continuidade e melhoria gradual dos serviços prestados pelo Tribunal à sociedade.

3 RESULTADOS A SEREM ALCANÇADOS

3.1 Demonstração dos benefícios esperados, ganhos de eficiência, continuidade, qualidade ou economicidade.

A contratação de solução de plataforma de assinatura digital tem como resultado principal assegurar a continuidade, a eficiência administrativa e a segurança jurídica dos atos e documentos eletrônicos produzidos no âmbito do Tribunal de Contas do Estado do Paraná, em consonância com o interesse público e com os princípios que regem a Administração Pública.

Sob a perspectiva da continuidade do serviço, a nova contratação permitirá mitigar riscos decorrentes do encerramento do contrato atualmente vigente, garantindo que os sistemas corporativos do Tribunal permaneçam aptos a realizar assinaturas e validações de documentos digitais de forma ininterrupta. Considerando que a assinatura digital constitui serviço essencial e transversal aos processos administrativos e finalísticos do TCE-PR, a continuidade operacional representa benefício indispensável à manutenção regular das atividades institucionais.

Conforme exposto no item 2.2, a solução possibilita a manutenção e a ampliação da automação dos fluxos de trabalho que dependem de assinatura digital, reduzindo a necessidade de procedimentos manuais, retrabalho e intervenções operacionais. A centralização da funcionalidade de assinatura digital em uma plataforma corporativa integrada contribui para a padronização dos procedimentos, para a simplificação da gestão tecnológica e para a redução do esforço operacional das equipes envolvidas, promovendo melhor aproveitamento dos recursos humanos disponíveis.

A qualidade dos serviços prestados pelo Tribunal também é aprimorada, na medida em que a solução demandada assegura aderência aos padrões e normativos da Infraestrutura de Chaves Públicas Brasileira, garantindo autenticidade, integridade, rastreabilidade e não repúdio dos documentos eletrônicos. Esses atributos fortalecem a segurança jurídica dos atos praticados, reduzem a possibilidade de questionamentos formais e diminuem a necessidade de refazimento de documentos e procedimentos administrativos.

Do ponto de vista da economicidade e do melhor aproveitamento dos recursos materiais e financeiros, a contratação de uma solução corporativa de assinatura digital evita a fragmentação tecnológica, a duplicidade de soluções por sistemas e a adoção de mecanismos isolados de assinatura. Esse modelo contribui para a racionalização dos investimentos em tecnologia da informação, reduz custos relacionados à manutenção, suporte e integração de soluções diversas e favorece o planejamento orçamentário ao longo da vigência contratual, atendendo ao disposto no art. 22, inciso IX, da IS nº 181/2024.

Adicionalmente, a definição clara dos resultados e benefícios a serem alcançados contribui para a adequada delimitação do objeto da contratação, em conformidade com as diretrizes estabelecidas na Instrução Normativa nº 94/2022, evitando especificações excessivas ou restritivas e preservando a competitividade do certame.

Por fim, os resultados pretendidos estão alinhados aos princípios da eficiência e do interesse público, previstos no art. 11 da Lei nº 14.133/2021, ao buscar uma solução que assegure a continuidade de serviço essencial, promova a eficiência administrativa, preserve a segurança jurídica dos atos do Tribunal e permita a evolução tecnológica controlada ao longo do tempo, em benefício da Administração Pública e da sociedade.

4 ALINHAMENTO ESTRATÉGICO

O Plano Estratégico de Tecnologia da Informação 2023-2027 (PETI 2023-2027), elaborado com base no Plano Estratégico Institucional 2022–2027 (PEI 2022-2027), e o Plano Diretor de Tecnologia da Informação 2025–2026 (PDTI 2025-2026), destacam como Objetivos de TIC:

- Promover soluções inovadoras e adequadas às necessidades do TCE-PR e da Sociedade;
- Prover infraestrutura de TIC;
- Promover a segurança da informação;
- Otimizar orçamento, recursos e serviços de TIC.
- A presente contratação de solução de plataforma de assinatura digital atende diretamente a esses objetivos:
- Promover soluções inovadoras e adequadas às necessidades do TCE-PR e da Sociedade: A plataforma de assinatura digital agiliza a formalização de atos e documentos eletrônicos, ampliando a eficiência, a celeridade processual e a prestação de serviços digitais ao cidadão;
- Prover infraestrutura de TIC: A solução integra-se à infraestrutura tecnológica corporativa do Tribunal, assegurando a continuidade e a disponibilidade de serviço essencial aos sistemas institucionais e aos processos eletrônicos e à infraestrutura tecnológica corporativa do Tribunal;
- Promover a segurança da informação: A contratação garante autenticidade, integridade, rastreabilidade e não repúdio dos documentos digitais, fortalecendo a proteção das informações institucionais e a conformidade jurídica dos atos administrativos;
- Otimizar orçamento, recursos e serviços de TIC: A adoção de uma solução corporativa centralizada reduz custos operacionais, elimina redundâncias, racionaliza o uso de recursos tecnológicos e otimiza a gestão dos serviços de TIC.

A contratação proposta está alinhada à Diretriz 09: Intensificar o Uso e os Recursos de Tecnologia da Informação e Comunicações (TIC) do Plano de Gestão, consolidando o uso de ferramentas eletrônicas que já integram a cultura institucional e permitindo que o Tribunal promova a evolução digital de seus atos e procedimentos.

Dessa forma, a solução de plataforma de assinatura digital atua como base tecnológica para sistemas críticos do Tribunal, promovendo inovação, eficiência, segurança e transparência no atendimento aos objetivos institucionais.

5 ANÁLISE DA SITUAÇÃO ATUAL

5.1 Descrição da situação vigente, contratos em execução, soluções existentes e suas limitações.

Atualmente, o Tribunal de Contas do Estado do Paraná dispõe de solução corporativa de assinatura digital contratada, formalizada por meio do Contrato nº 16/2021, cuja vigência é improrrogável, conforme já registrado nos documentos de planejamento da contratação. Essa solução é utilizada de forma transversal por diversos sistemas institucionais, constituindo serviço essencial à formalização de atos administrativos e à tramitação de documentos no contexto do processo eletrônico.

A arquitetura atualmente adotada pelo Tribunal baseia-se na existência de um assinador corporativo desenvolvido pelo próprio TCE-PR, responsável por intermediar a comunicação entre as aplicações internas e a solução de assinatura digital fornecida pela empresa contratada. As aplicações corporativas não se comunicam diretamente com a plataforma do fornecedor, mas utilizam o assinador do Tribunal como camada de integração padronizada, o que contribui para a organização, a governança e a manutenção da solução no ambiente institucional.

A solução de assinatura digital fornecida pela empresa contratada encontra-se implantada fora do ambiente computacional do TCE-PR, sendo executada na infraestrutura de nuvem da própria fornecedora. O acesso aos serviços de assinatura e validação ocorre por meio de interfaces de comunicação disponibilizadas pela contratada, cabendo ao assinador do Tribunal realizar as chamadas necessárias e consolidar os resultados para consumo pelas aplicações internas.

No cenário vigente, a solução atende aos requisitos essenciais de assinatura e verificação de documentos digitais em conformidade com os padrões da Infraestrutura de Chaves Públicas Brasileira, garantindo autenticidade, integridade, não repúdio e temporalidade dos documentos eletrônicos. Essa abordagem tem permitido ao Tribunal sustentar seus processos administrativos e finalísticos de forma digital, segura e juridicamente válida.

Entretanto, a situação atual apresenta limitações inerentes à própria vigência contratual e ao contexto tecnológico existente à época da contratação. O encerramento iminente do contrato impõe a necessidade de nova contratação para assegurar a continuidade do serviço, ao passo que a evolução das demandas institucionais e das tecnologias de assinatura digital aponta para a necessidade de avaliação de cenários que permitam maior flexibilidade, evolução funcional e adequação às práticas atualmente disponíveis no mercado.

Finalmente, a descrição da situação vigente evidencia a existência de solução funcional e integrada ao ambiente do Tribunal, porém vinculada a contrato com prazo determinado e a um contexto tecnológico que demanda reavaliação, em consonância com os princípios do planejamento, da eficiência administrativa e do interesse público.

6 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO E REQUISITOS

6.1 Requisitos de Negócio

Os requisitos de negócio definem o que a contratação deve entregar do ponto de vista institucional, considerando as necessidades permanentes do Tribunal, a criticidade do serviço e os objetivos estratégicos a serem atendidos, sem antecipar soluções técnicas específicas ou restringir indevidamente a competitividade do certame.

Considerando a caracterização da necessidade apresentada neste Estudo Técnico Preliminar, a solução a ser contratada deverá atender, no mínimo, aos seguintes requisitos de negócio:

6.1.1 Assinatura Digital de Documentos

A solução deve permitir a assinatura digital de documentos, de forma que seja possível determinar, de maneira inequívoca:

- A autenticidade do signatário, assegurando que a assinatura digital corresponde ao responsável pelo ato;
- A integridade do documento, garantindo que o conteúdo não foi alterado após a assinatura;
- O não repúdio, impedindo que o signatário negue a autoria da assinatura;
- A temporalidade, possibilitando identificar o momento exato em que a assinatura foi realizada.

JUSTIFICATIVA: Esses atributos são indispensáveis para assegurar a validade jurídica dos documentos eletrônicos produzidos no âmbito do Tribunal, em consonância com os princípios da segurança da informação e com os padrões adotados pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

6.1.2 Validação de Documentos Digitais

A solução deve permitir a validação de documentos assinados digitalmente, de modo a possibilitar:

- a verificação da autenticidade das assinaturas digitais, assegurando que foram produzidas por signatários legítimos;
- a confirmação da integridade dos documentos, garantindo que o conteúdo não foi alterado após a assinatura;
- a análise da regularidade e validade dos certificados digitais utilizados, considerando o momento da assinatura;
- a verificação dos atributos jurídicos associados às assinaturas, conforme os padrões aplicáveis a documentos eletrônicos.

JUSTIFICATIVA: O Tribunal recebe, produz e analisa documentos assinados digitalmente tanto em seus sistemas internos quanto por terceiros, sendo imprescindível dispor de mecanismo confiável para validação dessas assinaturas, a fim de assegurar segurança jurídica, conformidade normativa e confiança nos documentos eletrônicos que instruem processos administrativos e finalísticos.

6.1.3 Assinatura Individual e em Lote de Documentos

A solução deve possibilitar a assinatura de documentos de forma individual e em lote, permitindo:

- a assinatura de documentos de maneira unitária, conforme fluxos convencionais de trabalho;
- a assinatura simultânea de múltiplos documentos em uma única operação;
- a adequada integração dessa funcionalidade aos fluxos institucionais que demandam elevado volume de assinaturas.

JUSTIFICATIVA: Nos processos administrativos e finalísticos do Tribunal é recorrente a necessidade de assinatura de grande quantidade de documentos em uma mesma etapa do fluxo de trabalho. A possibilidade de assinatura em lote é essencial para assegurar produtividade, eficiência operacional e racionalização do esforço dos usuários, evitando procedimentos repetitivos e manuais.

6.1.4 Integração com os Sistemas Corporativos do Tribunal

A solução deve ser integrável aos sistemas corporativos do Tribunal, de modo a permitir:

- sua utilização de forma centralizada e transversal pelas aplicações institucionais;
- a preservação dos fluxos de trabalho atualmente existentes, minimizando impactos operacionais;
- a utilização da assinatura digital como serviço comum e compartilhado no ambiente tecnológico do Tribunal.

JUSTIFICATIVA: A assinatura digital constitui funcionalidade transversal, utilizada por diversos sistemas do Tribunal. A integração centralizada é necessária para evitar fragmentação de soluções, reduzir riscos operacionais, facilitar a governança e permitir evolução controlada do ambiente tecnológico.

6.1.5 Manutenção, Suporte e Atualização Tecnológica

A solução deve contemplar, como parte indissociável do objeto, serviços de manutenção, suporte e atualização tecnológica, assegurando:

- a continuidade do serviço ao longo da vigência contratual;
- a estabilidade e o adequado funcionamento da solução;
- a correção de falhas, incidentes ou degradações de desempenho;
- a atualização da solução frente a evoluções normativas, tecnológicas ou de segurança.

JUSTIFICATIVA: Trata-se de serviço essencial e contínuo, cuja indisponibilidade ou degradação impacta diretamente as atividades institucionais do Tribunal. A previsão de manutenção, suporte e atualização tecnológica é necessária para preservar o funcionamento adequado da solução, mitigar riscos operacionais e evitar obsolescência tecnológica ao longo do tempo.

6.1.6 Evolução Funcional da Solução

A solução deve permitir a evolução funcional ao longo do tempo, de modo a possibilitar, de forma planejada e controlada:

- a incorporação de novos formatos de assinatura digital, incluindo formatos documentais amplamente adotados no contexto institucional e no mercado;
- a adoção de novos modelos de uso da assinatura digital, compatíveis com diferentes formas de armazenamento e utilização de certificados digitais;
- a adaptação a mudanças normativas, institucionais ou tecnológicas que impactem os processos de assinatura e validação de documentos eletrônicos
- a implementação dessas evoluções sem prejuízo da continuidade, da estabilidade e da confiabilidade do serviço.

JUSTIFICATIVA: O contexto tecnológico e normativo relacionado à assinatura digital é dinâmico, com constante surgimento de novos formatos documentais, modelos de uso e requisitos regulatórios. Dessa forma, a solução contratada deve possuir capacidade de adaptação e evolução ao longo da vigência contratual, de maneira planejada e controlada, evitando contratações fragmentadas, soluções emergenciais ou interrupções em serviço essencial ao funcionamento do Tribunal.

6.2 Requisitos Técnicos

Os requisitos técnicos da solução foram definidos com base nas necessidades institucionais do Tribunal, na arquitetura tecnológica adotada e nas boas práticas aplicáveis à prestação de serviços de assinatura digital e validação de documentos eletrônicos, incluindo aspectos de integração com sistemas corporativos, segurança da informação, desempenho, disponibilidade, aderência aos padrões da ICP-Brasil e suporte à evolução tecnológica.

Tendo em vista a complexidade e o nível de detalhamento desses requisitos, optou-se por apresentá-los de forma estruturada em apêndice próprio, a fim de preservar a clareza e a objetividade do corpo principal deste Estudo Técnico Preliminar.

Dessa forma, os requisitos técnicos completos encontram-se consolidados no Apêndice A – Requisitos Técnicos da Solução, que constitui parte integrante deste ETP e servirá de referência para a elaboração do Termo de Referência.

JUSTIFICATIVA: O atendimento aos requisitos da Funcionalidade de Assinatura Digital de Documentos é indispensável para assegurar validade jurídica às assinaturas geradas, garantir interoperabilidade entre formatos, permitir a realização de assinaturas múltiplas exigidas por procedimentos internos, detalhar e organizar o protocolo de assinatura em etapas independentes, reduzir o tráfego de dados e a manipulação de arquivos inteiros, preservar a confidencialidade da chave privada do signatário, viabilizar a certificação confiável da data e da hora das assinaturas por Autoridade de Carimbo do Tempo, assegurar o uso de certificados válidos no momento da assinatura, possibilitar a conversão de representações de assinatura dentro da infraestrutura tecnológica do Tribunal e conferir desempenho adequado para cenários de assinaturas em lote concorrentes, conforme já demonstrado pela ferramenta atualmente contratada.

6.3 Requisitos operacionais e de implantação

Os requisitos operacionais e de implantação descrevem as condições necessárias para a implementação, início da execução e operação do objeto contratado, desde o início da vigência contratual, com o objetivo de reduzir riscos de descontinuidade, falhas operacionais ou impactos negativos às atividades do Tribunal.

6.3.1 Condições de Implantação e Início da Execução

A contratação deverá prever condições adequadas para a implantação da solução e para o início da prestação dos serviços, incluindo, quando aplicável, período de transição entre a solução atualmente em uso e a nova solução contratada.

JUSTIFICATIVA: A solução de assinatura digital é integrada a processos institucionais críticos, sendo imprescindível que sua implantação ocorra de forma planejada e controlada, sem prejuízo às atividades finalísticas e administrativas do Tribunal.

6.3.2 Continuidade do Serviço Durante a Transição

A implantação da solução deverá ocorrer de modo a preservar a continuidade dos serviços de assinatura e validação de documentos do TCE-PR, evitando interrupções ou degradações indevidas durante eventual período de transição contratual.

JUSTIFICATIVA: A indisponibilidade do serviço de assinatura digital pode impactar diretamente a formalização de atos administrativos e processuais desta Corte de Contas, tornando necessária a adoção de salvaguardas que garantam a continuidade operacional.

6.3.3 Adaptação e Integração com o Ambiente Institucional

Quando necessário, a implantação da solução poderá envolver serviços de adaptação ou integração com os sistemas e o ambiente tecnológico do Tribunal, observadas as características da solução adotada e os fluxos atualmente existentes.

Os requisitos operacionais da contratação deverão considerar a necessidade de prazo adequado para a realização das atividades de adaptação técnica e integração da solução contratada ao ambiente e às interfaces (APIs) do Tribunal, de modo a assegurar o início da operação em condições de estabilidade, segurança e aderência aos fluxos institucionais.

JUSTIFICATIVA: A assinatura digital é funcionalidade transversal utilizada por diversos sistemas institucionais. A previsão genérica de adaptação e integração reduz riscos técnicos, assegura a compatibilidade da solução com o ambiente do Tribunal e evita retrabalhos futuros.

6.3.4 Prazos para Implantação e Início da Operação

A contratação deverá estabelecer prazos máximos, contados em dias, para a conclusão da implantação e para o início efetivo da operação da solução, compatíveis com a complexidade do objeto e com a necessidade de continuidade do serviço.

A definição dos requisitos operacionais e de implantação deverá observar, ainda, a necessidade de transição planejada entre a solução atualmente em uso e a nova solução a ser contratada, considerando o encerramento da vigência contratual atual, de forma a evitar descontinuidade na prestação dos serviços de assinatura digital.

JUSTIFICATIVA: A definição de prazos claros e factíveis contribui para o planejamento da Administração, permite o adequado acompanhamento da execução contratual e reduz o risco de atrasos injustificados na disponibilização da solução.

6.3.5 Forma de Interação e Acompanhamento

Deverão ser definidos mecanismos formais de interação e acompanhamento entre a contratada e as equipes do Tribunal responsáveis pela gestão e fiscalização do contrato, especialmente no período inicial de implantação.

JUSTIFICATIVA: A comunicação estruturada e o acompanhamento contínuo permitem o alinhamento de expectativas, a identificação precoce de desvios e a adoção tempestiva de medidas corretivas durante a execução contratual.

6.3.6 Monitoramento da Execução Inicial

O Tribunal deverá possuir o direito de acompanhar e avaliar o desempenho da contratada durante a fase de implantação e no início da operação da solução, mediante solicitação de informações ou realização de reuniões de acompanhamento, quando necessário.

JUSTIFICATIVA: O monitoramento inicial da execução é instrumento essencial de governança contratual, permitindo verificar a aderência da solução às condições pactuadas e contribuir para a estabilidade da operação no início da vigência contratual.

6.4 Monitoramento

6.4.1 Acompanhamento

O CONTRATANTE terá o direito de, a qualquer momento, solicitar informações e avaliar o desempenho operacional e/ou de segurança da CONTRATADA em relação aos serviços contratados.

O CONTRATANTE terá o direito de estabelecer reuniões periódicas de acompanhamento, sempre que julgar necessário.

JUSTIFICATIVA: A avaliação do desempenho da CONTRATADA é uma importante ferramenta para garantir a qualidade dos serviços prestados; bem como colabora para a identificação precoce de desvios e anomalias na execução contatual.

6.4.2 Comunicações Obrigatórias

A CONTRATADA deve informar com antecedência ao CONTRATANTE, por meio dos canais formais de comunicação, quando identificado que as solicitações urgentes não forem passíveis de solução no prazo estabelecido.

JUSTIFICATIVA: As solicitações urgentes são aquelas que devem ser atendidas em um prazo reduzido, geralmente de horas ou dias. O atraso na resolução de uma solicitação urgente pode causar transtornos e prejuízos para o CONTRATANTE.

6.5 Qualidade, Metodologias e Padrões

Os requisitos de qualidade, metodologias e padrões estabelecem diretrizes gerais a serem observadas na execução dos serviços, com o objetivo de assegurar que a solução contratada seja implantada e operada de forma aderente às práticas institucionais do Tribunal, preservando a confiabilidade, a segurança e a qualidade da prestação dos serviços.

6.5.1 A execução dos serviços contratados deverá observar as diretrizes técnicas, operacionais, processos e padrões estabelecidos pela Diretoria de Tecnologia da Informação (DTI), bem como aquelas que vierem a ser formalmente definidas pelo CONTRATANTE ao longo da execução contratual, sob a supervisão de profissionais designados para a gestão e fiscalização do contrato.

JUSTIFICATIVA: A observância de diretrizes, metodologias e padrões institucionais é fundamental para garantir a qualidade, a uniformidade e a governança na prestação dos serviços de TIC. Ao alinhar a execução contratual aos processos e práticas definidos pela DTI, o Tribunal reduz riscos de inconsistências técnicas, facilita o acompanhamento e a fiscalização do contrato e assegura que a solução implantada permaneça compatível com o ambiente tecnológico, os princípios de segurança da informação e os objetivos institucionais.

6.6 Pagamento

6.6.1 Pagamento por Resultado (Níveis Mínimos de Serviço e Remuneração Variável)

O pagamento da solução ficará condicionado à efetiva prestação dos serviços, conforme modelo de medição por resultados a ser definido no Termo de Referência. Ocorrendo, preferencialmente, mensalmente.

6.6.2 Relatório Mensal de Serviços Prestados

A prestação dos serviços de assinatura digital, verificação de assinaturas digitais e validação de certificados deverá ocorrer de forma contínua ao longo da vigência contratual, com apuração periódica, preferencialmente mensal, do consumo efetivamente realizado pelas aplicações corporativas do Tribunal.

O valor a ser pago em cada período de apuração estará relacionado à quantidade efetiva de assinaturas e verificações de assinaturas realizadas, conforme os registros e evidências produzidos pela própria solução contratada e validados pelo Tribunal, em consonância com o modelo de solução definido neste Estudo Técnico Preliminar.

Para fins de apuração do consumo mensal, deverão ser considerados os registros de uso dos serviços, bem como a verificação da disponibilidade da solução ao longo do período, observado que aspectos relacionados à conformidade com níveis mínimos de serviço, eventuais impactos da indisponibilidade e mecanismos de ajuste financeiro serão definidos de forma detalhada no Termo de Referência e no instrumento contratual.

A adoção desse modelo de apuração visa assegurar a adequada correspondência entre a utilização dos serviços e o dispêndio de recursos públicos, preservando a transparência, a rastreabilidade e a aderência às boas práticas de contratação de soluções de Tecnologia da Informação e Comunicação.

6.7 Implantação

A implantação da solução deverá ocorrer de forma planejada, progressiva e controlada, de modo a assegurar a continuidade dos serviços de assinatura digital e de verificação de assinaturas digitais utilizados pelo Tribunal, evitando interrupções ou impactos indevidos aos sistemas e processos institucionais dependentes dessas funcionalidades.

Considerando a natureza crítica e transversal do serviço de assinatura digital, bem como sua integração com múltiplas aplicações corporativas, a implantação da solução poderá envolver, quando aplicável, atividades de configuração inicial, adaptação técnica e integração ao ambiente tecnológico do Tribunal, respeitado o modelo arquitetural atualmente adotado e os fluxos operacionais existentes.

Deverão ser observadas, ainda, condições adequadas para eventual transição entre a solução atualmente em uso e a nova solução a ser contratada, quando for o caso, de modo a preservar a estabilidade do ambiente, a rastreabilidade dos atos praticados e a regularidade dos serviços durante o início da vigência contratual.

Os aspectos específicos relacionados a cronograma, responsabilidades, procedimentos de implantação, critérios de acompanhamento e marcos de início de operação serão detalhados no Termo de Referência, em consonância com a solução escolhida e com as características definitivas do objeto contratado.

6.8 Componentes Tecnológicos

A execução, o acompanhamento e a fiscalização da contratação deverão estar apoiados em componentes tecnológicos compatíveis com o ambiente institucional do Tribunal de Contas do Estado do Paraná, de modo a assegurar a adequada integração da solução ao ecossistema corporativo, bem como a rastreabilidade, a transparência e a confiabilidade das informações relacionadas à prestação dos serviços.

A solução a ser contratada e o modelo de prestação dos serviços deverão ser compatíveis, quando aplicável, com os instrumentos e ambientes tecnológicos utilizados institucionalmente pelo Tribunal, especialmente aqueles voltados à gestão administrativa, ao acompanhamento da execução contratual e ao controle das informações produzidas no contexto da prestação dos serviços. Isso inclui a possibilidade de utilização de ferramentas corporativas de gestão e acompanhamento, bem como a observância de modelos institucionais de relatórios e registros, definidos e validados pelo TCE-PR, com vistas à padronização das informações, à rastreabilidade e ao apoio às atividades de fiscalização.

Os dados, evidências ou relatórios relacionados à execução dos serviços deverão ser passíveis de disponibilização em ambientes institucionais de consulta do Tribunal, respeitados os critérios de acesso, segurança da informação e os parâmetros administrativos definidos, de forma a viabilizar o acompanhamento tempestivo da execução contratual e a preservação do histórico das informações.

Considerando ainda os aspectos administrativos e operacionais associados à gestão contratual, a execução do contrato poderá demandar a utilização de certificado digital no padrão ICP-Brasil, preferencialmente do tipo A3 ou outro que venha a ser formalmente designado pelo Tribunal, como meio de autenticação e identificação eletrônica da CONTRATADA em sistemas institucionais, para envio e assinatura de documentos administrativos, formalização de comunicações, abertura e acompanhamento de procedimentos, bem como para outras atividades que exijam identificação digital no âmbito da relação contratual. O uso de certificado digital, nesses casos, constitui instrumento de interação administrativa, não se confundindo com os requisitos técnicos do serviço de assinatura digital objeto da contratação.

A consideração desses componentes tecnológicos no planejamento da contratação tem por finalidade favorecer a integração da solução aos processos institucionais existentes, reduzir riscos operacionais e administrativos, fortalecer os mecanismos de governança e fiscalização contratual e assegurar a aderência da execução às normas, diretrizes e práticas adotadas pelo Tribunal.

> JUSTIFICATIVA: A identificação prévia dos componentes tecnológicos necessários à execução, acompanhamento e fiscalização da contratação contribui para a mitigação de riscos, para a melhoria da governança contratual e para a adequada integração da solução ao ambiente tecnológico do TCE-PR, assegurando condições propícias à transparência, ao controle administrativo e à confiabilidade das informações produzidas no contexto da prestação dos serviços.

6.9 Legais, de Segurança e Privacidade

A solução a ser contratada deverá observar integralmente a legislação vigente, os normativos institucionais e as diretrizes aplicáveis à segurança da informação, à proteção de dados e à privacidade, considerando a criticidade do serviço de assinatura digital para as atividades administrativas e finalísticas do Tribunal de Contas do Estado do Paraná.

A contratação deverá estar em conformidade com os princípios e disposições da Lei nº 14.133/2021, especialmente no que se refere à segurança da execução contratual, à proteção do interesse público e à adoção de soluções compatíveis com os princípios da legalidade, da eficiência, da transparência e da governança. Deverão ser observadas, ainda, as diretrizes estabelecidas na Instrução Normativa IS nº 181/2024, em especial aquelas relacionadas à caracterização da necessidade, à análise de riscos e à avaliação de impactos, conforme previsto em seu art. 22.

Considerando que a solução envolve o tratamento de informações institucionais e, eventualmente, de dados pessoais, deverão ser observados os princípios, fundamentos e requisitos estabelecidos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), notadamente no que se refere à finalidade, à necessidade, à segurança, à prevenção e à responsabilização, de modo a assegurar a proteção dos dados tratados no contexto da execução contratual.

No que diz respeito aos serviços de assinatura digital e de verificação de assinaturas, a solução deverá observar os normativos aplicáveis à Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, quando pertinentes, de forma a garantir a validade jurídica, a autenticidade, a integridade, o não repúdio e a confiabilidade dos documentos eletrônicos produzidos ou tratados no âmbito do Tribunal.

A concepção da solução e o modelo de prestação dos serviços deverão, ainda, estar alinhados às políticas, normas e diretrizes internas do TCE-PR relacionadas à segurança da informação, à proteção de ativos institucionais e à gestão de riscos, adotando medidas técnicas e organizacionais compatíveis com a natureza e a criticidade do serviço.

Os requisitos específicos, controles técnicos, responsabilidades, procedimentos de segurança, mecanismos de auditoria e demais aspectos necessários à plena conformidade legal, à segurança da informação e à proteção de dados serão definidos de forma detalhada no Termo de Referência e nos instrumentos contratuais correspondentes.

> JUSTIFICATIVA: A observância das normas legais, dos normativos institucionais e dos princípios de segurança da informação e de proteção de dados é condição essencial para assegurar a confiabilidade da solução de assinatura digital, a proteção das informações institucionais sob responsabilidade do Tribunal e a aderência da contratação aos princípios da legalidade, da segurança jurídica, da transparência e do interesse público.

6.10 Propriedade Intelectual

A contratação deverá observar as disposições legais e os normativos institucionais aplicáveis à propriedade intelectual, considerando a natureza híbrida da solução a ser contratada, que poderá envolver tanto o licenciamento de plataforma de assinatura digital operada como serviço (SaaS) quanto o desenvolvimento de componentes específicos para integração com os sistemas do Tribunal.

No que se refere à plataforma de assinatura digital fornecida como serviço, inclusive seus componentes, códigos-fonte, bibliotecas, algoritmos, modelos e demais ativos pré-existentes de propriedade da contratada, a relação jurídica se dará sob a forma de licenciamento de uso, limitado ao escopo e à vigência contratual, não se caracterizando cessão de direitos de propriedade intelectual.

Por outro lado, eventuais componentes de software, serviços auxiliares, módulos de adaptação, conectores, bibliotecas ou códigos desenvolvidos especificamente para atender às necessidades do Tribunal, com a finalidade de integração da solução contratada aos sistemas institucionais do TCE-PR ou de viabilização de fluxos operacionais próprios, deverão observar regime diferenciado de propriedade intelectual, a ser definido no Termo de Referência e no instrumento contratual, podendo contemplar a cessão dos direitos patrimoniais ao Tribunal, nos termos da legislação aplicável.

Nesse contexto, deverão ser considerados, quando pertinentes, os dispositivos da Lei nº 9.609/1998 (Lei do Software) e da Lei nº 9.610/1998 (Lei de Direitos Autorais), de modo a assegurar ao Tribunal o direito de utilizar, manter, evoluir ou substituir os componentes desenvolvidos sob encomenda, preservada a continuidade dos serviços e a independência tecnológica institucional.

As informações, documentos, especificações técnicas, registros, dados e demais conteúdos produzidos ou tratados no âmbito da execução contratual deverão ser considerados de uso restrito institucional, observadas as regras de confidencialidade, segurança da informação e proteção de dados adotadas pelo TCE-PR.

Os critérios específicos relacionados à titularidade, à cessão ou ao licenciamento de direitos de propriedade intelectual, bem como à forma de entrega, custódia e acesso aos artefatos produzidos no contexto da contratação, serão detalhados no Termo de Referência, em consonância com a solução adotada e com o interesse público envolvido.

> JUSTIFICATIVA: A adequada definição do regime de propriedade intelectual é necessária para preservar o equilíbrio entre o modelo de prestação da solução como serviço, a proteção dos direitos da contratada e o interesse do Tribunal na autonomia, na continuidade operacional e na governança dos componentes desenvolvidos especificamente para seu ambiente institucional, mitigando riscos de dependência tecnológica e assegurando a sustentabilidade da solução ao longo do tempo.

6.11 Sociais, Ambientais e Culturais

A execução dos serviços decorrentes da contratação deverá observar as diretrizes de sustentabilidade ambiental adotadas pelo Tribunal de Contas do Estado do Paraná, pautando-se pelo uso racional de recursos e

equipamentos, de modo a evitar e prevenir o desperdício de insumos e materiais consumidos, bem como a geração excessiva de resíduos, sempre que compatível com a natureza da solução e do modelo de prestação dos serviços.

Nesse contexto, espera-se que a atuação da CONTRATADA considere práticas que favoreçam a eficiência no uso de recursos, a redução de desperdícios e a adequada destinação de resíduos eventualmente gerados no âmbito da execução contratual, em consonância com os princípios de responsabilidade ambiental e desenvolvimento sustentável observados pela Administração Pública.

A CONTRATADA deverá, ainda, orientar seus profissionais quanto à importância da racionalização de recursos no desempenho de suas atividades, bem como quanto à observância das diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE, quando aplicáveis ao objeto da contratação.

> JUSTIFICATIVA: A consideração de diretrizes e critérios de sustentabilidade ambiental no planejamento da contratação contribui para a proteção do meio ambiente, para a promoção do desenvolvimento sustentável e para o alinhamento da execução contratual às boas práticas adotadas pelo Tribunal de Contas do Estado do Paraná, em conformidade com os princípios que regem a Administração Pública.

7 IDENTIFICAÇÃO E ANÁLISE DE SOLUÇÕES

7.1 Introdução

Considerando a caracterização da necessidade, a análise da situação atual e os requisitos de negócio e técnicos já identificados neste Estudo Técnico Preliminar, verificou-se como solução apta a atender às demandas institucionais do Tribunal de Contas do Estado do Paraná a contratação de plataforma corporativa de assinatura digital, integrada aos sistemas internos por meio de interfaces padronizadas e compatível com a arquitetura atualmente adotada pelo Tribunal.

A solução planejada deve ser capaz de prover, de forma centralizada e contínua, os serviços de assinatura digital e de verificação de assinaturas digitais utilizados pelas aplicações corporativas do TCE-PR, preservando o modelo arquitetural no qual o assinador desenvolvido pelo Tribunal atua como camada intermediária entre os sistemas internos e a solução de assinatura digital fornecida por terceiros.

No contexto da evolução tecnológica observada desde a contratação anterior, a solução identificada deve ser compatível com os requisitos de negócio e técnicos já consolidados, bem como admitir a incorporação de funcionalidades atualmente demandadas pelo Tribunal, tais como o suporte à assinatura digital de documentos no padrão PDF/PAdES, incluindo a possibilidade de aplicação de assinatura com representação visual e posicionamento controlado no documento, e a utilização de certificados digitais armazenados em nuvem, observando os normativos aplicáveis. Tais características são consideradas extensões naturais do serviço de assinatura digital e não alteram a natureza da solução identificada.

A identificação da solução, portanto, não se vincula a produto, fornecedor ou modelo de implantação específico, mas a um modelo de solução tecnológica que assegure a continuidade do serviço, a interoperabilidade com os sistemas institucionais, a aderência normativa e a capacidade de evolução ao longo da vigência contratual, em consonância com as diretrizes de planejamento previstas.

A análise das soluções foi realizada à luz dos elementos levantados nos itens anteriores deste Estudo Técnico Preliminar, bem como das diretrizes estabelecidas no art. 18, inciso IV, da Lei nº 14.133/2021, que impõe a avaliação das alternativas possíveis e a demonstração da adequação da solução ao interesse público.

Sob o aspecto técnico, a solução de plataforma de assinatura digital integrada ao assinador do Tribunal apresenta aderência à arquitetura atualmente em uso, ao preservar a separação entre as aplicações internas e os serviços de assinatura fornecidos por terceiros. Esse modelo reduz impactos sobre os sistemas corporativos em caso de

substituição de fornecedor e permite que eventuais ajustes ou evoluções concentrem-se na camada de integração, sem necessidade de alterações estruturais nas aplicações institucionais.

Do ponto de vista institucional e operacional, as soluções a serem analisadas devem atender à necessidade de continuidade e confiabilidade do serviço, considerando seu caráter transversal e essencial para os processos administrativos e finalísticos do TCE-PR. Dessa forma, a centralização da funcionalidade de assinatura digital contribui para a padronização dos fluxos de trabalho, para a governança da solução e para a racionalização da gestão tecnológica no âmbito da Diretoria de Tecnologia da Informação.

A análise também considerou a viabilidade de evolução da solução, uma vez que o modelo identificado permite a adoção de funcionalidades e modelos de uso compatíveis com as práticas atuais do mercado, como a assinatura de documentos em PDF e a utilização de certificados digitais em nuvem, sem ruptura da arquitetura existente. Eventuais necessidades de desenvolvimento, adaptação ou evolução da camada de integração entre o assinador do Tribunal e a plataforma de assinatura digital são compatíveis com práticas usuais de contratação de soluções de tecnologia da informação e não comprometem a viabilidade da solução analisada.

Dessa forma, a solução identificada mostra-se adequada sob os aspectos técnico, institucional e normativo, atendendo às diretrizes de planejamento da contratação previstas na Instrução Normativa nº 94/2022 e na Instrução de Serviço nº 181/2024, e constituindo base suficiente para o levantamento e a descrição das alternativas de implementação a serem apresentadas no item seguinte deste Estudo Técnico Preliminar.

8 LEVANTAMENTO DE ALTERNATIVAS

8.1 Cenário A1: Desenvolvimento de software assinador de documentos digitais pelo TCE-PR:

No presente cenário, a solução de assinatura digital seria desenvolvida sob demanda pelo Tribunal de Contas do Estado do Paraná, por meio da contratação vigente de serviços de desenvolvimento de software (fábrica de software), utilizando-se equipes técnicas alocadas especificamente para a concepção, implementação, testes, implantação e manutenção evolutiva da solução, por meio de postos de trabalho alocados com dedicação exclusiva de mão de obra para os perfis profissionais contratados.

Nesse modelo, o TCE-PR assumiria a definição detalhada dos requisitos funcionais e não funcionais da solução de assinatura digital, incluindo, entre outros aspectos já identificados neste Estudo Técnico Preliminar, o suporte à assinatura de documentos em formato PDF, a utilização de certificados digitais em nuvem e a integração com os sistemas corporativos existentes. A solução seria desenvolvida de forma aderente à arquitetura institucional do Tribunal, respeitando os padrões tecnológicos, metodologias de desenvolvimento, processos de segurança da informação e diretrizes de governança de TIC já adotados pela Diretoria de Tecnologia da Informação.

A implementação da solução envolveria o desenvolvimento completo dos componentes necessários à prestação do serviço de assinatura digital, incluindo os módulos responsáveis pela geração, validação e verificação de assinaturas, bem como os mecanismos de integração com o assinador corporativo do Tribunal e com os sistemas consumidores. A solução resultante seria implantada no ambiente tecnológico do TCE-PR, sob sua gestão direta, incluindo a infraestrutura de execução, os mecanismos de monitoramento e os controles de acesso e segurança.

Diante disso, caberia à equipe interna do Tribunal, com o apoio da fábrica de software contratada, a condução das atividades de especificação, acompanhamento, homologação e aceitação das entregas, bem como a gestão do ciclo de vida da solução desenvolvida. Eventuais evoluções, correções ou adequações decorrentes de mudanças normativas, tecnológicas ou de requisitos institucionais seriam tratadas como demandas de desenvolvimento e manutenção no âmbito do contrato de fábrica de software.

O cenário descrito pressupõe, portanto, a construção de uma solução própria de assinatura digital, desenvolvida especificamente para atender às necessidades do TCE-PR, integrada aos seus sistemas internos e mantida sob sua

responsabilidade operacional, observadas as condições contratuais, técnicas e organizacionais vigentes para a prestação de serviços de desenvolvimento de software.

8.2 Cenário A2: Aquisição de Solução de Assinatura Implantada e Operada no Ambiente do TCE PR:

No presente cenário, a solução de assinatura digital seria adquirida de fornecedor especializado, sob a forma de software a ser instalado e executado no ambiente computacional do Tribunal de Contas do Estado do Paraná, passando a integrar a infraestrutura tecnológica institucional sob gestão direta do TCE-PR.

Nesse modelo, o fornecedor contratado seria responsável pelo fornecimento da plataforma de assinatura digital, bem como pela disponibilização dos componentes necessários à sua implantação, operação e manutenção no ambiente do Tribunal. A solução deve atender aos requisitos de negócio e técnicos previamente identificados neste Estudo Técnico Preliminar, incluindo o suporte à assinatura de documentos em formato PDF, a utilização de certificados digitais armazenados em nuvem e a conformidade com os normativos aplicáveis à assinatura digital e à segurança da informação.

A integração da solução com os sistemas corporativos do Tribunal ocorreria por meio do assinador desenvolvido pelo TCE-PR, preservando o modelo arquitetural atualmente adotado, no qual as aplicações internas não se comunicam diretamente com a plataforma de assinatura digital. Para viabilizar essa integração, o fornecedor da solução seria responsável pelo desenvolvimento, adaptação ou disponibilização dos componentes de integração necessários, incluindo eventual implementação ou evolução do software adaptador, de modo a assegurar a interoperabilidade entre o assinador do Tribunal e a plataforma de assinatura digital instalada localmente.

A solução, uma vez implantada, passaria a operar nos ambientes de infraestrutura do TCE-PR, incluindo os ambientes de desenvolvimento, homologação e produção, observadas as políticas internas de segurança, controle de acesso, monitoramento e continuidade de serviços. Caberia ao Tribunal definir, em conjunto com o fornecedor, os procedimentos de implantação, atualização, suporte técnico e correção de falhas, de acordo com os termos contratuais estabelecidos.

Nesse cenário, a gestão operacional da solução de assinatura digital, bem como a administração de sua infraestrutura de execução, seria realizada pelo TCE-PR, com apoio do fornecedor contratado para atividades de suporte, manutenção e evolução tecnológica. Eventuais atualizações decorrentes de mudanças normativas, tecnológicas ou de requisitos institucionais seriam tratadas conforme as condições previstas no contrato, preservando a aderência da solução às necessidades do Tribunal ao longo de sua vigência.

O cenário descrito contempla, portanto, a adoção de solução de assinatura digital fornecida por terceiro, implantada e operada no ambiente do TCE-PR, integrada aos sistemas internos por meio do assinador corporativo e alinhada às diretrizes institucionais de governança, segurança e gestão de tecnologia da informação.

8.3 Cenário A3: Aquisição de Solução de Assinatura Implantada e Operada em Ambiente Externo

No presente cenário, a solução de assinatura digital seria contratada de fornecedor especializado e executada fora do ambiente computacional do Tribunal de Contas do Estado do Paraná, permanecendo hospedada e operada na infraestrutura tecnológica da própria empresa contratada, em modelo semelhante ao atualmente adotado pelo TCE-PR.

Nesse modelo, o fornecedor é responsável pela disponibilização da plataforma de assinatura digital em seu ambiente de execução, bem como pela operação, manutenção, suporte técnico e atualização tecnológica da solução ao longo da vigência contratual. A solução contratada deve atender aos requisitos de negócio e técnicos previamente identificados neste Estudo Técnico Preliminar, incluindo o suporte à assinatura de documentos em formato PDF, a utilização de certificados digitais armazenados em nuvem e a observância dos normativos aplicáveis à assinatura digital e à segurança da informação.

A integração entre os sistemas corporativos do Tribunal e a solução de assinatura digital ocorreria por meio do assinador desenvolvido pelo TCE-PR, preservando o modelo arquitetural atualmente adotado, no qual as aplicações internas não realizam comunicação direta com a plataforma da contratada. Para viabilizar essa integração, o fornecedor seria responsável pelo desenvolvimento, disponibilização ou manutenção do software adaptador, encarregado de intermediar a comunicação entre o assinador do Tribunal e a solução de assinatura digital executada em seu ambiente.

A infraestrutura necessária à execução da solução de assinatura digital, incluindo servidores, armazenamento, mecanismos de segurança, monitoramento e alta disponibilidade, permaneceria sob responsabilidade da empresa contratada. Caberia ao Tribunal, por sua vez, a gestão do assinador corporativo, das aplicações consumidoras do serviço e da fiscalização da execução contratual, conforme os parâmetros definidos no instrumento de contratação.

Destaca-se que a operação da solução fora do ambiente do TCE-PR pressupõe a definição de interfaces de comunicação seguras entre o Tribunal e a infraestrutura da contratada, bem como a observância das políticas institucionais de segurança da informação, proteção de dados e continuidade de serviços. Eventuais evoluções funcionais, adequações normativas ou ajustes decorrentes de mudanças nos requisitos institucionais seriam tratadas no âmbito da relação contratual estabelecida com o fornecedor da solução.

O cenário descrito contempla, portanto, a contratação de plataforma de assinatura digital fornecida e operada por terceiro em ambiente externo ao Tribunal, integrada aos sistemas internos por meio do assinador corporativo e do adaptador de comunicação, mantendo-se a separação entre a infraestrutura do TCE-PR e a infraestrutura da empresa contratada.

9 ESTIMATIVA DAS QUANTIDADES

9.1 Desenvolvimento de software assinador de documentos digitais pelo TCE-PR

No que se refere ao cenário de desenvolvimento de solução própria de assinatura digital pela fábrica de software, a estimativa de quantitativos foi realizada com base na complexidade funcional da solução necessária para atender aos requisitos de negócio e técnicos já identificados neste Estudo Técnico Preliminar.

A solução de assinatura digital considerada neste cenário compreende um conjunto significativo de funcionalidades, incluindo, entre outras, serviços de assinatura e validação de documentos digitais, suporte à assinatura de documentos em formato PDF, utilização de certificados digitais armazenados em nuvem, carimbo do tempo, validação de certificados e integração com os sistemas corporativos do Tribunal por meio do assinador institucional. Trata-se, portanto, de solução de porte relevante, comparável a plataformas de assinatura digital já consolidadas no mercado.

Com base nesse contexto, adota-se, para fins de estimativa preliminar, um tamanho funcional da ordem de 1.500 (mil e quinhentos) Pontos de Função, valor considerado conservador e compatível com a complexidade da solução a ser desenvolvida. Ressalta-se que essa estimativa tem caráter indicativo, suficiente para subsidiar a análise comparativa entre os cenários, não substituindo eventual contagem detalhada a ser realizada caso esse cenário fosse efetivamente adotado.

Considerando a referência de produtividade usualmente adotada nos contratos de desenvolvimento de software do Tribunal, na qual se utiliza o parâmetro HH/PF = 10 (dez) horas por Ponto de Função, o desenvolvimento de uma solução dessa ordem de grandeza demandaria aproximadamente 15.000 (quinze mil) horas de esforço de desenvolvimento.

Ao converter esse esforço para uma perspectiva de execução por equipe, observa-se que, mesmo com a atuação simultânea de aproximadamente 7 (sete) desenvolvedores em tempo integral, o prazo estimado para a entrega de uma solução dessa complexidade situar-se-ia em torno de um ano de trabalho, desconsiderando-se, para fins de simplificação, períodos adicionais de planejamento, homologação, estabilização e ajustes pós-implantação.

Além do esforço direto de desenvolvimento, esse cenário pressupõe a participação de outros perfis técnicos indispensáveis ao ciclo de vida do software, tais como analistas de requisitos, arquitetos de software, profissionais de

testes e garantia da qualidade, bem como atividades de gestão de projeto. Esses perfis, ainda que não alocados em regime de dedicação integral ao longo de todo o período, representam custos adicionais e esforço organizacional relevante, que devem ser considerados na avaliação global do cenário.

Deve-se considerar o esforço administrativo e transacional associado à execução e fiscalização de um contrato dessa natureza. Para fins de estimativa preliminar de quantitativos, considera-se a necessidade de atuação de mais de um servidor na função de fiscais técnicos do contrato, responsáveis pelo acompanhamento das ordens de serviço, validação das entregas e interlocução técnica com a contratada, bem como de no mínimo um servidor na função de fiscal administrativo, responsável pelo acompanhamento dos aspectos formais e contratuais, além de servidores atuando nas comissões de recebimento e também na gestão do contrato.

Esses servidores não estariam alocados em regime de dedicação exclusiva ao projeto, porém teriam participação recorrente e relevante ao longo de todo o período de desenvolvimento e estabilização da solução, envolvendo atividades de acompanhamento, controle, registros formais de aceite e gestão das interações contratuais. Esse esforço representa quantitativo organizacional adicional que deve ser considerado na avaliação global do cenário, ainda que não mensurável em pontos de função ou horas técnicas de desenvolvimento.

Diante do exposto, resta evidenciado que o desenvolvimento de solução própria de assinatura digital implicaria elevado esforço técnico, temporal e organizacional, o que serve como parâmetro de comparação para a análise dos demais cenários avaliados neste Estudo Técnico Preliminar, em especial aqueles que preveem a contratação de solução pronta disponibilizada por fornecedor especializado.

9.2 Aquisição de Solução de Assinatura Implantada e Operada no Ambiente do TCE-PR

Neste cenário, em que a solução de assinatura digital seria adquirida sob a forma de subscrição e instalada para execução no ambiente computacional do Tribunal, o dimensionamento de quantitativos envolve não apenas o software propriamente dito, mas também os recursos técnicos e operacionais necessários para sua sustentação ao longo do tempo.

Do ponto de vista de recursos humanos, esse cenário pressupõe a atuação recorrente de especialistas técnicos do TCE-PR para garantir a operação contínua da solução, incluindo profissionais com conhecimentos em infraestrutura de servidores, sistemas operacionais, redes e segurança da informação. Esses profissionais não estariam necessariamente alocados de forma exclusiva à solução de assinatura digital, mas teriam participação regular em atividades de instalação, configuração, atualização, monitoramento e tratamento de incidentes.

Adicionalmente, a execução local da solução demanda a disponibilização e manutenção de infraestrutura tecnológica própria, incluindo servidores de aplicação, recursos de armazenamento, conectividade de rede, acesso à internet e mecanismos de segurança, tais como controles de acesso, monitoramento e soluções de proteção contra malware. Ressalta-se, ainda, que a funcionalidade de carimbo de tempo pressupõe a utilização de hardware dedicado, o que implica a provisão e manutenção de equipamentos específicos no ambiente do Tribunal para garantir a operação segura e contínua desse serviço. Seriam necessários, no mínimo, uma equipe contendo 3 (três) desenvolvedores sênior, além do acompanhamento e gestão de 3 (três) servidores efetivos do TCE-PR.

9.3 Aquisição de Solução de Assinatura Implantada e Operada em Ambiente Externo

No cenário em que a solução de assinatura digital é fornecida como serviço (SaaS) e executada integralmente no ambiente da empresa contratada, os quantitativos associados à sua operação restringem-se ao volume de consumo dos serviços de assinatura e validação de documentos, não havendo necessidade de dimensionamento de infraestrutura própria no âmbito do TCE-PR. Com base no histórico de utilização observado no contrato vigente, bem como nos quantitativos previstos nos instrumentos contratuais anteriores, estimou-se um consumo médio mensal da ordem de 56.250 chamadas de assinatura e 81.250 chamadas de validação. Projetando-se esse comportamento para a vigência contratual de 60 meses, obtém-se o total de 3.375.000 chamadas de assinatura digital e 4.875.000 chamadas de validação.

Para fins de planejamento e melhor visualização da demanda, esses quantitativos correspondem a aproximadamente 675.000 assinaturas digitais por ano e 975.000 validações por ano, valores compatíveis com o padrão histórico de consumo do Tribunal e com a quantidade anual anteriormente prevista em contrato, da ordem de 1.100.000 chamadas totais. A estimativa adotada contempla, ainda, margem de segurança para absorver variações sazonais e eventual crescimento da demanda ao longo da execução contratual, mantendo coerência com o comportamento real já verificado.

Ressalta-se que tais quantitativos não implicam qualquer necessidade de ampliação da infraestrutura tecnológica do TCE-PR, uma vez que todos os recursos necessários à execução da solução, incluindo servidores, armazenamento, conectividade, mecanismos de segurança, carimbo de tempo, alta disponibilidade e contingência, são integralmente providos e mantidos pela empresa contratada. Da mesma forma, sob a ótica de recursos humanos, não se verifica a necessidade de alocação de equipes técnicas especializadas para sustentação da solução, restringindo-se a atuação do Tribunal às atividades de fiscalização técnica e administrativa do contrato, acompanhamento dos níveis de serviço e interlocução com a contratada.

10 ESTIMATIVA PRELIMINAR DE PREÇOS

10.1 Desenvolvimento de software assinador de documentos digitais pelo TCE-PR

A estimativa preliminar de preços do Cenário que prevê o desenvolvimento de solução própria de assinatura digital por meio da fábrica de software contratada pelo Tribunal foi elaborada com base nos quantitativos estimados no item anterior e nas práticas adotadas nos contratos de desenvolvimento de software do TCE-PR.

Para fins de dimensionamento, considera-se que a solução possui porte estimado de 1.500 (mil e quinhentos) Pontos de Função, compatível com a complexidade funcional envolvida. Adotando-se o parâmetro de produtividade QMHPF = 10 (dez) horas por Ponto de Função, utilizado como referência institucional, obtém-se um esforço estimado de aproximadamente 15.000 (quinze mil) horas de desenvolvimento, o que corresponde a cerca de 1.875 dias de trabalho ou 7,4 homens-ano de desenvolvedores pleno, considerando o número médio de dias úteis anuais. Esse dimensionamento pressupõe, ainda, a participação de outros perfis profissionais necessários ao ciclo de desenvolvimento, tais como arquiteto de software, profissionais de testes e atividades de gestão de projeto, com dedicação parcial ao longo da execução.

Com base nessas premissas, a estimativa preliminar indica que o custo global, em caráter conservador, para o desenvolvimento interno de uma solução de assinatura digital desse porte seria da ordem de R$ 1.413.000,00 (um milhão, quatrocentos e treze mil reais). Esse valor é apresentado exclusivamente para fins de estimativa preliminar e comparação entre os cenários, nos termos do art. 22, inciso VI, da IS nº 181/2024, sendo suficiente para demonstrar a magnitude do esforço financeiro envolvido neste cenário, sem a necessidade de detalhamento da composição de custos neste Estudo Técnico Preliminar.

10.2 Aquisição de Solução de Assinatura Implantada e Operada no Ambiente do TCE-PR

A estimativa preliminar de preços do cenário em questão prevê a aquisição de solução de assinatura digital sob a forma de subscrição, com execução no ambiente computacional do Tribunal, considera o conjunto de custos necessários à sua disponibilização, operação e sustentação ao longo do tempo, abrangendo não apenas os valores diretamente associados à solução de mercado, mas também os custos indiretos decorrentes de sua internalização no âmbito do TCE-PR.

No que se refere à solução identificada na pesquisa de preços, o custo estimado contempla o licenciamento do software, o suporte técnico associado ao período contratual, bem como a possibilidade de contratação de serviços adicionais, tais como horas de consultoria especializada para apoio à implantação, ajustes, integrações, atualizações ou adequações específicas ao ambiente institucional do Tribunal. Esses elementos são considerados de forma agregada na estimativa, sem detalhamento pormenorizado nesta etapa, por se tratar de análise preliminar simplificada.

Adicionalmente, o cenário pressupõe a manutenção de esforço operacional interno contínuo para a execução, administração e sustentação da solução no ambiente do TCE-PR. Para fins de estimativa preliminar, considera-se a equivalência média de alocação de recursos humanos internos ao longo do horizonte analisado, ainda que, na prática, as atividades sejam distribuídas entre diferentes unidades técnicas, como sustentação de sistemas, segurança da informação, administração de ambientes computacionais, governança de TIC e suporte à infraestrutura.

Nesse contexto, a estimativa global também incorpora, de forma consolidada, os custos administrativos e transacionais associados à gestão do contrato, os custos relacionados à segurança da informação e à proteção de dados, bem como os custos indiretos vinculados à infraestrutura de TIC necessária ao funcionamento da solução, tais como ambientes computacionais, armazenamento, conectividade, mecanismos de segurança, controles de acesso e demais componentes correlatos.

Considerando-se o conjunto desses fatores, o valor estimado para esse cenário, ao longo de um horizonte de cinco anos, é da ordem de R$ 2.820.000,00. Ressalta-se que essa estimativa possui caráter preliminar e é suficiente, no âmbito deste Estudo Técnico Preliminar, para subsidiar a análise comparativa entre os cenários avaliados, atendendo ao disposto no art. 22, inciso VI, da IS nº 181/2024, sem prejuízo de detalhamento posterior na fase de planejamento da contratação.

10.3 Aquisição de Solução de Assinatura Implantada e Operada em Ambiente Externo

A estimativa preliminar de preços do cenário que prevê a contratação de solução de assinatura digital implantada e operada em ambiente externo à infraestrutura do Tribunal foi elaborada com base no modelo de cobrança por uso dos serviços, considerando os volumes médios anuais de assinaturas e validações atualmente demandados pelo TCE-PR.

Para fins de estimativa, adota-se como referência o custo médio unitário de R$ 0,10 (dez centavos) por assinatura digital com carimbo de tempo e R$ 0,06 (seis centavos) por validação de documentos. Considerando-se um volume médio anual estimado de 675.000 (seiscentas e setenta e cinco mil) assinaturas com carimbo de tempo e 975.000 (novecentas e setenta e cinco mil) validações de documentos, obtém-se um custo anual aproximado de R$ 126.000,00 (cento e vinte e seis mil reais).

Projetando-se esse consumo para um horizonte de 5 (cinco) anos, o custo global estimado para a prestação contínua dos serviços de assinatura digital e validação de assinaturas digitais seria da ordem de R$ 630.000,00 (seiscentos e trinta mil reais). Esse valor contempla a execução dos serviços em ambiente externo, incluindo a infraestrutura tecnológica necessária, os mecanismos de segurança, a operação da funcionalidade de carimbo de tempo com hardware dedicado e a manutenção evolutiva da solução no ambiente da fornecedora, sem necessidade de investimentos adicionais em infraestrutura de hospedagem ou em equipe técnica especializada por parte do Tribunal.

Adicionalmente, o cenário considerado pressupõe a necessidade de realização de serviço específico de adaptação das aplicações do Tribunal à solução contratada, de modo a viabilizar a integração técnica com os serviços de assinatura e validação disponibilizados externamente. Para fins desta estimativa preliminar, considera-se um valor aproximado de R$ 50.000,00 (cinquenta mil reais) para a execução do serviço de adaptação, correspondendo a um custo pontual, associado à implantação inicial da solução, abrangendo atividades de integração, testes, ajustes técnicos e adequação às diretrizes arquiteturais e de segurança da informação do TCE-PR.

Dessa forma, considerando o custo estimado da prestação contínua dos serviços (R$ 630.000,00) e o custo estimado do serviço de adaptação (R$ 50.000,00), o valor global estimado para esse cenário é da ordem de R$ **680.000,00 (seiscentos e oitenta mil reais), para o horizonte de 5 (cinco) anos**.

Ressalta-se que a presente estimativa possui caráter preliminar e comparativo, atendendo ao disposto no art. 22, inciso VI, da IS nº 181/2024, sendo suficiente, neste Estudo Técnico Preliminar, para subsidiar a análise entre os cenários avaliados, sem detalhamento da composição dos custos neste momento, os quais serão oportunamente definidos e refinados na fase de planejamento da contratação.

11 JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

A análise dos cenários apresentados neste Estudo Técnico Preliminar indica que a contratação de solução de assinatura digital executada no ambiente da fornecedora (Cenário A3) configura-se como a alternativa tecnicamente adequada e economicamente mais vantajosa para o atendimento da necessidade institucional do Tribunal.

Do ponto de vista econômico, esta solução apresenta custo significativamente inferior quando comparado às alternativas que envolvem o desenvolvimento de solução própria ou à execução da solução no ambiente do Tribunal. Conforme demonstrado no item anterior, o desenvolvimento interno de uma solução de assinatura digital de porte compatível com as necessidades do TCE-PR demandaria investimento elevado, associado a esforço prolongado de desenvolvimento e à alocação de múltiplos perfis técnicos especializados. Em contraste, o modelo de contratação baseado em serviço em nuvem permite a obtenção da funcionalidade necessária por meio de cobrança proporcional ao uso, com custo global substancialmente menor ao longo do horizonte contratual analisado.

Sob a perspectiva técnica e operacional, este cenário também se mostra mais adequado ao contexto institucional. O desenvolvimento de solução própria implicaria prazo estimado de aproximadamente um ano para disponibilização da plataforma, o que não se mostra compatível com a necessidade de continuidade do serviço, considerando o encerramento do contrato vigente no curto prazo. Já a execução local da solução pressupõe a manutenção de infraestrutura própria, a gestão de servidores, armazenamento, conectividade, segurança e hardware dedicado para carimbo de tempo, além da dependência de equipes internas especializadas para operação, atualização e resolução de incidentes, aumentando a complexidade operacional e os riscos associados.

Neste modelo adotado, tais responsabilidades permanecem concentradas na empresa fornecedora da solução, que assume a provisão da infraestrutura, a operação contínua do serviço, a manutenção da segurança, a atualização tecnológica e a gestão de componentes críticos, como o carimbo de tempo com hardware dedicado. Esse arranjo reduz a carga operacional interna, mitiga riscos técnicos e permite que o Tribunal concentre seus esforços em atividades finalísticas, mantendo-se apenas a atuação necessária de fiscalização técnica e administrativa do contrato.

Ademais, a adoção do prazo contratual de 60 (sessenta) meses mostra-se juridicamente adequada e tecnicamente vantajosa, nos termos do art. 106 da Lei nº 14.133/2021, que autoriza a celebração de contratos de serviços contínuos por período de até 5 (cinco) anos, desde que devidamente demonstrada a maior vantagem econômica decorrente da contratação plurianual.

Ainda que as propostas apresentem equivalência de valores quando comparados os prazos de 12 (doze) e 60 (sessenta) meses, a fragmentação contratual implicaria a recorrência de procedimentos administrativos de renovação, com aumento de custos transacionais, esforços operacionais e riscos associados, em prejuízo à economicidade e à eficiência administrativa, princípios expressamente consagrados na Lei nº 14.133/2021. A contratação plurianual, por sua vez, favorece o planejamento tecnológico e orçamentário da Administração, permitindo maior previsibilidade, estabilidade operacional e melhor gestão dos recursos públicos.

Destaca-se, ainda, que sucessivas renovações contratuais tendem a ampliar riscos de descontinuidade do serviço, incompatibilidade tecnológica e perda de integração entre sistemas corporativos. Tais riscos são especialmente relevantes no caso em análise, uma vez que a solução contratada possui caráter essencial e transversal, atendendo a múltiplos sistemas institucionais resilientes que dependem, de forma crítica, de assinaturas eletrônicas em documentos. Nesse contexto, o prazo de 60 (sessenta) meses atende de forma mais adequada ao interesse público, assegurando continuidade do serviço, estabilidade tecnológica e aderência aos objetivos de planejamento e eficiência definidos pelo art. 106 da Lei nº 14.133/2021.

Dessa forma, a escolha deste cenário atende aos critérios de eficácia, ao assegurar a continuidade imediata do serviço; de eficiência, ao reduzir a complexidade operacional e o esforço interno; de efetividade, ao garantir a entrega da funcionalidade necessária com níveis adequados de serviço; e de economicidade, ao apresentar menor custo global quando comparado às demais alternativas analisadas. A solução escolhida revela-se, portanto, a mais vantajosa para a Administração, nos termos do art. 11 da Lei nº 14.133/2021, atendendo ao disposto no art. 22, inciso V, e no art. 22,

inciso XIII, da IS nº 181/2024, bem como ao art. 11, inciso V, da IN nº 94/2022, que exige a declaração da viabilidade da contratação com justificativa fundamentada da solução escolhida.

12 BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

12.1 Bens e serviços que compõe a solução

A solução proposta para atendimento da necessidade identificada neste Estudo Técnico Preliminar é composta por um conjunto integrado e indissociável de bens e serviços, os quais, de forma conjunta, viabilizam a obtenção dos resultados pretendidos pela Administração, nos termos do art. 21 e do art. 22, incisos VII e VIII, da IS nº 181/2024, bem como do art. 18, inciso II, da Lei nº 14.133/2021.

Considerando a alternativa selecionada neste ETP, a solução é composta, de forma exemplificativa e não exaustiva, pelos itens descritos na tabela abaixo:

Lote	Item	Descrição	Métrica	Quantidade (ano)	Valor unitário	Valor total
1	1	Assinatura Digital de documentos, com carimbo de tempo	Chamadas a serviço	675.000	R$??	R$???
	2	Validação de Assinatura Digital de Documentos	Chamadas a serviço	975.000	R$???	R$???
	3	Desenvolvimento de solução adaptativa para integração das aplicações do Tribunal com as soluções descritas nos Itens 1 e 2	Unidade	1	R$???	R$???

O Item 1 refere-se ao serviço de assinatura digital de documentos, executado no ambiente da fornecedora, incluindo obrigatoriamente o uso de carimbo de tempo e a observância dos padrões e normativos aplicáveis da ICP-Brasil. Este serviço compreende, de forma integrada, a geração de assinaturas digitais em múltiplos padrões, o suporte à assinatura de documentos em formato PDF (incluindo os requisitos específicos desse formato, quando aplicável) além da utilização de certificados digitais armazenados em nuvem ou em token físico, desde que em conformidade com a regulamentação vigente. Tais características decorrem diretamente dos requisitos de negócio e técnicos definidos neste Estudo Técnico Preliminar e são consideradas inerentes à solução demandada, não se caracterizando como serviços acessórios ou evoluções contratadas à parte. A estimativa de volumetria considera cerca de 675.000 chamadas ao serviço por ano, conforme projeção de uso institucional.

O Item 2 refere-se ao serviço de validação de assinaturas digitais de documentos, igualmente executado no ambiente da fornecedora, destinado à verificação da autenticidade, integridade, cadeia de certificação, carimbo de tempo e validade jurídica das assinaturas digitais produzidas ou recebidas pelo Tribunal. A estimativa de volumetria considera cerca de 975.000 chamadas ao serviço por ano, compatíveis com os fluxos institucionais de tramitação e análise de documentos eletrônicos.

O Item 3 refere-se, quando necessário, ao desenvolvimento ou adaptação de solução de integração entre os sistemas corporativos do Tribunal e os serviços contratados de assinatura e validação digital. Considerando que o TCE-PR já adota arquitetura baseada no consumo de serviços por meio de interfaces padronizadas e mantém assinador corporativo próprio como camada intermediária, esse item tem por objetivo preservar o modelo arquitetural existente, permitindo a substituição ou atualização da solução contratada sem impactos diretos nas aplicações institucionais. A efetiva necessidade de execução deste item dependerá do grau de compatibilidade da solução ofertada pela empresa vencedora do certame com o modelo de integração atualmente adotado pelo Tribunal, podendo não demandar execução caso a solução já atenda plenamente a esse requisito.

A definição desses elementos considera a solução como um todo funcional, no qual os serviços principais, os serviços complementares e as atividades de integração são essenciais para a adequada execução contratual, evitando fragmentações indevidas do objeto, conforme o disposto no art. 23, §1º, da Lei nº 14.133/2021.

A descrição detalhada de cada item, bem como seus quantitativos definitivos, métricas, níveis de serviço e demais características técnicas, será aprofundada no Termo de Referência, permanecendo este item restrito à identificação da composição estrutural da solução no âmbito deste Estudo Técnico Preliminar.

Apesar de não estarem explicitados os serviços de suporte e manutenção, estes devem estar contemplados no modelo de execução do objeto.

12.2 Vigência do contrato

A vigência inicial do CONTRATO será de **60 (sessenta) meses**, contados da data de publicação do extrato do contrato no Diário Eletrônico do TCE-PR, podendo ser prorrogada por iguais e sucessivos períodos, até o limite máximo de 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, desde que atendidas as condições legais e mantida a vantajosidade para a Administração.

JUSTIFICATIVA: Considerando que a solução de assinatura digital constitui serviço de TIC prestado de forma continuada, integrado a processos institucionais críticos do Tribunal e a sistemas corporativos que demandam estabilidade operacional, a adoção de vigência plurianual mostra-se tecnicamente recomendável. A manutenção prolongada da mesma solução reduz riscos decorrentes de substituições frequentes de fornecedor, preserva o conhecimento acumulado sobre o ambiente tecnológico, favorece o amadurecimento das integrações implementadas e proporciona maior previsibilidade para o planejamento, a gestão e a evolução dos serviços durante toda a execução contratual.

Além dos aspectos técnicos e operacionais, a maior vantagem econômica da contratação plurianual foi demonstrada na Peça de Preços e em seu respectivo Anexo, documentos integrantes do processo administrativo de planejamento da contratação. Conforme análise realizada, a estimativa do valor de referência foi baseada em pesquisa direta junto a fornecedores, considerando cenários de vigência contratual de 12 (doze) e 60 (sessenta) meses, cujos valores foram consolidados a partir da média das propostas válidas recebidas. A comparação entre os cenários evidencia que a contratação plurianual apresenta melhor relação custo-benefício para a Administração, atendendo ao disposto no art. 106, inciso I, da Lei nº 14.133/2021.

Ademais, ainda que os valores unitários apresentados pelos fornecedores fossem equivalentes entre os cenários analisados, a adoção de contratações com vigências reduzidas implicaria a repetição de procedimentos administrativos de renovação ou de nova contratação, elevando custos transacionais, esforços operacionais e riscos associados à descontinuidade dos serviços.

12.3 Qualificação técnica do fornecedor

12.3.1 Para fins de habilitação técnica, visando mitigar riscos de descontinuidade e de execução inadequada do objeto, será exigida da LICITANTE a comprovação de aptidão técnica por meio de atestado(s) de capacidade técnica, nos termos do art. 67 da Lei nº 14.133/2021, emitido(s) por pessoa jurídica de direito público ou privado, que demonstre(m) a execução satisfatória de objeto(s) pertinente(s) e compatível(eis) com o desta contratação.

12.3.2 O(s) atestado(s) deverá(ão) conter, no mínimo, identificação do emitente, descrição do objeto executado, período de execução e manifestação de que os serviços foram prestados de forma satisfatória, em condições que permitam aferir a compatibilidade com o objeto.

12.3.3 Para fins de aceitação e julgamento da compatibilidade do(s) atestado(s) com o objeto licitado, o Termo de Referência estabelecerá critérios objetivos, observando-se que a comprovação poderá ser feita de forma cumulativa, por um ou mais atestados, desde que, em conjunto, demonstrem a aptidão da LICITANTE.

12.3.4 Será considerado compatível o(s) atestado(s) que comprove(m) a prestação de serviços de assinatura digital e/ou validação/verificação de assinaturas digitais, em conformidade com os padrões da ICP-Brasil (ou padrão legalmente aceito no Brasil), contemplando ao menos parte relevante do escopo contratado.

- Será considerado compatível o(s) atestado(s) que demonstre(m) a disponibilização do serviço por meio de interfaces de integração (APIs/Webservices), utilizadas por sistemas/aplicações de terceiros para consumo das operações de assinatura e/ou validação.
- Será considerado compatível o(s) atestado(s) que evidencie(m) a operação do serviço em ambiente externo ao CONTRATANTE (ex.: nuvem/ambiente do fornecedor) ou em modelo equivalente de prestação continuada, com responsabilidades do fornecedor por operação, manutenção e atualização.
- Para demonstração de capacidade operacional, o(s) atestado(s) deverá(ão) indicar que a execução ocorreu de forma satisfatória, com suporte técnico e manutenção durante a vigência, incluindo atendimento a níveis de serviço (quando informados pelo emitente) e/ou disponibilidade compatível com o caráter crítico do serviço.
- Quando disponíveis no(s) atestado(s), serão aceitos como elementos de reforço à análise de compatibilidade: volume de transações (assinaturas/validações), número de usuários/sistemas integrados e uso de carimbo do tempo (quando aplicável), sem que tais informações constituam requisito mínimo obrigatório.
- Não será considerado compatível com o objeto licitado, para fins de comprovação de capacidade técnica, o(s) atestado(s) que se enquadre(m) em qualquer das situações a seguir:
- atestado(s) referente(s) exclusivamente a fornecimento de certificados digitais (emissão/renovação), sem a prestação de plataforma/serviço de assinatura e/ou validação integrada a sistemas;
- atestado(s) de digitalização, GED, workflow ou solução documental genérica que não comprove(m), de forma clara, a execução de serviços de assinatura digital e/ou validação de assinaturas;
- atestado(s) restrito(s) a assinatura eletrônica não qualificada (ex.: aceite por e-mail, login/senha, clique), sem mecanismos criptográficos e sem comprovação de aderência a padrão normativo aplicável à validade jurídica pretendida;
- atestado(s) de desenvolvimento de software ou serviços de TI genéricos, sem correlação direta com assinatura digital, verificação de assinaturas, carimbo do tempo ou cadeia de confiança equivalente;
- atestado(s) que não indique(m) claramente o objeto executado, o período de execução e a identificação do emitente, ou que não permita(m) aferir a execução satisfatória do serviço.

A exigência de qualificação técnica será definida no Termo de Referência de forma proporcional e não restritiva, admitindo-se a apresentação de um ou mais atestados que, em conjunto, comprovem a aptidão para o desempenho de atividade pertinente e compatível com o objeto, preservada a competitividade do certame e a finalidade de mitigação de riscos inerentes a serviço essencial e contínuo.

12.4 Parcelamento do Objeto

12.4.1 A avaliação quanto ao parcelamento do objeto foi realizada à luz do art. 23, §1º, da Lei nº 14.133/2021 e do art. 22, inciso VIII, da IS nº 181/2024, considerando-se a viabilidade técnica, a vantajosidade econômica e os impactos na gestão e continuidade do serviço, conforme boas práticas indicadas pela IN nº 94/2022.

Considerando a solução definida neste Estudo Técnico Preliminar — composta por serviços de assinatura digital com carimbo do tempo, validação de assinaturas digitais e atividades de integração/adaptação ao assinador corporativo do TCE-PR— conclui-se que há forte interdependência técnica e operacional entre esses componentes, pois:

- a assinatura e a validação devem operar de forma integrada e consistente (mesmas políticas, cadeia de confiança, carimbo do tempo e requisitos de disponibilidade), sob pena de retrabalho, inconsistências e riscos à segurança jurídica dos documentos;
- a integração com o assinador corporativo e com as aplicações institucionais demanda alinhamento de interfaces, suporte coordenado e tratamento unificado de incidentes, o que é dificultado quando há múltiplos fornecedores com responsabilidades fracionadas;
- a necessidade de continuidade do serviço (caráter essencial e transversal) recomenda a concentração de responsabilidades por operação, suporte, monitoramento e evolução, reduzindo riscos de indisponibilidade e disputas de responsabilidade entre contratadas;
- a governança contratual, a fiscalização e a apuração de níveis de serviço (NMS/IMR) tornam-se mais objetivas quando os indicadores e a cadeia de prestação do serviço se encontram sob um mesmo arranjo contratual.

Dessa forma, embora seja possível discriminar os componentes da solução *para fins de mensuração, precificação e controle* (itens de planilha/itens de faturamento), a contratação não deve ser parcelada em lotes independentes com adjudicação a fornecedores distintos, por não se mostrar tecnicamente recomendável nem economicamente vantajosa no contexto desta contratação. A adoção de lote único (solução integrada) preserva a competitividade do certame ao permitir a participação de fornecedores especializados que ofertem a solução como serviço, ao mesmo tempo em que reduz riscos de integração, facilita a responsabilização e reforça a continuidade operacional.

CONCLUSÃO: Adota-se, para o Termo de Referência, o não parcelamento do objeto (lote único), nos termos do art. 23, §1º, da Lei nº 14.133/2021, registrando-se que a eventual separação em itens terá finalidade exclusivamente gerencial (mensuração e acompanhamento), sem fracionamento da responsabilidade pela entrega dos resultados pretendidos.

12.5 Da Aceitação ou Não de Consórcio e Cooperativas

12.5.1 Para esta contratação, não será admitida a participação de licitantes constituídas sob a forma de consórcio.

JUSTIFICATIVA: o objeto consiste na prestação continuada de serviços de plataforma de assinatura digital/validação, com responsabilidades integradas de operação, suporte, manutenção e atualização tecnológica, exigindo interlocução técnica e responsabilização unificada. A participação em consórcio tende a aumentar a complexidade de governança, fiscalização e apuração de responsabilidades, com risco de fragmentação do atendimento, especialmente em situações de indisponibilidade, incidentes de segurança e cumprimento de níveis mínimos de serviço (NMS/IMR).

12.5.2 Adicionalmente, a vedação não compromete a competitividade do certame, pois o mercado dispõe de fornecedores que, isoladamente, têm condições de atender às exigências de habilitação técnica e econômico-financeira e de executar o objeto de ponta a ponta, conforme evidenciado por contratações similares e práticas observadas no setor.

12.5.3 O entendimento acima está alinhado às diretrizes de planejamento da contratação de TIC (IN nº 94/2022), que recomendam avaliar os riscos de execução e a gestão contratual (incluindo consórcio/subcontratação), bem como à Lei nº 14.133/2021, que admite a participação em consórcios, porém condiciona sua aceitação ao juízo de conveniência e oportunidade da Administração, motivado no processo.

12.5.4 Assim, a opção por vedar consórcios busca mitigar riscos de execução e assegurar maior previsibilidade na gestão e fiscalização, mantendo-se compatível com os princípios da eficiência, da segurança jurídica e da seleção da proposta mais vantajosa.

12.5.5 **Cooperativas**: não será admitida a participação de cooperativas de trabalho quando a execução do objeto demandar, na prática, intermediação de mão de obra com pessoalidade, habitualidade e subordinação direta ao CONTRATANTE, situação incompatível com a natureza do modelo cooperativo e com o regime de contratação pretendido. Caso, no detalhamento do Termo de Referência, reste demonstrado que o objeto pode ser executado sem tais elementos, a Administração poderá reavaliar a vedação, com a devida motivação.

12.6 Subcontratação e Alteração Subjetiva

12.6.1 Fica vedada a subcontratação total do objeto da contratação, bem como a subcontratação dos serviços essenciais relacionados à operação, disponibilização e gestão da solução de assinatura digital e validação de assinaturas digitais, tendo em vista a necessidade de assegurar a unicidade de responsabilidade técnica e contratual, a segurança da informação e a continuidade dos serviços.

12.6.2 Admite-se a subcontratação parcial do serviço de adaptação das aplicações do Tribunal à solução contratada, desde que tal subcontratação não comprometa a governança da solução, a integração entre os componentes contratados e o adequado atendimento aos requisitos técnicos e funcionais estabelecidos.

12.6.3 Na hipótese de subcontratação, a contratada permanecerá integralmente responsável pela execução do objeto, cabendo-lhe a coordenação técnica das atividades, a garantia de qualidade dos serviços prestados e o cumprimento de todas as obrigações contratuais perante o Tribunal.

12.6.4 A possibilidade de subcontratação da adaptação visa preservar a flexibilidade técnica para implementação da integração com os sistemas do Tribunal, sem prejuízo da responsabilidade centralizada da contratada pela solução como um todo.

12.6.5 No que se refere à alteração subjetiva, admite-se a fusão, cisão ou incorporação da contratada com ou por outra pessoa jurídica, desde que sejam mantidos os requisitos de habilitação exigidos na contratação, não haja prejuízo à execução contratual, sejam preservadas as condições pactuadas e haja anuência expressa da Administração.

13 INSTRUMENTO DE MEDIÇÃO DE RESULTADO (IMR) e NÍVEIS MÍNIMOS DE SERVIÇOS (NMS)

A execução contratual deverá adotar Instrumento de Medição de Resultado (IMR), de modo que o pagamento dos serviços esteja vinculado à efetiva prestação, à conformidade com os níveis mínimos de serviço e ao atendimento dos requisitos de qualidade definidos no Termo de Referência, em alinhamento às boas práticas de contratação de soluções de TIC.

14 INTERDEPENDÊNCIA COM OUTRAS CONTRATAÇÕES

14.1 Relação com o Contrato n.º 07/2026 (Desenvolvimento de Software):

O Contrato n.º 07/2026 tem como objeto a contratação de serviços técnicos especializados para o desenvolvimento e manutenção de soluções de software. Tais serviços visam desenvolver novas soluções, além de evoluir, aprimorar e modernizar a estrutura tecnológica do Tribunal de Contas do Estado do Paraná (TCE-PR).

É fundamental que os serviços de assinatura estejam alinhados às práticas de desenvolvimento estabelecidas pelo TCE-PR, garantindo que as soluções implementadas sigam padrões técnicos e metodológicos adotados pela instituição. Isso assegura a integração eficiente entre os sistemas, a conformidade com requisitos internos e o atendimento às necessidades específicas do Tribunal.

Além disso, destaca-se a existência de uma interdependência entre a solução de assinatura objeto deste estudo e o desenvolvimento das aplicações contratadas. Essa interdependência implica que qualquer evolução, aprimoramento ou implementação de funcionalidades relacionadas à assinatura digital deve considerar as diretrizes técnicas e os fluxos de trabalho definidos no âmbito do Contrato n.º 07/2026, promovendo sinergia entre as equipes e soluções envolvidas.

14.2 Relação com o Contrato n.º 02/2026 (Certificados Digitais):

A utilização dos certificados digitais, conforme previsto no Contrato n.º 02/2026, é essencial para garantir que a assinatura de documentos pelos servidores e membros do Tribunal de Contas do Estado do Paraná ocorra de forma segura e conforme as exigências técnicas dos sistemas internos. Para que o processo de assinatura seja eficiente, é fundamental que a solução adotada pelo TCE-PR seja compatível e integrada com todas as plataformas de certificados digitais em uso. Essa integração assegura que as assinaturas realizadas estejam alinhadas com os padrões de segurança e autenticidade exigidos, evitando incompatibilidades e garantindo a validade jurídica dos documentos assinados eletronicamente.

A correlação entre os certificados digitais utilizados pelo Tribunal de Contas e as assinaturas emitidas é um ponto de atenção indispensável. A escolha de uma solução de assinatura que reconheça e utilize corretamente os certificados contratados permite não apenas a operacionalização eficiente dos processos internos, mas também a conformidade com os requisitos legais e técnicos. Dessa forma, todos os documentos assinados eletronicamente contam com a autenticidade e integridade garantidas por certificados confiáveis, fortalecendo a transparência e a segurança institucional.

Por fim, destaca-se uma distinção relevante entre Certificado Digital (abordado no Contrato n.º 02/2026) e a Assinatura Digital (tema deste estudo). O Certificado Digital refere-se a um arquivo eletrônico que funciona como identidade virtual para pessoas físicas ou jurídicas, sendo classificado como um produto em termos de aquisição. Por outro lado, a Assinatura Digital constitui um método baseado em criptografia que vincula o certificado digital do signatário ao documento eletrônico assinado, caracterizando-se como um serviço conforme a análise deste ETP.

14.3 Relação com o Contrato n.º 36/2024 (Novo Trâmite):

A construção do sistema Novo Trâmite, prevista no Contrato n.º 36/2024, demanda serviços técnicos especializados para garantir a tramitação eficiente de documentos, processos e procedimentos tanto internos quanto externos. Um dos pontos centrais é a utilização de assinaturas digitais, que asseguram a autenticidade e integridade das informações processadas.

Para que o Novo Trâmite opere adequadamente, torna-se indispensável que haja interoperabilidade e compatibilidade com as soluções de assinatura digital analisadas neste estudo. Essa integração permite que todos os fluxos documentais sejam realizados de maneira segura, conforme os requisitos técnicos estabelecidos e alinhados com as demais contratações relacionadas.

A interoperabilidade entre o sistema Novo Trâmite e as soluções de assinatura digital é fundamental para a tramitação eletrônica de documentos, garantindo a validação jurídica, integridade e autenticidade dos processos jurisdicionais e administrativos. Dessa forma, o objeto do presente estudo se revela essencial para a efetivação dos objetivos do Contrato n.º 36/2024, viabilizando a transformação digital e a segurança documental no âmbito do Tribunal de Contas do Estado do Paraná.

14.4 Relação com o Contrato n.º 15/2024 (Sustentação de Software):

O Contrato n.º 15/2024 tem como finalidade a contratação de uma empresa especializada para a prestação de serviços técnicos voltados à sustentação de software. Essa atuação é fundamental para garantir a estabilidade e o correto funcionamento das aplicações do Tribunal de Contas do Estado do Paraná (TCE-PR).

Os serviços de sustentação mantêm as aplicações do TCE-PR estáveis, assegurando que os sistemas estejam operacionais e aptos a atender as demandas institucionais. A utilização de assinaturas digitais em diferentes módulos e soluções do tribunal é uma característica central, pois reforça a segurança e autenticidade dos documentos processados eletronicamente.

A compatibilidade e interoperabilidade entre as manutenções e evoluções realizadas pelos serviços de sustentação de software e o objeto deste Estudo Técnico Preliminar (ETP) são essenciais. Esse alinhamento permite que as soluções de assinatura digital estejam integradas aos sistemas mantidos, garantindo a continuidade das operações e atendendo aos requisitos técnicos e jurídicos necessários para a tramitação eletrônica de documentos.

Por fim, destaca-se uma distinção relevante entre serviços de desenvolvimento de software (Contrato n.º 07/2026) e serviços de sustentação de software (Contrato n.º 15/2024), conceitos que, embora relacionados ao ciclo de vida dos sistemas, possuem naturezas e finalidades distintas.

Os serviços de desenvolvimento de software compreendem o conjunto de atividades voltadas à criação de novos sistemas ou à evolução significativa de soluções existentes, mediante a implementação de novas funcionalidades ou alterações estruturais relevantes, sendo usualmente tratados como demandas de projeto e remunerados com base em métricas de produtividade, como ponto de função. Por outro lado, os serviços de sustentação de software concentram-se na manutenção do software em ambiente de produção, com foco na garantia de disponibilidade, estabilidade, desempenho e atendimento a incidentes, caracterizando-se como uma atividade contínua e operacional, normalmente enquadrada como serviço recorrente e remunerada de forma fixa, vinculada ao cumprimento de níveis mínimos de serviço estabelecidos no contrato.

15 NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

A análise da solução identificada neste Estudo Técnico Preliminar indica que não há necessidade de adequações estruturais relevantes no ambiente tecnológico do Tribunal de Contas do Estado do Paraná para a execução da contratação, considerando que a solução de assinatura digital será prestada, predominantemente, no modelo de serviço, com integração aos sistemas institucionais por meio de interfaces padronizadas.

Eventuais ajustes no ambiente do Tribunal, quando necessários, restringem-se a configurações pontuais, parametrizações ou adaptações de natureza lógica, relacionadas à integração da solução contratada aos sistemas existentes, à adequação de fluxos operacionais ou ao atendimento de requisitos de segurança da informação e governança institucional, não demandando investimentos significativos em infraestrutura adicional.

A eventual realização desses ajustes será avaliada no contexto do planejamento da contratação e da solução efetivamente adotada, observados os princípios do planejamento adequado, da economicidade e da proporcionalidade, nos termos da Lei nº 14.133/2021, em especial os dispositivos relacionados à estimativa de preços e ao planejamento da contratação (arts. 18, inciso VI, e 23).

As diretrizes estabelecidas na Instrução Normativa IS nº 181/2024, notadamente aquelas relativas à identificação de impactos da contratação e à suficiência do ambiente para execução contratual (art. 22), bem como as disposições da IN nº 94/2022, que tratam da fase de planejamento da contratação e da estimativa preliminar do valor (art. 10), foram consideradas na avaliação ora realizada.

Eventuais necessidades específicas de adequação do ambiente, caso identificadas em função da solução contratada ou do modelo de prestação dos serviços, serão detalhadas no Termo de Referência, de forma compatível com os resultados da pesquisa de preços e com a estimativa do valor da contratação, sem prejuízo da continuidade dos serviços institucionais.

16 ESTRATÉGIA DE CONTINUIDADE EM CASO DE INTERRUPÇÃO CONTRATUAL

16.1 As ações abaixo descritas serão adotadas nos casos de descontinuidade, por cancelamento ou inexecução.

TIPO AÇÃO	AÇÃO	RESPONSÁVEL
Ação Preventiva	Acompanhar continuamente a execução contratual, por meio de atividades de gestão e fiscalização, visando identificar antecipadamente riscos à continuidade dos serviços de assinatura digital	Gestor do Contrato e Fiscais
Ação de Preparação	Manter documentação técnica atualizada, registros de integrações e informações essenciais à operação da solução, de modo a permitir rápida tomada de decisão em caso de interrupção ou transição contratual	Gestor do Contrato
Ação de Contingência - Início da Execução Contratual	Caso sejam identificadas falhas iniciais relevantes na prestação do serviço, adotar medidas administrativas para correção tempestiva, conforme previsto no instrumento contratual, preservando a continuidade dos serviços institucionais	Gestor do Contrato
Ação de Contingência – Execução Contratual	Em caso de interrupção parcial ou total da prestação dos serviços, acionar os mecanismos contratuais previstos, avaliar soluções alternativas temporárias e adotar providências visando mitigar impactos aos sistemas e processos institucionais	Gestor do Contrato e Fiscais
Ação de Contingência – Execução Parcial do Contrato	Avaliar a possibilidade de manutenção temporária de funcionalidades essenciais, priorizando os serviços críticos de assinatura e verificação de assinaturas digitais, até a regularização da situação contratual	Gestor do Contrato
Ação de Transição	Na hipótese de encerramento ou rescisão contratual, adotar as providências necessárias para a transição controlada da solução, garantindo a preservação das informações, a continuidade dos serviços essenciais e a minimização de impactos às atividades do Tribunal	Gestor do Contrato

17 IMPACTOS AMBIENTAIS E MEDIDAS MITIGADORAS

A análise da solução objeto deste Estudo Técnico Preliminar indica que a contratação não enseja impactos ambientais relevantes, considerando que se trata de solução predominantemente prestada na forma de serviço, com natureza essencialmente digital, sem demanda por obras, intervenções físicas, consumo significativo de recursos naturais ou geração relevante de resíduos.

Não se identificam, portanto, medidas mitigadoras específicas a serem adotadas, além da observância das diretrizes gerais de sustentabilidade e responsabilidade ambiental já praticadas pelo Tribunal e aplicáveis às contratações públicas, nos termos da Lei nº 14.133/2021, art. 11, inciso IV, e da Instrução Normativa IS nº 181/2024, art. 22, inciso XII.

18 DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Com base nas análises realizadas neste Estudo Técnico Preliminar, conclui-se que a contratação de solução de plataforma corporativa de assinatura digital é tecnicamente viável, economicamente adequada e compatível com o interesse público, atendendo às necessidades institucionais do Tribunal de Contas do Estado do Paraná.

Do ponto de vista técnico, a solução identificada mostra-se compatível com a arquitetura tecnológica adotada pelo Tribunal, com capacidade de integração aos sistemas corporativos existentes e aderência aos requisitos de negócio, técnicos, de segurança e normativos previamente definidos, assegurando a continuidade e a confiabilidade dos serviços de assinatura digital.

Sob o aspecto econômico, a contratação revela-se adequada, considerando a estimativa preliminar de preços e os resultados da pesquisa de mercado realizada, em conformidade com os princípios da economicidade, da eficiência e do planejamento, nos termos da Lei nº 14.133/2021, art. 18, caput, e das diretrizes estabelecidas na Instrução Normativa IS nº 181/2024, art. 22, inciso XIII.

Dessa forma, restam atendidos os pressupostos necessários à continuidade do processo de contratação, mediante a elaboração do correspondente Termo de Referência, observadas as diretrizes e conclusões consolidadas neste Estudo Técnico Preliminar.

19 APÊNDICE A - DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA SOLUÇÃO

19.1 Requisitos técnicos

O serviço de assinatura digital e/ou validação de assinatura digital refere-se à solução de Tecnologia de Informação de Comunicação (TIC) responsável por realizar o processamento de assinatura digital em documentos, bem como a verificação detalhada das conformidades necessárias para validação de assinaturas digitais.

O serviço de implantação e adaptação da solução refere-se à construção de solução de software com objetivo de adaptar a interface de comunicação entre a solução a ser construída ou adquirida e a solução atualmente utilizada pelo Tribunal para comunicar-se com os serviços atualmente contratados.

O objeto deste estudo, que inclui os serviços descritos nos dois parágrafos anteriores, compreende as funcionalidades, licenças e serviços descritos na Tabela 1, na forma de requisitos de alto nível. A primeira coluna indica o número do requisito de alto nível, utilizado para referências neste documento; a segunda coluna indica o nome do requisito, e a terceira coluna indica seu mnemônico, que será usado deste ponto em diante.

Requisito	DESCRIÇÃO DA FUNCIONALIDADE/LICENÇA	MNEMÔNICO
1	Assinatura Digital de Documentos (unitário e em lote)	FADD
2	Validação de Assinatura Digital de Documentos	FVADD
3	Validação de Certificado Digital	FVCD
4	Gerenciamento de Lista de Certificados Revogados – LCR	FGLCR
5	Carimbo de Tempo	FCT
6	Conjunto de API[1]s que permitam a realização de chamadas de serviços para a execução dos serviços descritos nos itens 1 a 3 desta tabela.	FLAPI
7	Licença de Software para Execução de Assinaturas Digitais Via Navegadores Web	FLSAW
8	Licença de Componente para Execução, no Servidor de Aplicações, de Assinaturas Digitais com Suporte a Certificados A1	FLSA1
9	Serviço de adaptação para integração das aplicações do Tribunal com a solução contratanda	SAISC

Tabela 1 - Funcionalidades da solução contratada

Os requisitos técnicos são descritos em detalhes nas seções que seguem. Inicialmente são descritos os requisitos que devem ser atendidos por todas as funcionalidades esperadas da solução, e em seguida são apresentados os requisitos específicos de cada funcionalidade.

19.2 Requisitos genéricos da solução

Requisito 1: a solução deve estar em conformidade com a políticas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil para certificação de documentos.

Requisito 2: a solução e todos os seus componentes devem estar acompanhados de garantia, suporte técnico e atualizações tecnológicas.

Requisito 3: todas as interfaces, mensagens e indicativos textuais das soluções devem ser exibidos no idioma português.

Requisito 4: dúvidas com relação ao mecanismo de execução dos serviços e consulta sobre a melhor arquitetura de soluções para otimização do desempenho da solução no uso dos serviços devem ser sanados via chamado de serviço e/ou suporte telefônico e/ou chamada de vídeo e, em última instância, em encontro presencial.

[1] API é um conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por aplicativos que **não pretendem envolver-se** em detalhes da implementação do software, mas apenas usar seus serviços (Wikipedia, 2021, grifo nosso).

19.3 FADD – Requisitos da Funcionalidade de Assinatura Digital de Documentos

Requisito 5: a FADD deverá permitir a geração de assinaturas no padrão brasileiro de assinatura digital, nos formatos PAdES, CAdES e XAdES, de acordo com as políticas de assinatura definidas no DOC-ICP-15.03 da ICP-Brasil.

Requisito 6: a FADD deverá permitir as representações *attached* e *detached* por meio da codificação DER para o padrão CAdES, em formato PKCS#7, bem como as representações *enveloped*, *enveloping* e *detached* para o padrão XAdES.

Requisito 7: a FADD deverá ser capaz de gerar assinaturas simples, coassinaturas[2] e contra-assinaturas[3].

Requisito 8: a assinatura de documentos deverá ser executada em três etapas:

Etapa 1: geração do *hash* de informações a serem cifradas (FADD, FLAPI);

Etapa 2: cifragem do *hash* produto da Etapa 1 (FLSAW, FLSA1, FLSASN , ou por serviço de assinatura remota com certificado em nuvem, quando aplicável, conforme requisitos específicos definidos na seção FLAPI);

Etapa 3: geração do arquivo assinado (FADD, FLAPI).

Requisito 8-A: Para documentos no formato PAdES (PDF), deverá ser disponibilizado um módulo de manipulação de PDF a ser executado em ambiente computacional sob responsabilidade do CONTRATANTE (ex.: servidor de aplicações), com a finalidade de criar e/ou validar assinaturas extraindo e produzindo as informações necessárias (especialmente *hashes*) sem necessidade de expor o conteúdo integral do arquivo ao serviço remoto do fornecedor, exceto nos casos de contingência previstos neste requisito.

Esse módulo deverá:

a) Oferecer as seguintes funcionalidades mínimas:

- Adicionar assinatura PAdES, com ou sem elemento visual associado, conforme parâmetros fornecidos pela aplicação do CONTRATANTE, a partir do PDF original e dos dados da nova assinatura, incluindo cenários de assinaturas múltiplas/seriais, conforme definições do padrão PAdES.
- Obter assinaturas existentes no documento e retornar tabela contendo, para cada assinatura, o algoritmo de hash associado; e o hash calculado sobre o conteúdo assinado, utilizando o respectivo algoritmo.

[2] Também conhecida como assinaturas paralelas (ver item 1.4 em https://bityli.com/Vjxvx)

[3] Também conhecida como assinaturas em série (ver item 1.4 em https://bityli.com/Vjxvx)

- Calcular o hash do conteúdo a ser assinado, utilizando algoritmo de hash informado pela aplicação do CONTRATANTE (além dos hashes associados às assinaturas já existentes).

b) Ser disponibilizado em uma das seguintes formas equivalentes (não cumulativas)

(i) Serviço HTTPS hospedado e executado em ambiente do CONTRATANTE, preferencialmente com processamento baseado em streams, sem necessidade de manipulação do arquivo integral em memória, devendo ser disponibilizado por meio de contêiner Docker; ou

(ii) Biblioteca .NET (C# Standard) fornecida pela CONTRATADA, dependente apenas de componentes *open source* ou de componentes de terceiros cujo licenciamento para uso seja integralmente provido e mantido pela CONTRATADA, sem ônus adicional ao CONTRATANTE.

c) Requisitos de desempenho e uso de recursos:

- Permitir o processamento de arquivos em paralelo;
- Limitar, caso necessário o uso de memória RAM para o processamento do PDF, o consumo de memória a até 3 (três) vezes o tamanho do arquivo manipulado.
- Suportar arquivos de tamanho até, no mínimo, 1 GB.
- Permitir o processamento de, no mínimo, 20 arquivos em paralelo.
- O tempo de processamento do PDF será contabilizado como parte do processo de assinatura será contabilizada nos requisitos de tempo estabelecidos para a execução dessa funcionalidade.

d) Suporte, manutenção e atualização Deverá oferecer suporte e atualização necessários à manutenção do serviço HTTPS ou biblioteca .NET para:

- corrigir falhas funcionais ou de segurança;
- disponibilizar melhorias;
- adequar-se às atualizações do ambiente;
- adequar-se às atualizações dos padrões de assinatura PDF/PAdES e normativos aplicáveis no âmbito do ITI/ICP-Brasil, quando aplicável.

A indisponibilidade do módulo em virtude dos motivos listados nesse tópico, ainda que utilizando o serviço de contingência, será considerada indisponibilidade do serviço e estará sujeita aos prazos definidos nos requisitos de qualidade.e) Contingência (fallback): Para o caso de falha ou indisponibilidade no uso do módulo local, a manipulação do arquivo para assinatura ou validação poderá ser executada via API em servidor remoto durante o período de manutenção/contingência. O serviço remoto oferecido pelo fornecedor deverá suportar arquivos de tamanho até, no mínimo, 200 MB.

Requisito 9: a FADD deverá oferecer serviço REST para execução da Etapa 1 da assinatura em 3 etapas (*Requisito 8:* Requisito 8) dado:

- entrada: *hash* do arquivo, o algoritmo gerador do *hash* e o certificado do signatário;
- saída: *hash* de informações para cifragem (Etapa 2) e geração da assinatura (Etapa 3).

Requisito 10: a FADD deverá oferecer serviço REST para execução da Etapa 3 da assinatura em 3 etapas (*Requisito 8:*Requisito 8*)* dado:

- entrada: o *hash* da assinatura cifrado (produto da Etapa 2 do *Requisito 8:*Requisito 8), o certificado público do signatário e, nos casos aplicáveis aos padrões CAdES e XAdES, o arquivo pkcs12 detachado para cenários de co-assinatura ou contra-assinatura;
- saída: assinatura no formato aplicável ao padrão utilizado. Para padrões *detached* (ex.: CAdES/CMS), a saída deverá ser assinatura detachada. Para o caso de documentos PAdES, no fluxo normal, a saída deverá consistir nos dados de assinatura necessários à conclusão do empacotamento local do PDF (ex.: hash assinado, algoritmos utilizados e metadados), cabendo ao módulo local descrito nos requisitos específicos de PAdES a geração do artefato final. Excepcionalmente, em situações de falha ou indisponibilidade do módulo local, a saída poderá contemplar o documento PDF assinado (artefato final), nos termos do mecanismo de contingência previsto nos requisitos específicos.

Requisito 11: é necessária a disponibilização de biblioteca em C# ou, alternativamente, serviço HTTPS, executado em ambiente sob responsabilidade do CONTRATANTE por meio de contêiner Docker, destinado à interpretação e, quando tecnicamente viável, à conversão do resultado da assinatura entre representações compatíveis (attached/detached) do padrão CAdES, observadas as limitações técnicas inerentes a cada padrão e as políticas aplicáveis da ICP-Brasil.

Requisito 12: a FADD deverá incluir carimbos de tempo nas assinaturas digitais geradas segundo as regulamentações e padrões da ICP-Brasil (DOC-ICP 15) e RFC 3161, utilizando certificado emitido por uma Autoridade de Carimbo do Tempo (ACT) certificada pela ICP-Brasil.

Requisito 13: a FADD deverá verificar a validade do certificado digital do signatário e sua correspondente cadeia de certificação no momento da geração da assinatura digital.

Requisito 14: a FADD deverá gerar a assinatura digital sem requerer a exportação da chave privada do signatário do repositório seguro onde ela estiver armazenada.

Requisito 14A: O uso de certificados digitais em nuvem tem por objetivo permitir que, mediante credenciais e autorização do usuário, o CONTRATANTE consiga processar assinaturas digitais em seus servidores de aplicação com maior autonomia e previsibilidade operacional, reduzindo limitações heterogêneas impostas por sistemas operacionais, navegadores e hardwares.

Considerando que o ITI não impõe aos Prestadores de Serviço de Confiança (PSC) uma API padronizada e intercambiável, a solução deverá disponibilizar um serviço unificador que centralize, em uma única API, a comunicação com PSCs homologadas, de modo a padronizar o consumo pelo CONTRATANTE.

Esse serviço unificador deverá prover, no mínimo:

a) Descoberta de PSCs com certificados válidos do usuário:

- Dadas informações do usuário, retornar uma lista de PSCs que possuam certificados válidos associados ao usuário.

É obrigatório suportar PSCs homologadas pelo ITI à época da contratação, bem como PSCs que venham a ser homologadas durante a vigência contratual, observada a viabilidade técnica e o processo de atualização da solução.

b) Obtenção assíncrona de autorização/credenciais para assinatura:

- Dadas informações do usuário e a PSC selecionada, solicitar à PSC a emissão de credenciais transitórias/tokens de autorização necessários para uso dos serviços de assinatura/criptografia.

A obtenção dessas credenciais deverá ocorrer mediante autenticação e autorização do usuário por meios próprios da PSC, conforme responsabilidades regulamentadas pelo ITI no DOC-ICP-17.

A operação deverá ser assíncrona, com suporte a webhook e/ou polling, permitindo acompanhamento do estado e resultado.

c) Obtenção do certificado público do usuário:

- Dadas informações do usuário e a PSC selecionada, o serviço deverá retornar o certificado público do usuário (e metadados mínimos necessários), para uso em registros e validações em sistemas do CONTRATANTE.

d) Assinatura de hash (criptografia remota):

- Dadas as credenciais transitórias do usuário, um hash (array de bytes) e a indicação do(s) algoritmo(s) de hash, o serviço deverá solicitar à PSC a geração da assinatura digital do hash.

Em nenhum momento a solução poderá ter acesso à chave privada do usuário final, a qual deverá permanecer sob custódia exclusiva da PSC.

A assinatura de hash poderá ser utilizada isoladamente ou integrada ao fluxo de assinatura documental definido pelos requisitos da funcionalidade FADD, quando aplicável.

e) Regras gerais de conformidade

Por se tratar de etapa integrante do processo de assinatura de documentos, os serviços descritos neste requisito deverão respeitar as restrições e exigências estabelecidas na seção FADD e os demais requisitos não funcionais aplicáveis (segurança, auditoria, disponibilidade, suporte e atualização).

Requisito 15: a FADD deverá atender a, no mínimo, 100 solicitações de assinatura por segundo, tendo como referência assinaturas executadas com certificado digital de chave RSA 2048 bits e algoritmo de *hash* SHA256 para assinatura padrão CAdES.

19.4 FVAAD – Requisitos da Funcionalidade de Validação E VERIFICAÇÃO de Assinatura Digital de Documentos

Requisito 16: a FVADD deverá seguir as regulamentações e padrões da ICP-Brasil (DOC-ICP 15).

Requisito 17: a FVADD deverá ser capaz de validar qualquer formato de uma assinatura digital dos padrões CMS, PAdES, CAdES e XAdES.

Requisito 18: a FVADD deverá fornecer serviço REST cuja interface responda minimamente a:

- entrada: apenas a assinatura detachada e os *hashes* do arquivo codificados segundo o algoritmo determinado por cada assinatura presente na assinatura em validação;
- saída: resultado da validação conforme requisitos a seguir.

Para documentos no formato PAdES, quando aplicável, os hashes e demais dados necessários à validação poderão ser extraídos localmente a partir do arquivo PDF, por meio do serviço/biblioteca de manipulação de PDF fornecido e mantido pela CONTRATADA, conforme requisito específico de PAdES (Requisito 8 A), de modo que o conteúdo integral do arquivo não precise ser exposto ao serviço remoto.

Requisito 19: a FVADD deverá validar o certificado digital (válido, inválido revogado, expirado) no ato da conferência da assinatura, respeitada a data e hora da assinatura.

Requisito 20: para cada assinatura digital, a FVADD deverá permitir que seja visualizada a situação da verificação juntamente com descrição do erro caso a assinatura digital não seja válida.

Requisito 21: a descrição de erros em assinaturas deve diferenciar e, se necessário, enumerar a ocorrência de erros de integridade na assinatura, padrão e política da assinatura.

Requisito 22: quando a assinatura a ser validada possuir carimbo do tempo associado, a referência temporal a ser considerada para as validações necessárias deverá ser a data presente no carimbo do tempo.

Requisito 23: na ausência do carimbo do tempo, a FVADD deve efetuar a validação, condicionada à validade do certificado do signatário, considerando a data e local do signatário indicada na assinatura do documento.

Observação: Nos casos em que a assinatura digital for produzida no âmbito desta contratação, a ausência de carimbo do tempo deverá ser tratada como situação excepcional, observadas as políticas e padrões aplicáveis no âmbito da ICP-Brasil. Permanecem abrangidos por esta regra os documentos recebidos já assinados por terceiros, que eventualmente não contenham carimbo do tempo.

Requisito 24: a resposta a uma solicitação de validação de documentos deverá conter valores que permitam visualização das informações das assinaturas digitais e os atributos do certificado de cada signatário do documento.

Requisito 25: a resposta a uma solicitação de validação de assinatura deverá conter, no mínimo:

a) status da Verificação (integridade da assinatura);
b) status dos certificados digitais (válido, inválido, revogado, expirado, ainda não válido, não confiável);
c) tipo de política de assinatura utilizada;
d) data da Assinatura e data da validade do certificado;
e) *hash* do Documento Assinado;
f) dados dos Assinantes (no mínimo: nome, RG, CPF, data de nascimento, email, título de eleitor);
g) dados dos Carimbos do Tempo (para as políticas que exijam carimbo: AD-RT, AD-RV, AD-RC, AD-RA, no mínimo: data do carimbo, número serial, emissor);
h) informações sobre LCRs e Cadeia de Certificados (para as políticas que exijam estas informações); e
i) dados das LCRs e Cadeia de Certificados (para as políticas que exijam estas informações)

Requisito 26: em caso de questões relativas à validação de documentos segundo integridade, padrões e políticas de assinatura, será tomado por base o serviço Verificador de Conformidade do ITI[4].

19.5 FVCD – Requisitos da Funcionalidade de Validação E VERIFICAÇÃO DE CERTIFICADO DIGITAL

Requisito 27: A FVCD deverá ser capaz de validar qualquer tipo de certificado digital, e sua correspondente cadeia de certificação, padrão ICP-Brasil e padrão X509 v3 de acordo com a RFC 5280 e DOC-ICP 04 da ICP Brasil.

Requisito 28: a FVCD deverá ser capaz de validar lotes de certificados digitais, incluindo certificados de cadeias de certificação diferentes no mesmo lote.

Requisito 29: a FVCD deverá informar o status do certificado e da respectiva cadeia de certificação.

Requisito 30: a FVCD deverá permitir a identificação de certificados expirados, revogados, ou cujo período de validade ainda não tenha iniciado, ou cuja integridade não tenha sido verificada, ou cuja autoridade emissora não seja confiável, retornando como resposta tais status ao solicitante do serviço de validação.

Requisito 31: a FVCD deverá informar a validade e o estado de revogação da cadeia de certificação do certificado em um dado momento do tempo, tendo uma data e hora como referência.

[4] https://verificador.iti.gov.br/ em (20/04/2021)

Requisito 32: a FVCD deverá possuir opção para solicitar uma resposta contendo a decodificação e os todos os dados presentes tanto no certificado validado quanto em sua respectiva cadeia de certificação, conforme DOC-ICP 04 da ICP Brasil.

Requisito 33: a FVCD deverá possuir opção para solicitar uma resposta contendo a cadeia de certificação completa do certificado validado no formato Base 64.

19.6 FGLCR – Requisitos da Funcionalidade de Gerenciamento de Lista de Certificados Revogados

Requisito 34: a FGLCR deve possibilitar a gestão de um repositório de certificados revogados bem como a respectiva consulta.

Requisito 35: a gestão do repositório de LCRs ficará a cargo da fornecedora da solução que deverá mantê-la em conformidade com as normas e regulamentos vigentes, especialmente aqueles especificados pela ICP Brasil.

Requisito 36: a fornecedora da solução deverá manter histórico de revogação de certificados para avaliação de assinaturas por certificados revogados que foram válidos no momento da assinatura, conforme definido em FVCD - Requisitos da Solução de Verificação do certificado Digital.

Requisito 37: a FGLCR deverá ser capaz de validar a assinatura de cada LCR obtida junto às ACs, conferindo se realmente a LCR foi emitida pela Autoridade Certificadora indicada.

Requisito 38: a FGLCR deverá permitir a consulta de LCR baseada em uma data e um dos seguintes parâmetros:

a) por meio do certificado que será validado;
b) por meio da chave de autoridade do certificado que emitiu a LCR; e
c) por meio do ponto de distribuição onde a LCR é publicada pela Autoridade Certificadora.

Requisito 39: a FGLCR deverá ser capaz de identificar e lidar com todos os tipos de certificados digitais X.509, padrão ICP-Brasil.

Requisito 40: a FGLCR deverá ser capaz de manipular listas de certificados revogados que implementam a versão 2, ou versão superior, do padrão ITU-T X.509, conforme RFC 5280.

19.7 FCT – Requisitos da Funcionalidade de Carimbo de Tempo

Requisito 41: a FCT deverá permitir o uso de Carimbo de Tempo por meio de chamadas de serviço REST, para integração com solução externa.

O carimbo do tempo deverá ser aplicado às assinaturas digitais geradas no âmbito desta contratação, conforme as políticas de assinatura da ICP-Brasil, ressalvados os casos de validação de documentos previamente assinados por terceiros, nos quais o carimbo do tempo poderá estar ausente.

Requisito 42: a FCT deverá decodificar carimbo do tempo e extrair todas as informações presentes conforme resolução nº 78 de 06 de Abril de 2010 do ITI.

Requisito 43: a FCT deverá validar carimbo do tempo por meio da validação da integridade da assinatura do carimbo em relação ao documento com base em seu *hash*, e status do certificado que assinou o carimbo.

Requisito 44: a FCT deverá possuir opção para gerar requisição de carimbo do tempo baseado no *hash* de um conteúdo.

Requisito 45: a FCT deverá permitir a obtenção de carimbo do tempo de ACT com requisição autenticada de acordo com a RFC 3161.

Requisito 46: o serviço contratado deverá ser fornecido por uma ACT credenciada na ICP-Brasil, utilizando certificados tipo T3 e tipo T4.

19.8 FLAPI – Requisitos da APIs para a Execução dos Serviços Descritos nos Requisitos 4.2.1 a 4.2.6

Requisito 47: os serviços remotos fornecidos pela solução (assinatura, validação e funcionalidades correlatas acessadas por webservices) deverão rodar no ambiente em nuvem da empresa fornecedora da solução, ressalvada a existência de componentes auxiliares locais, quando previstos neste Termo, executados em ambiente sob responsabilidade do CONTRATANTE exclusivamente para fins de integração, manipulação local de documentos e/ou mitigação de exposição de conteúdo.

Requisito 48: a solução e suas funcionalidade deverão disponibilizar integração com aplicações ASP.NET (C#) por meio de APIs e webservices sem estado (*stateless*). Ou seja, todas funcionalidades descritas nos requisitos 1 a 5 da Tabela 1 deverão ser acessíveis por meio da internet via chamadas de webservices,

seguindo os requisitos de segurança aplicáveis. É vedado o uso de bibliotecas locais cujo estado impossibilite completar o conjunto de chamadas necessárias à assinatura por diferentes threads em diferentes instâncias ou que retirem o controle do gerenciamento de memória da aplicação cliente.

Requisito 49: a solução deve permitir que suas funcionalidades sejam executadas por aplicação intermediária (e não diretamente pelas aplicações cliente), que encapsulará o acesso aos serviços para as demais aplicações do Tribunal.

Requisito 50: os resultados da execução de todos os webservices, quando houver, deverão ser expressos no formato JSON (JavaScript Object Notation).

Requisito 51: a solução deve parametrizável de modo a permitir:

a) configuração da conexão segura (SSL) a ser utilizada com base nos parâmetros fornecidos;
b) autenticação respeitando protocolo HTTP;
c) comunicação via REST utilizando JSON como formato dos parâmetros de entrada e saída;
d) transmissão de binários em parâmetros de conteúdo em Base64.

Requisito 52: O tempo de execução das chamadas que não respeitem os limites abaixo serão objeto de abertura de chamado indicando indisponibilidade parcial da aplicação, conforme sessão a Requisitos de Qualidade, desse capítulo:

a) O limite médio diário de 2000ms.

b) O limite médio por 10 minutos superior a 5000ms.

- Exceto em caso de manutenção programada
- Exceto em caso de manutenção emergencial, informada através de email aos fiscais do contrato, não podendo ultrapassar 8 horas por mês.

Requisito 53: deverá ser disponibilizado pela fornecedora de serviços um ambiente de testes/homologação que possibilite ao Tribunal realizar testes de integração da solução com os seus sistemas. Eventuais assinaturas realizadas em ambientes que não sejam de produção não serão computadas para o total de assinaturas faturadas.

Requisito 54: o acesso a cada uma das funcionalidades de assinatura digital de documentos (assinatura, validação de assinatura digital e validação de certificados digitais – requisitos 1, 2 e 3 da Tabela

1) deverá ser disponibilizado de forma independente, ficando facultado ao fornecedor a organização em módulos.

Requisito 55: todas as interfaces de serviço (URI, descrição, entradas, saídas, formatos e assinaturas) devem ser documentadas e disponibilizadas para consulta.

Requisito 56: códigos e mensagens de erro devem estar catalogados e descritos na documentação dos serviços;

19.9 FLSAW – Requisitos da Licença de Software para Execução de Assinaturas Digitais Via Navegadores Web (plugin5)

Requisito 57: a solução deve contemplar licença de software, incluindo suporte e atualização, de *plugin* para execução de assinaturas digitais, em documento unitário e em lote de documentos, via navegadores web.

Requisito 58: o *plugin* para assinatura via navegador deve ser capaz de listar os certificados disponíveis para assinatura (A1 ou A3, em arquivo local ou em token) para que o usuário escolha o certificado a ser usado para a assinatura.

Requisito 59: o *plugin* deve receber da aplicação cliente web as informações cuja cifragem serão insumo da assinatura de documentos, cumprindo a Etapa 2 do *Requisito 8:*Requisito 8.

Requisito 60: o *plugin* deve possibilitar a integração com os seguintes sistemas operacionais e navegadores:

- Windows 10 ou superior (versões 32 bits e 64 bits), utilizando os navegadores Google Chrome d Mozilla Firefox e Edge;
- Linux utilizando o navegador Mozilla Firefox;

Requisito 61: a integração desta solução com as aplicações do Tribunal deve permitir customização e utilizar boas práticas definidas pela W3C sem, por exemplo, uso de Applets ou outras tecnologias reconhecidamente defasadas e geradoras de problemas de compatibilidade.

[5] Na informática, um plugin ou módulo de extensão (também conhecido por *plug-in*, *add-in*, *add-on*) é um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica. Geralmente pequeno e leve, é usado somente sob demanda (Wikipedia, 2021).

Requisito 62: a instalação do *plugin* e de componentes necessários à sua execução deve ser orientada e gerenciada pela própria solução. A identificação da ausência do *plugin* deve ocorrer de forma automática na própria interface web do usuário, permitindo redirecionamento para página que oriente a sua instalação. Caso o dependa da instalação de outros componentes, o *plugin* deve identificar a situação e orientar sua instalação ao usuário de forma a minimizar a necessidade de suporte

Requisito 63: a instalação dos componentes necessários à interação do *plugin* com o Sistema Operacional para acesso a drivers e certificados não pode ser dependente de permissões especiais do usuário como acesso de administrador ou super usuário do sistema, por exemplo.

Requisito 64: o uso do *plugin* não deve exigir configurações adicionais de segurança de navegadores.

Requisito 65: componentes necessários à interação do *plugin* com o sistema operacional devem ser acionados pelo *plugin*, vedado a instalação de processos (agentes) cujo erro na sua inicialização provoque necessidade de intervenção humana ou reinstalações. Caso necessário o uso de agentes, o *plugin* deve conseguir identificar se o agente não foi instalado, se está instalado e não foi inicializado ou se não foi possível inicializá-lo devido à ocorrência de erros. Em caso de instalado e não inicializado, o plugin deve inicializá-lo sem intervenção humana. Caso não tenha sido possível inicializá-lo devido a erros, deve-se orientar o usuário a contatar o suporte e indicar as informações adicionais necessárias para análise e solução do problema.

Requisito 66: erros recorrentes[6] na execução do plugin serão classificados como problemas cuja solução será de responsabilidade da fornecedora da solução.

Requisito 67: a CONTRATADA é responsável pelo fornecimento de documentação operacional atualizada. Caso essa documentação não seja suficiente para solucionar incidentes e/ou problemas, o Tribunal poderá acionar a fornecedora da solução com vistas a sanar a ocorrência.

Requisito 68: a solução deve fornecer suporte a certificados do tipo A3 armazenados em dispositivo físicos homologados na ICP-Brasil.

[6] Erro recorrente, nesse contexto, entende-se por dois ou mais chamados de mesmo usuário, ou referente a ocorrências distintas de um mesmo erro.

19.10 FLSA1 – Requisitos da Licença de Componente para Execução, no Servidor de Aplicações, de Assinaturas Digitais com Suporte a Certificados A1

Requisito 69: a fornecedora da solução deve disponibilizar biblioteca em C#, licença de software com suporte e atualização para execução, via servidor, de assinaturas digitais em documento unitário ou em lote de documentos.

Requisito 70: a solução deve fornecer suporte a certificados do tipo A1 armazenado em arquivo no formato pfx.

Requisito 71: dado um certificado A1 e o produto da primeira etapa do *Requisito 8:*Requisito 8, a biblioteca deve efetuar, sem intervenção humana, a cifragem das informações que serão insumo da assinatura de documentos, cumprindo a Etapa 2 do *Requisito 8:*Requisito8.

19.11 Requisitos temporais

Requisito 72: a solução e todos os seus componentes devem possuir atendimento de suporte telefônico e acompanhamento dos níveis de serviços prestados por meio de número específico, das 8h às 18h, de segunda-feira a sexta-feira, exceto em feriados nacionais e feriados municipais na cidade de Curitiba-PR. Além disso, deve possuir portal de serviços online 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, para abertura de chamados de incidentes e demais informações.

Requisito 73: as interrupções programadas das soluções para testes, ajustes, manutenções e/ou substituições de equipamentos ou meios utilizados no provimento do serviço deverão ser informadas ao Tribunal com antecedência mínima de 5 (cinco) dias úteis. A interrupção programada não será computada para fins de medição do nível de serviço.

19.12 Requisitos de capacitação e transferência de conhecimento

Requisito 74: para a implantação e manutenção dos serviços não há necessidade de capacitação específica, uma vez que todas essas atividades (incluindo suporte técnico) permanecerão, exclusivamente, sob responsabilidade do fornecedor da solução. Contudo, é importante o fornecimento dos documentos e informações inerentes às funcionalidades da solução para que a equipe técnica do Tribunal possa controlar a disponibilidade dos serviços, realizar as intervenções por ela julgadas necessárias e entender os problemas que venham a ocorrer em algum momento.

Requisito 75: as informações prestadas inerentes à solução poderão ser fornecidas por meio de canais de acesso web, tutoriais, atendimento presencial ou manuais específicos. Independentemente do meio de comunicação, o contato deve resultar sempre num documento final a ser encaminhado para e-mail a ser fornecido pela equipe de fiscalização.

19.13 Requisitos de segurança

Requisito 76: para garantir alta disponibilidade do serviço, deverá ser disponibilizada redundância para a solução e todas as suas funcionalidades. Essa redundância deve ser contemplada por pelo menos 2 (dois) ambientes (nós) de acesso a solução trabalhando em modo ativo-ativo, com chaveamento automático.

Requisito 77: todos os *webservices* e interfaces web de acesso disponibilizados pela solução devem utilizar mecanismo de segurança para autenticação e autorização de acesso aos serviços, por meio de canal SSL/TLS (v1.1, v1.2, v1.3) duplamente autenticado, com o uso de certificado digital, de acordo com a RFC5746.

Requisito 78: a solução e suas funcionalidades deverão permitir a geração, visualização e armazenamento de registro eletrônico (LOG) dos procedimentos executados bem como das informações pertinentes ao usuário e rede para fins de auditoria, conforme item 6.13 do DOC-ICP 15 da ICP Brasil.

Requisito 79: a solução e suas funcionalidades deverão disponibilizar os logs gerados sempre que solicitados pelo Tribunal, conforme prazo estabelecido o nível Baixo de criticidade descrito na Tabela 2.

Requisito 80: a solução e suas funcionalidades deverão possuir configuração para controle de integridade dos arquivos de LOG com garantia de temporalidade.

19.14 Requisitos de monitoramento

Requisito 81: a solução deve possuir interface de acompanhamento e monitoramento dos serviços. Essa interface deverá prover acesso a relatório atualizado sobre o quantitativo de assinaturas e verificações realizadas por período estipulado. Quando não for possível, por qualquer motivo, obter o relatório do quantitativo de assinaturas e verificações por meio da interface de acompanhamento, ou na ausência deste recurso, o provedor da solução deverá fornecê-lo sempre que for solicitado, no prazo de 48 horas a contar da solicitação.

Requisito 82: a interface de acompanhamento e monitoramento dos serviços deverá prover acesso a relatório atualizado (pelo menos até o final do mês anterior ao da solicitação) com dados sobre disponibilidade do serviço por período estipulado. Quando não for possível obter o relatório sobre a

disponibilidade do serviço por meio da interface de acompanhamento, ou na sua ausência, o provedor da solução deverá fornecê-lo sempre que for solicitado, no prazo de 5 dias a contar da solicitação.

Requisito 83: a interface de acompanhamento e monitoramento dos serviços deverá prover acesso a informações sobre o tempo médio de resposta às chamadas aos serviços (*webservices*). Quando não for possível obter estas informações por meio da interface de acompanhamento, ou na sua ausência, o provedor da solução deverá fornecê-las sempre que for solicitado, no prazo de 5 dias a contar da solicitação.

Requisito 84: a interface de acompanhamento e monitoramento dos serviços deverá notificar o Tribunal em casos de situações críticas na execução das soluções como, por exemplo, paralisação total dos serviços ou queda no desempenho descrito no **Requisito 15**. Quando não for possível a notificação por este meio, ou na sua ausência, o provedor da solução deverá proativamente notificar o fiscal do contrato por e-mail fornecido por ocasião da reunião inicial.

19.15 Requisitos de sustentabilidade

Requisito 85: os serviços prestados deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos.

Requisito 86: o fornecedor do serviço deverá instruir os seus colaboradores quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo Tribunal.

19.16 Requisitos de qualidade

Requisito 87: a solução deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. A disponibilidade do serviço corresponde ao percentual de tempo, durante o mês, em que o serviço esteve em condições plenas de funcionamento, sem registro de indisponibilidade pelo monitoramento proativo do provedor da solução e/ou do Tribunal. Esse percentual não poderá ser inferior a 99,5% (noventa e nove vírgula cinco por cento).

Requisito 88: o provedor da solução deverá cumprir os Tempos de Resposta descritos na Tabela 2, de acordo com a criticidade do processo. O Prazo Máximo de Solução é o tempo máximo compreendido entre a solicitação formal do Tribunal, por meio de um canal de atendimento, para a solução de um incidente/problema e o fornecimento de uma solução definitiva do chamado por parte do provedor da

solução. Chamados recorrentes sobre o mesmo problema, durante o mês, deverão ser contabilizados em conjunto para composição dos prazos para resposta.

Criticidade	Processo	Prazo máximo de atendimento	Prazo máximo de solução
Alto	Indisponibilidade de qualquer das funcionalidades ou da solução	02 horas	08 horas
Médio	Indisponibilidade parcial de qualquer das funcionalidades da solução. Entende-se por indisponibilidade parcial o funcionamento intermitente da solução e/ou comportamento inesperado em determinadas situações.	03 horas	36 horas
Baixo	Sem impactos sobre o ambiente de produção. Nesse nível estão incluídas as dúvidas sobre o funcionamento da solução.	04 horas	72 horas

Tabela 2 - Tempos de atendimento por criticidade

Requisito 89: o prazo mínimo aceito para garantia de resolução de chamados é 72 horas. O prazo para garantia de resolução de chamados é a quantidade de horas transcorridas entre a solução de um chamado e um novo registro com a mesma natureza/teor do anterior. O cálculo do prazo para garantia de resolução de chamados é feito por ocorrência, avaliando o horário de fechamento do chamado técnico e horário de abertura de novo chamado na central de atendimento contendo registro de igual natureza.

19.17 Requisitos de implantação

19.17.1 Requisitos de implantação

Faz parte da solução a ser contratada o item 9 da Tabela 1, que compreende:

a. desenvolvimento de solução para adaptação das interfaces do Assinador do Tribunal àquelas fornecidas pela nova solução contratada;
b. adaptação das aplicações do Tribunal para fornecimento de novas informações à solução contratada, caso seja necessário;
c. adaptação das aplicações do Tribunal para integração com a nova solução de assinatura digital em servidores com certificado A1.

As seções seguintes tratam individualmente cada uma dessas necessidades de adaptação das aplicações do Tribunal para estarem em conformidade com a nova solução a ser contratada. Todas as adaptações necessárias nas aplicações, bem como a construção do software Adaptador, devem ocorrer **em até 60 (sessenta) dias corridos** a contar do início da vigência contratual.

19.17.2 Adaptação das interfaces dos serviços de assinatura e validação em nuvem

Uma visão mais voltada para as interfaces de comunicação é apresentada na Figura 1. A figura destaca a composição da arquitetura de aplicações do TCE no que diz respeito à utilização do serviço de assinatura digital.

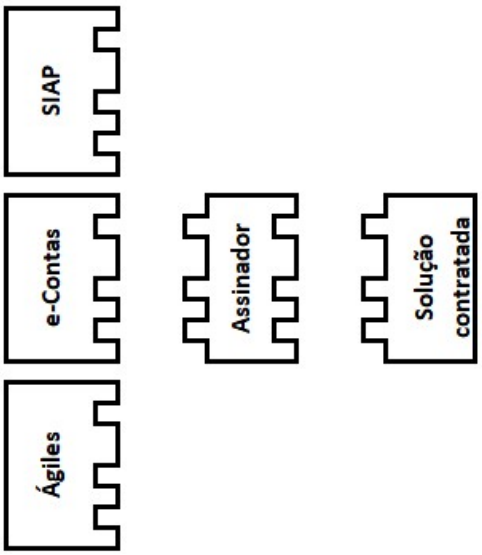


Figura 1 - Arquitetura sob o aspecto da integração

A Figura 1 busca destacar que existem características específicas (ilustradas pelos encaixes dos retângulos) das interfaces compartilhadas entre Assinador do Tribunal e a Solução Contratada. Estas características envolvem quantidades e tipos de dados específicos no envio e no recebimento de informações, bem como fluxos específicos de execução da lógica de assinatura.

Como o Tribunal não conhece a solução de assinatura digital que será fornecida na nova contratação, é necessário que seja fornecido, junto com a própria solução, um software adaptador de interfaces. Este software irá compor uma nova arquitetura de aplicações conforme ilustra a Figura 2.

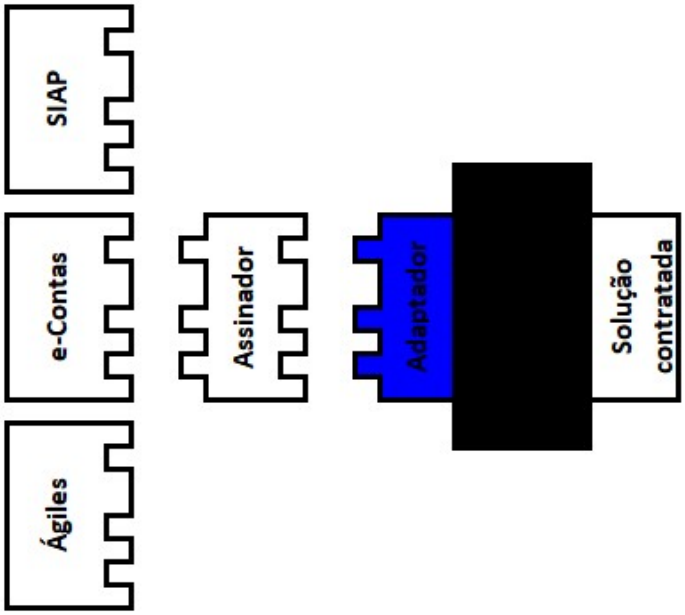


Figura 2 - Nova arquitetura de aplicações

A caixa azul destacada na Figura 2, doravante chamado de Adaptador, é o software que deverá ser construído e fornecido pela fornecedora da solução de assinatura digital. Observa-se que a partir dessa nova arquitetura o Tribunal desconhece a forma com que o Adaptador se conecta à solução contratada. Esta forma de comunicação é representada pela caixa preta. Para o Tribunal de fato não interessa a forma que este Adaptador utilizará para se conectar à solução de assinatura digital; apenas interessa que o Adaptador irá se conectar ao Assinador por meio da interface atualmente utilizada por este. Desse modo, o software Adaptador passa ser parte integrante da solução a ser contratada.

É importante ressaltar que o Adaptador deve ser construído respeitando a arquitetura SaaS e deve realizar a tarefa definida pelo Design Patter Adapter[7]. Ou seja, o Adaptador deve ser entregue no formado de *webservices* e terá a tarefa de realizar as conversões de dados necessárias para compatibilizar o Assinador do Tribunal com a solução de assinatura digital fornecida. A documentação completa das interfaces exigidas pelo assinador está disponível no Apêndice B.

20 APÊNDICE B - ESPECIFICAÇÃO DO SERVIÇO DE ADAPTAÇÃO para integração das aplicações do TCE-PR

20.1 Introdução

Este apêndice descreve a especificação técnica da solução de software Adaptador de interface para integração com o software Assinador do Tribunal de Contas do Estado do Paraná.

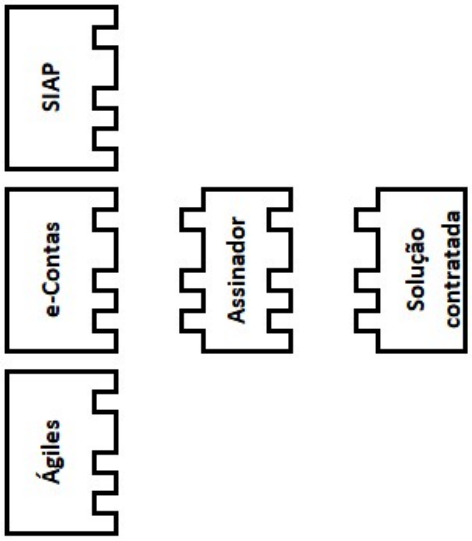
São detalhados neste apêndice as interfaces requeridas pelo Assinador, os tipos de dados enviados e recebidos por cada um dos serviços web, bem como o fluxo das chamadas destes *webservices*.

O software Adaptador aqui descrito deve ser desenvolvido na arquitetura Software as a Service (SaaS). Ou seja, o resultado de sua programação deve ser acessível por meio de chamadas a *webservices* a serem disponibilizados no ambiente computacional da empresa desenvolvedora.

Além disso, o Adaptador deve ser construído segundo preconiza o Design Patter Adapter[8]. Ou seja, o Adaptador terá a tarefa de realizar as conversões de dados necessárias para compatibilizar o Assinador do Tribunal com a solução de assinatura digital fornecida.

20.2 Interfaces Do Assinador

Este capítulo apresenta a especificação das interfaces requeridas pelo Assinador do Tribunal. O Assinador é o software desenvolvido pelo TCE para intermediar a comunicação entre as aplicações assinadoras e a solução de assinatura digital. A Figura 3 ilustra a participação do Assinador na arquitetura utilizada pelo tribunal.



[7] Sobre o padrão Adapter: https://refactoring.guru/pt-br/design-patterns/adapter

[8] Sobre o padrão Adapter: https://refactoring.guru/pt-br/design-patterns/adapter

Figura 3 – Arquitetura sob o aspecto da integração

À esquerda estão algumas das aplicações que utilizam o serviço de assinatura digital em nuvem. À direita da figura está a solução atualmente contratada que fornece os serviços de assinatura digital em nuvem. No centro da comunicação está o software Assinador do Tribunal que, apesar do nome, faz apenas a intermediação da comunicação, e não o processo de assinatura em si.

O Adaptador a ser construído formará uma nova visão arquitetural das aplicações, semelhante ao que ilustra a Figura 4. A caixa azul destacada é o software que deverá ser construído e fornecido pela fornecedora da solução de assinatura digital.

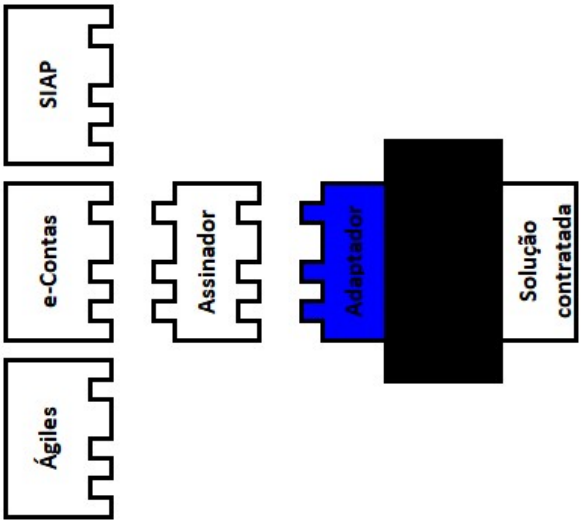


Figura 4 – Nova arquitetura de aplicações

As seções seguintes apresentam os fluxos que devem ser implementados pelo Adaptador. São apresentados diagramas de sequência com a visão geral da lógica aplicada a cada um dos processos que devem ser implementados. As estruturas de dados das chamadas e dos retornos dos serviços estão descritas no Apêndice A,

20.3 Fluxo da assinatura

Esta seção descreve o fluxo de chamada dos serviços para assinatura digital de documentos. No ETP, esse fluxo representa a solução descrita no requisito ***FADD – Requisitos da Funcionalidade de Assinatura Digital de Documentos****. A*

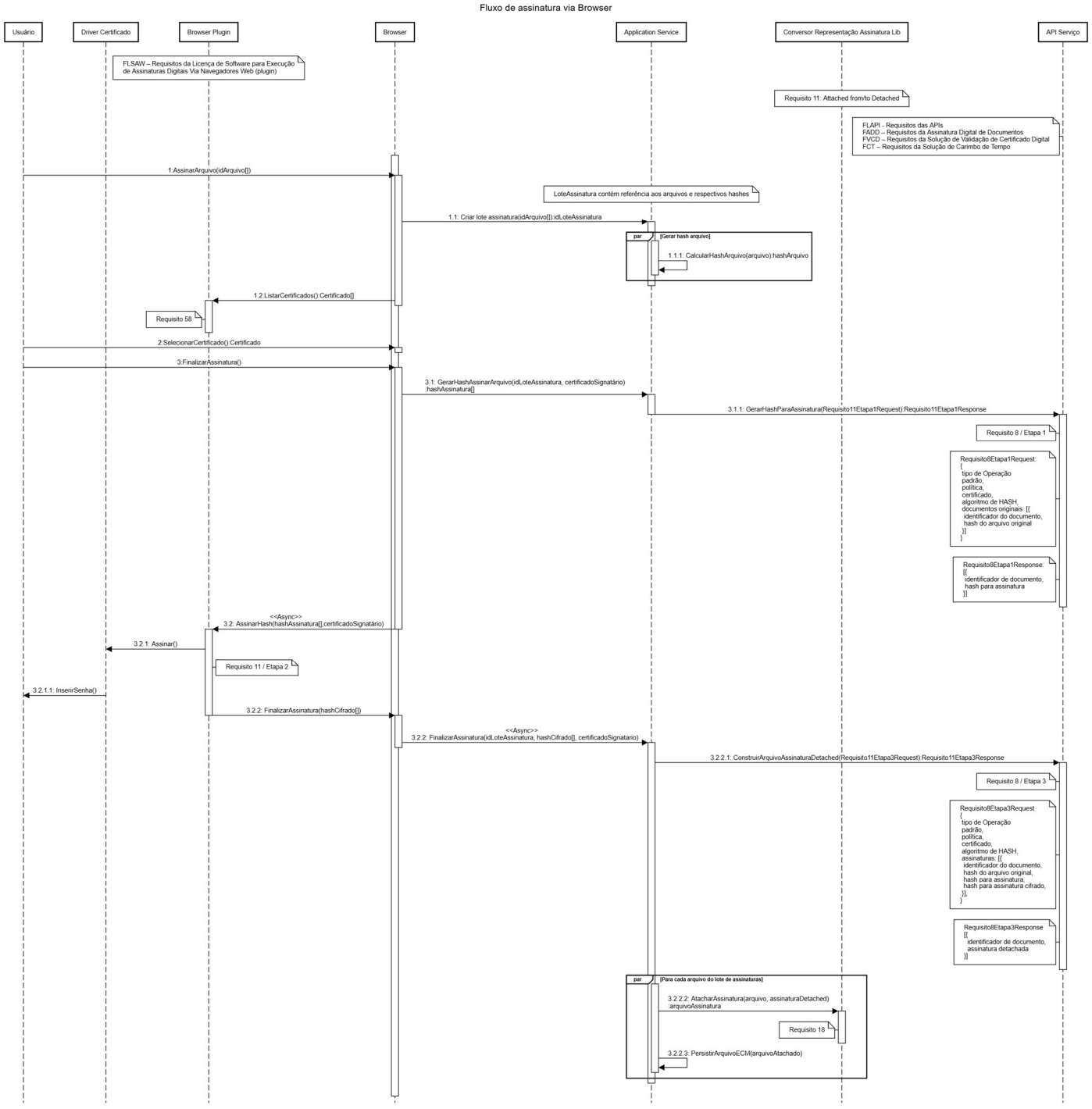


Figura 5 apresenta a sequência do processo completo de assinatura.

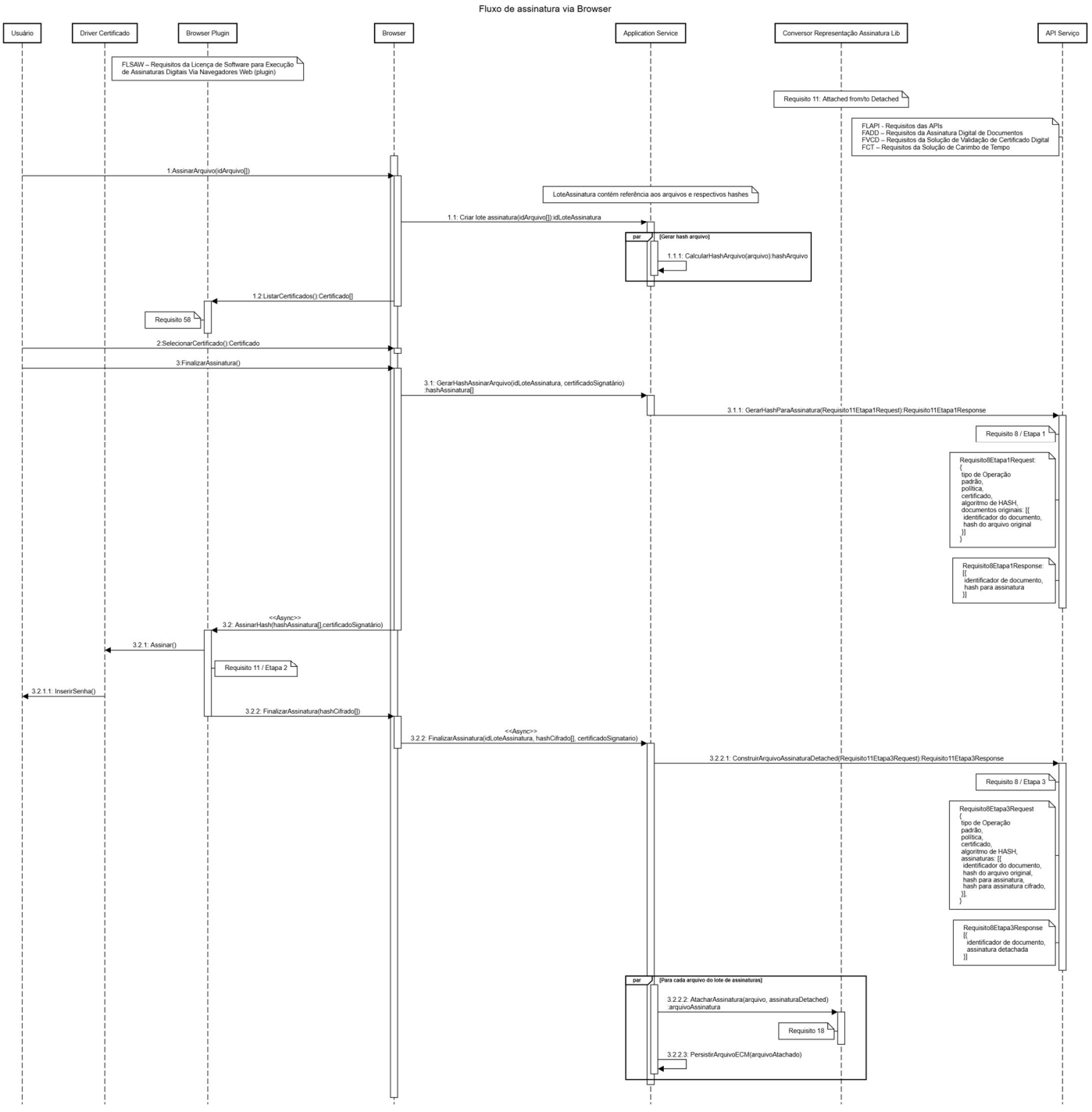


Figura 5 - Fluxo da assinatura

No diagrama, o Adaptador a ser desenvolvido pela empresa contratada é identificado pelo nome API Serviço. As seguintes chamadas devem ser atendidas pelo Adaptador:

- 3.1.1: `GerarHashParaAssinatura()`
- 3.2.2.1: `ConstruirArquivoAssinadutaDetached()`

As estruturas de dados das chamadas e dos retornos dos serviços estão descritas na sessão Dicionário de Dados.

20.4 Fluxo da Coassinatura

Esta seção descreve o fluxo de chama dos serviços para coassinatura[9] digital de documentos. No ETP, esse fluxo representa a solução descrita no requisito **FADD – Requisitos da Funcionalidade de Assinatura Digital de Documentos**. A Figura 6 apresenta a sequência do processo completo de coassinatura.

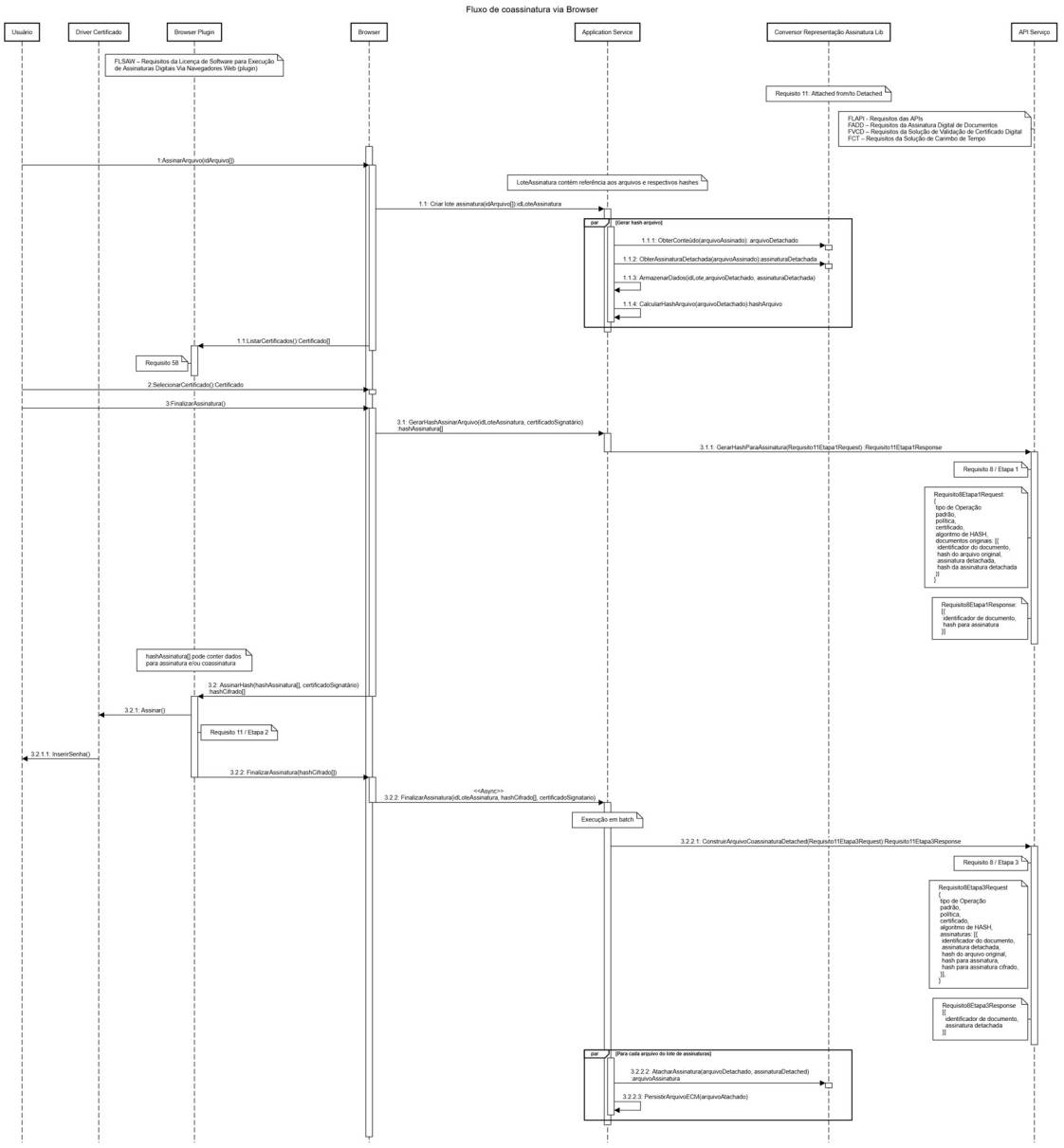


Figura 6 - Fluxo da Coassinatura

[9] Também conhecida como assinaturas paralelas

No diagrama, o Adaptador a ser desenvolvido pela empresa contratada é identificado pelo nome **API Serviço**. As seguintes chamadas devem ser atendidas pelo Adaptador:

- 3.1.1: `GerarHashParaAssinatura()`
- 3.2.2.1: `ConstruirArquivoCoassinadutaDetached()`

As estruturas de dados das chamadas e dos retornos dos serviços estão descritas na sessão Dicionário de Dados.

20.5 Fluxo de assinatura com certificado em nuvem

Esta seção estende a descrição o fluxo de chama dos serviços para assinatura digital de documentos, detalhando o suporte a assinatura com certificado em nuvem. Esse fluxo representa a solução descrita no requisito **FADD – Requisitos da Funcionalidade de Assinatura Digital de Documentos**. A Figura 6 apresenta a sequência do processo completo de assinatura, com detalhamento do **Requisito 14A**.

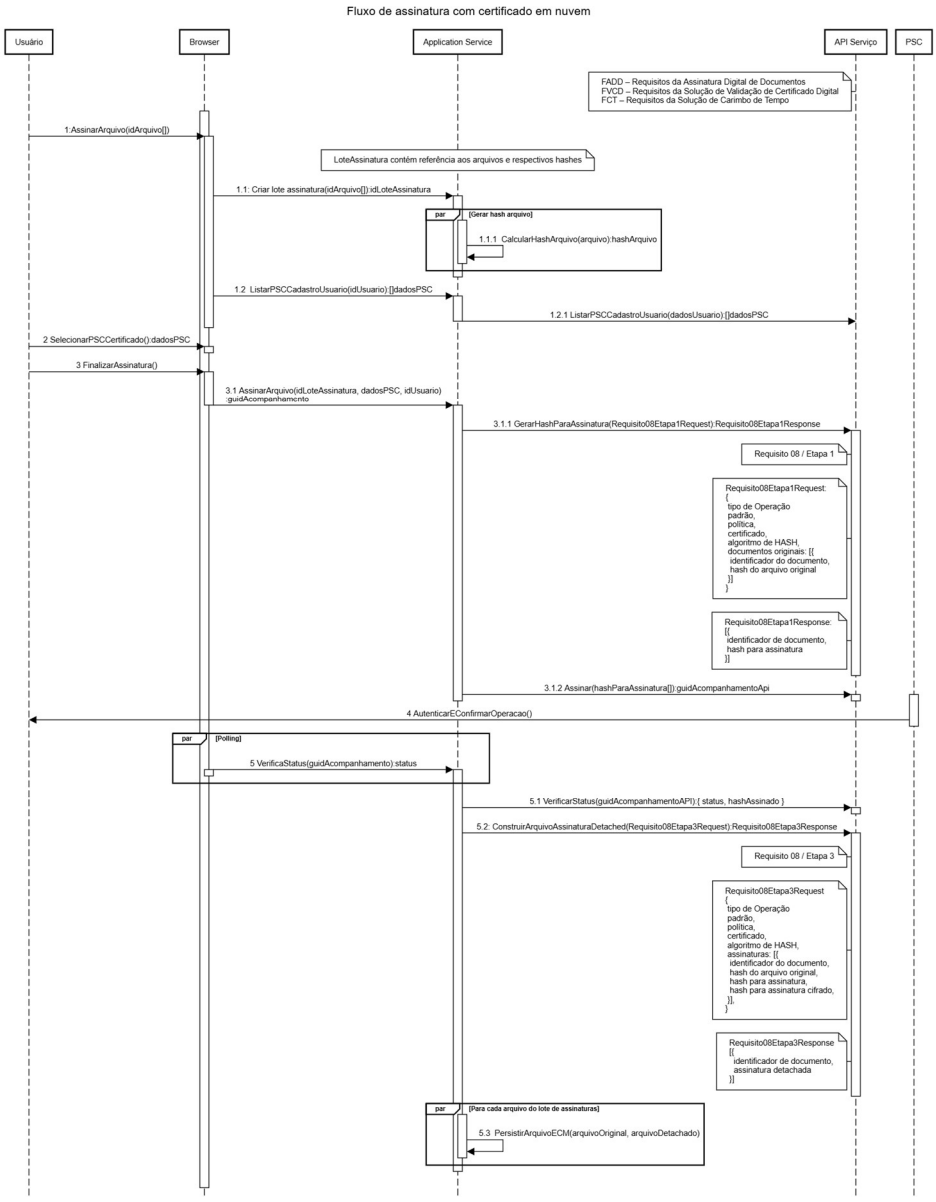


Figura 5 - Fluxo de Assinatura de Documentos com Certificado em Nuvem

20.6 Fluxo da validação de assinatura

Esta seção descreve o fluxo de chama dos serviços para validação de assinaturas digitais em documentos. No ETP, esse fluxo representa a solução descrita no requisito **FVAAD – Requisitos da Funcionalidade de Validação de Assinatura Digital de Documentos**. A Figura apresenta a sequência do processo completo de validação de assinaturas.

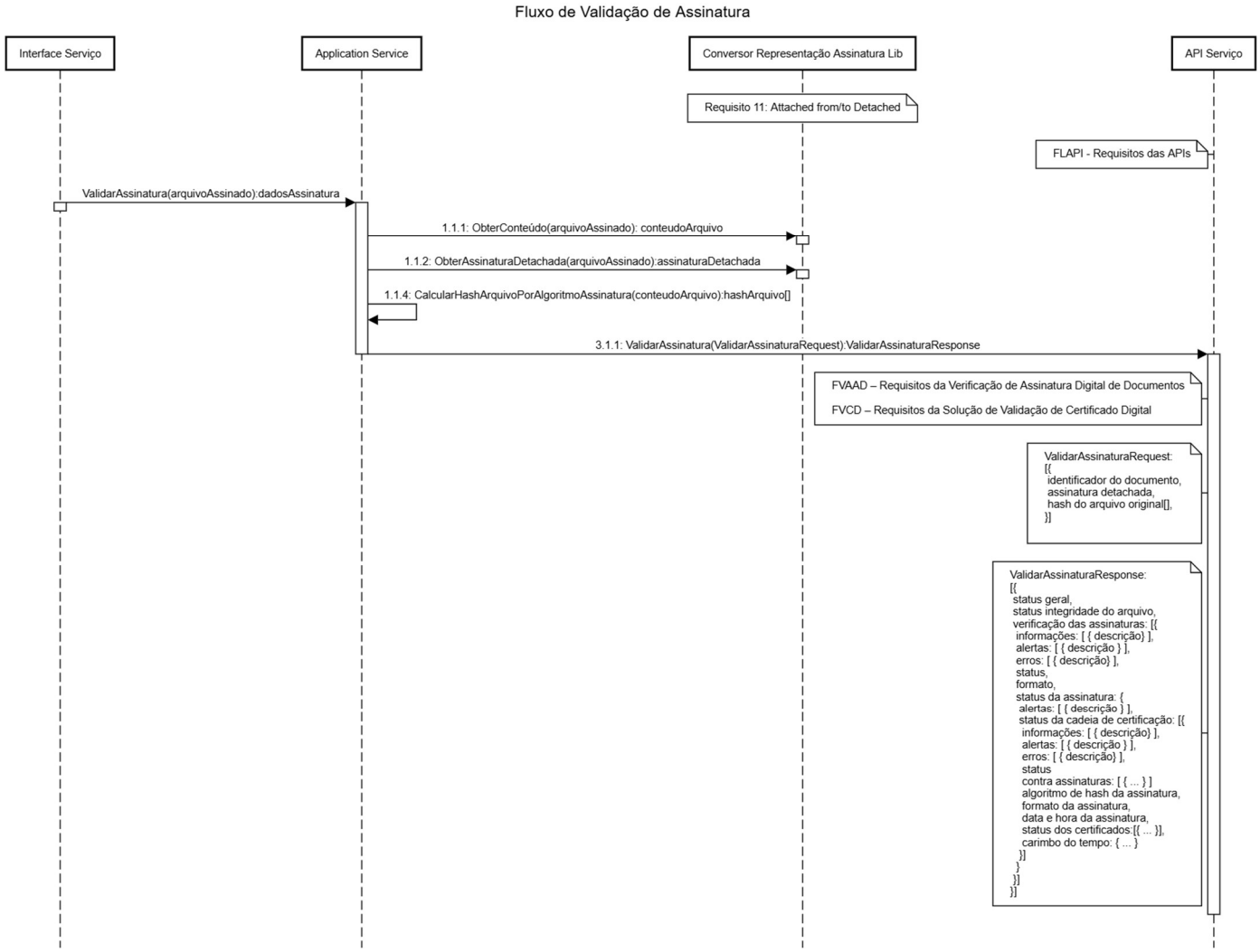


Figura 6 - Fluxo de Validação de Assinatura

No diagrama, o Adaptador a ser desenvolvido pela empresa contratada é identificado pelo nome **API Serviço**. A seguinte chamada deve ser atendida pelo Adaptador:

- 3.1.1: `ValidarAssinatura()`

As estruturas de dados das chamadas e dos retornos dos serviços estão descritas na sessão Dicionário de Dados.

20.7 Fluxo da assinatura no servidor

Esta seção descreve o fluxo de chama dos serviços para assinatura digital de documentos via servidor de aplicações, com certificado tipo A1. No ETP, esse fluxo representa a solução descrita no requisito **FVAAD – Requisitos da Funcionalidade de Validação de Assinatura Digital de Documentos**, porém, para execução a partir do servidor de aplicação. A Figura apresenta a sequência do processo completo de validação de assinaturas.

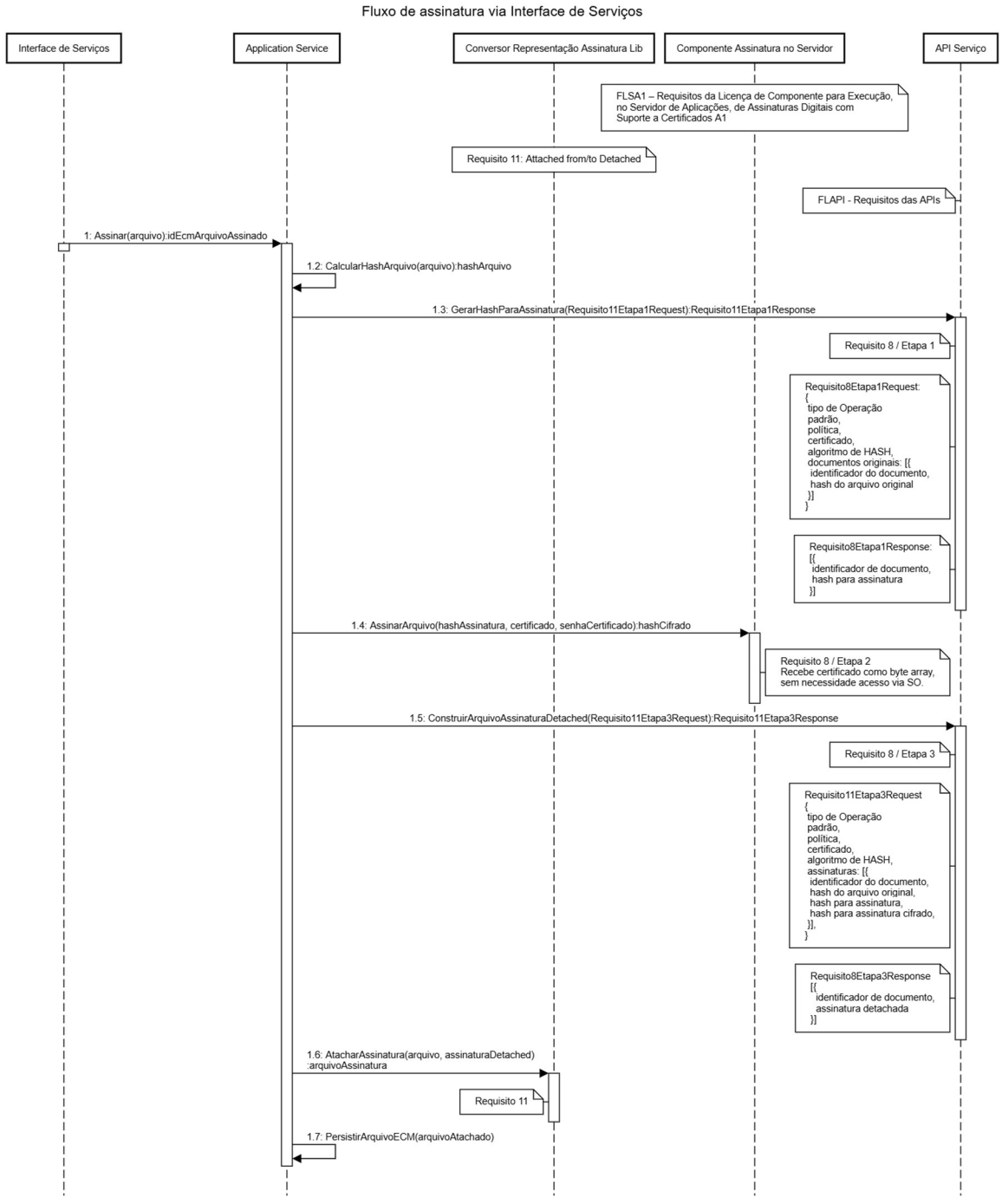


Figura 7 - Fluxo de Assinatura via Servidor de Aplicação

No diagrama, o Adaptador a ser desenvolvido pela empresa contratada é identificado pelo nome **API Serviço**. As seguintes chamadas devem ser atendidas pelo Adaptador:

- 3.1.1: `GerarHashParaAssinatura()`
- 3.2.2.1: `ConstruirArquivoAssinadutaDetached()`

As estruturas de dados das chamadas e dos retornos dos serviços estão descritas na sessão Dicionário de Dados.

20.8 Dicionário de Dados

Este capítulo apresenta as estruturas de dados utilizadas nas chamadas e retornos dos serviços descritos nos diagramas do capítulo anterior.

Requisito 8, Etapa 1: Gerar Hash para assinatura

Requisito11Etapa1Request

Nome do parâmetro: tipo de Operação

Tipo de dados: string

Semântica: descreve o tipo de operação requisitada. Assume um dente os valores: [ASSINATURA, COASSINATURA, CONTRA_ASSINATURA]

Nome do parâmetro: padrão

Tipo de dados: string

Semântica: Indica o padrão da assinatura desejada: [CADES, CMS]

Nome do parâmetro: política

Tipo de dados: string

Semântica: Indica a política de assinatura desejada. Assume um dentre os valores:

Caso padrão CADES: [ADRB, ADRT, ADRV, ADRC, ADRA];

caso padrão CMS [ETSI_B, ETSI_T, ETSI_LT, ETSI_LTA].

Nome do parâmetro: certificado

Tipo de dados: string

Semântica: certificado público ICP-Brasil do signatário em base64

Nome do parâmetro: algoritmo de hash

Tipo de dados: string

Semântica: descreve o algoritmo que, aplicado ao conteúdo original a ser assinado que gera o hash necessário à assinatura.

Nome do parâmetro: hash do arquivo original

Tipo de dados: string

Semântica: hash do conteúdo original a ser assinado descrito em hexadecimal

---

Nome do parâmetro: assinatura detachada

Tipo de dados: string

Semântica: arquivo em base64 utilizado para contra assinatura.

Nome do parâmetro: hash da assinatura detachada

Tipo de dados: string

Semântica: hash hexadecimal da assinatura a ser contra assinada

---

Nome do parâmetro: identificador do documento

Tipo de dados: string

Semântica: identificador do documento no contexto da aplicação. Necessário para rastreabilidade da assinatura e vinculação ao documento durante as chamadas assíncronas necessárias à consolidação da assinatura.

Requisito11, Etapa 1 Response

Nome do parâmetro: identificador do documento

Tipo de dados: string

Semântica: identificador do documento no contexto da aplicação. Necessário para rastreabilidade da assinatura e vinculação ao documento durante as chamadas assíncronas necessárias à consolidação da assinatura.

Nome do parâmetro: hash para assinatura

Tipo de dados: string

Semântica: hash de informação composta por campos do certificado público e do hash do conteúdo assinado. Essa informação será parâmetro para criptografia com chave privada do signatário.

Requisito 8, Etapa 3: FinalizarAssinatura

Requisito11Etapa3Request

Nome do parâmetro: tipo de Operação[10]

Tipo de dados: string

Semântica: descreve o tipo de operação requisitada. Assume um dente os valores: [ASSINATURA, COASSINATURA, CONTRA_ASSINATURA]

Nome do parâmetro: padrão[11]

Tipo de dados: string

Semântica: Indica o padrão da assinatura desejada: [CADES, CMS]

Nome do parâmetro: política[12]

Tipo de dados: string

Semântica: Indica a política de assinatura desejada. Assume um dentre os valores:

Caso padrão CADES: [ADRB, ADRT, ADRV, ADRC, ADRA];

caso padrão CMS [ETSI_B, ETSI_T, ETSI_LT, ETSI_LTA].

Nome do parâmetro: certificado[13]

Tipo de dados: string

Semântica: certificado público ICP-Brasil do signatário em base64

---

[10] Valor informado em RequestRequisito11Etapa 1

[11] Idem a Nota1

[12] Idem a Nota1

[13] Idem a Nota1

Nome do parâmetro: algoritmo de hash[14]

Tipo de dados: string

Semântica: descreve o algoritmo que, aplicado ao conteúdo original a ser assinado que gera o hash necessário à assinatura.

Nome do parâmetro: hash do arquivo original[15]

Tipo de dados: string

Semântica: hash do conteúdo original a ser assinado descrito em hexadecimal

---

Nome do parâmetro: assinatura detachada[16]

Tipo de dados: string

Semântica: arquivo em base64 utilizado para contra assinatura.

Nome do parâmetro: hash da assinatura detachada[17]

Tipo de dados: string

Semântica: hash hexadecimal da assinatura a ser contra assinada

---

Nome do parâmetro: hash para assinatura[18]

Tipo de dados: string

Semântica: hash de informação composta por campos do certificado público e do hash do conteúdo assinado. Essa informação será parâmetro para criptografia com chave privada do signatário.

---

[14] Idem a Nota1

[15] Idem a Nota1

[16] Idem a Nota1

[17] Idem a Nota1

[18] Valor retornado em ResponseRequisito11Etapa 1

Nome do parâmetro: hash para assinatura cifrado

Tipo de dados: string

Semântica: campo 'hash para assinatura' retornado em ResponseRequisito11Etapa1 criptograpado com a chave privada do signatário.

Nome do parâmetro: identificador do documento

Tipo de dados: string

Semântica: identificador do documento no contexto da aplicação. Necessário para rastreabilidade da assinatura e vinculação ao documento durante as chamadas assíncronas necessárias à consolidação da assinatura.

Requisito11Etapa3Response

Nome do parâmetro: identificador do documento[19]

Tipo de dados: string

Semântica: identificador do documento no contexto da aplicação. Necessário para rastreabilidade da assinatura e vinculação ao documento durante as chamadas assíncronas necessárias à consolidação da assinatura.

Nome do parâmetro: assinatura detachada

Tipo de dados: string

Semântica: arquivo em base64 string resulte do processo de assinatura.

Validar Assinatura

ValidarAssinaturaRequest

Nome do parâmetro: identificador do documento

Tipo de dados: string

Semântica: identificador do documento no contexto da aplicação. Necessário para vinculação do documento validado ao resultado da validação para o caso de chamadas assíncronas ou validação de múltiplos documentos numa única chamada.

---

[19] Idem ao identificador do arquivo utilizado no request (3.2.2)

Nome do parâmetro: assinatura detachada

Tipo de dados: string

Semântica: arquivo no formato base64 contendo a assinatura detachada do documento em validação.

Nome do parâmetro: algoritmo de hash da assinaturas do arquivo em validação

Tipo de dados: string[]

Semântica: array contendo o algoritmo utilizado para cada assinatura do arquivo, em ordem de leitura.

Nome do parâmetro: hash do arquivo original[]

Tipo de dados: string[]

Semântica: array contendo hash hexadecimal do arquivo original conforme cada algoritmo indicado por cada assinatura do arquivo, em ordem de leitura.

ValidarAssinaturaResponse

Nome do parâmetro: status geral

Tipo de dados: string

Semântica: Enumeração indicando validade das assinaturas do documento.

Nome do parâmetro: status integridade do arquivo

Tipo de dados: string

Semântica: Enumeração indicando se a integridade do arquivo foi ou não violada. Utilizado para determinar, em caso de integridade inviolada, a viabilidade de coleta de nova assinatura em caso de erro na assinatura.

Nome do parâmetro: informações

Tipo de dados: string

Semântica: texto indicando observações sobre indicadores opcionais ao documento DOC-ICP 15

Nome do parâmetro: alertas

Tipo de dados: string

Semântica: texto indicando recomendações indicadas pelo documento DOC-ICP 15

Nome do parâmetro: erros

Tipo de dados: string

Semântica: texto indicando descumprimentos ao documento DOC-ICP 15

Nome do parâmetro: status das assinaturas

Tipo de dados: string

Semântica: Enumeração indicando cumprimento de todas as assinaturas às normas do documento DOC-ICP 15

Nome do parâmetro: padrão

Tipo de dados: string

Semântica: Enumeração indicando padrão da assinatura [CADES | CMS]

Nome do parâmetro: Status da Assinatura

Tipo de dados: Tipo Status da Assinatura

Semântica: array de dados relativos a cada assinatura do documento

---

Tipo Status da Assinatura

Nome do parâmetro: informações

Tipo de dados: string

Semântica: texto indicando observações sobre indicadores opcionais ao documento DOC-ICP 15

Nome do parâmetro: alertas

Tipo de dados: string

Semântica: texto indicando recomendações indicadas pelo documento DOC-ICP 15

Nome do parâmetro: erros

Tipo de dados: string

Semântica: texto indicando descumprimentos ao documento DOC-ICP 15

Nome do parâmetro: status

Tipo de dados: string

Semântica: Enumeração indicando cumprimento às normas do documento DOC-ICP 15

Nome do parâmetro: tipo do certificado

Tipo de dados: string

Semântica: Enumeração indicando o tipo do certificado [A1, A3]

Nome do parâmetro: algoritmo de hash

Tipo de dados: string

Semântica: indica algoritmo de hash utilizado na assinatura

Nome do parâmetro: padrão

Tipo de dados: string

Semântica: Enumeração indicando padrão da assinatura [CADES | CMS]

Nome do parâmetro: política

Tipo de dados: string

Semântica: Indica a política da assinatura. Assume um dentre os valores:

Caso padrão CADES: [ADRB, ADRT, ADRV, ADRC, ADRA];

caso padrão CMS [ETSI_B, ETSI_T, ETSI_LT, ETSI_LTA].

Nome do parâmetro: data e hora da assinatura

Tipo de dados: data

Semântica: data e hora da assinatura. Considerada para validação do certificado em caso de inexistência de carimbo do tempo.

Nome do parâmetro: status dos certificados

Tipo de dados: Tipo Status dos Certificados

Semântica: array contendo informações do certificado do signatário e dos certificados da sua cadeia de certificação.

Nome do parâmetro: carimbo do tempo

Tipo de dados: Tipo Carimbo do Tempo

Semântica: informações do carimbo do tempo e do certificado que o assina.

Tipo Status dos Certificados

Nome do parâmetro: informações

Tipo de dados: string

Semântica: texto indicando observações sobre indicadores opcionais ao documento DOC-ICP 04

Nome do parâmetro: alertas

Tipo de dados: string

Semântica: texto indicando recomendações indicadas pelo documento DOC-ICP 04

Nome do parâmetro: erros

Tipo de dados: string

Semântica: texto indicando descumprimentos ao documento DOC-ICP 04

Nome do parâmetro: status

Tipo de dados: string

Semântica: Enumeração indicando cumprimento às normas do documento DOC-ICP 04

Nome do parâmetro: data de revogação

Tipo de dados: data e hora

Semântica: data e hora de expiração da validade do certificado

---

Nome do parâmetro: data de verificação

Tipo de dados: data e hora

Semântica: data e hora da verificação da validade do certificado conforme LCRs (Lista de Certificados Revogados) da cadeia de certificação.

Nome do parâmetro: ICP-Brasil

Tipo de dados: booleano

Semântica: indicativo de que o certificado está sujeito à cadeia ICP-Brasil

---

Nome do parâmetro: Dados do Certificado

Tipo de dados: Tipo Dados do Certificado

Semântica: descrição do certificado

Tipo Carimbo do Tempo

Nome do parâmetro: informações

Tipo de dados: string

Semântica: texto indicando observações sobre indicadores opcionais ao documento DOC-ICP 04

Nome do parâmetro: alertas

Tipo de dados: string

Semântica: texto indicando recomendações indicadas pelo documento DOC-ICP 04

Nome do parâmetro: erros

Tipo de dados: string

Semântica: texto indicando descumprimentos ao documento DOC-ICP 04

Nome do parâmetro: status

Tipo de dados: string

Semântica: Enumeração indicando cumprimento às normas do documento DOC-ICP 04

Nome do parâmetro: data de revogação

Tipo de dados: data e hora

Semântica: data e hora de expiração da validade do certificado

---

Nome do parâmetro: algoritmo da assinatura

Tipo de dados: data e hora

Semântica: data e hora da verificação da validade do certificado conforme LCRs (Lista de Certificados Revogados) da cadeia de certificação.

Nome do parâmetro: data e hora da assinatura

Tipo de dados: data e hora

Semântica: data e hora da assinatura do documento segundo Hora Legal Brasileira obtido do Observatório Nacional através de equipamento homologado pelo ITI conforme normas ICP-Brasil.

Nome do parâmetro: Dados do Certificado do Carimbo do Tempo

Tipo de dados: Tipo Dados do Certificado do Carimbo do Tempo

Semântica: descrição do certificado que assina o carimbo do tempo

---

Tipo Status do Certificado

Nome do parâmetro: authorityKeyIdentifier

Tipo de dados: string

Semântica: chave pública do certificado em base64.

Nome do parâmetro: Issuer

Tipo de dados: json

Semântica: atributos do Issuer do certificado conforme rfc5280 em conformidade com DOC-ICP 04.

{
"c": "string",
"cn": "string",
"dn": "string",
"e": "string",
"email": "string",
"formattedCn": "string",
"l": "string",
"o": "string",
"ou": [
"string"
],
"st": "string"
}

Nome do parâmetro: status

Tipo de dados: string

Semântica: Enumeração indicando cumprimento do certificado às normas do documento DOC-ICP 04

Nome do parâmetro: data de revogação

Tipo de dados: data e hora

Semântica: data e hora de expiração da validade do certificado

---

Nome do parâmetro: data de emissão

Tipo de dados: data e hora

Semântica: data e hora de início da validade do certificado

Nome do parâmetro: data de validade

Tipo de dados: data e hora

Semântica: data e hora de expiração da validade do certificado

---

Tipo Dados do Certificado do Carimbo do Tempo

Nome do parâmetro: Certificado holder

Tipo de dados: Tipo Status do Certificado

Semântica: dados do certificado do emissor do certificado do signatário do carimbo do tempo

---

Nome do parâmetro: Certificado issuer

Tipo de dados: Tipo Status do Certificado

Semântica: dados do certificado do signatário do carimbo do tempo

---

20.9 Exemplo de Estrutura de Dados

```
// ********************************************************
// ********************************************************
// Requisito 11, Etapa 1: Gerar Hash para assinatura
// ********************************************************
// ********************************************************
Requisito11Etapa1Request: {
    tipo de Operação // [ASSINATURA, COASSINATURA, CONTRA_ASSINATURA ]
    padrão, // [ CADES, CMS ]
    política, // [ ADRB, ADRT, ADRV, ADRC, ADRA,  ETSI_B, ETSI_T, ETSI_LT, ETSI_LTA ]
//Políticas ICP-Brasil e CMS
    certificado, // certificado público do signatário em Base64
    algoritmo de HASH, // algoritmo que gerou o hash do arquivo original [ SHA1, SHA256,
SHA512, (...) ]
    documentos originais: [{
            identificador do
                documento, // identificador para rastreamento do arquivo no processo.
                hash do
                    arquivo original, // hash do arquivo detachado, parâmetro da operação
'Gerar Hash para assinatura'
                    assinatura detachada, // caso coassinatura ou contra-assinatura
                    hash da assinatura detachada // caso coassinatura ou contra-assinatura
        }
    ]
}

// ********************************************************
Requisito11Etapa1Response:
[{
        identificador de documento, // identificador para rastreamento do arquivo no processo.
        hash para assinatura // atributos da assinatura para cifragem (Requisito 11, etapa 2)
    }
]
```

```
// ********************************************************
// ********************************************************
// Requisito 11, Etapa 3: FinalizarAssinatura
// ********************************************************
// ********************************************************
Requisito11Etapa3Request{
    tipo de Operação // [ASSINATURA, COASSINATURA, CONTRA_ASSINATURA ]
    padrão, // [ CADES, CMS ]
    política, // [ ADRB, ADRT, ADRV, ADRC, ADRA,  ETSI_B, ETSI_T, ETSI_LT, ETSI_LTA ]
//Políticas ICP-Brasil e CMS
    certificado, // certificado público do signatário em Base64
    algoritmo de HASH, // algoritmo que gerou o hash do arquivo original [ SHA1, SHA256,
SHA512, (...) ]
    assinaturas: [{
            identificador do documento, // identificador para rastreamento do arquivo no
processo.
            assinatura detachada, // caso coassinatura ou contra-assinatura
            hash do arquivo original, // hash do arquivo detachado, parâmetro da operação
'Gerar Hash para assinatura'
            hash para assinatura, // Produto do da operação 'Gerar Hash para assinatura
(Requisito 11, Etapa 1)'
            hash para assinatura cifrado, // Produto cifrado da operação 'Gerar Hash para
assinatura (Requisito 11, Etapa 2)'
        }
    ],
}

// ********************************************************
Requisito11Etapa3Response
[{
        identificador de documento, // identificador para rastreamento do arquivo no processo.
        assinatura detachada
    }
]
```

```
// ********************************************************
// ********************************************************
// Validação de assinatura
// ********************************************************
// ********************************************************
ValidarAssinaturaRequest:
[{
        identificador do documento, // identificador para rastreamento do arquivo no processo.
        assinatura detachada, // assinatura do arquivo
        hash do arquivo original[], // para cada assinatura do arquivo, utilizar o algoritmo de
hash da assinatura para gerar hash do conteúdo do arquivo original
    }
]

// ********************************************************
ValidarAssinaturaResponse:
[{
        status geral, // indica erros na assinatura
        status integridade do arquivo, // permite diferenciar erros no processo de assinatura
ou arquivo corrompido
        verificação das assinaturas: [{ // registro para cada assinatura do arquivo
                informações: [{
                        descrição
                    }
                ],
                alertas: [{
                        descrição
                    }
                ],
                erros: [{
                        descrição
                    }
                ],
                status, // [ VALIDO, INVÁLIDO ]
                formato, // [ PADES, XADES, CADES, CMS]
                status da assinatura: {
                    alertas: [{
                            descrição
                        }
                    ],
                    status da cadeia de certificação: [{
                            informações: [{
                                    descrição
                                }
                            ],
                            alertas: [{
                                    descrição
                                }
                            ],
                            erros: [{
                                    descrição
                                }
                            ],
                            status // [ VALIDO, INVÁLIDO ]
                            contra assinaturas: [] // fomato idem a '$.verificação das
assinaturas[]'
                            algoritmo de hash da assinatura,
                            formato da assinatura, // [PADES, XADES, CADES, CMS]
```

```
                        data e hora da assinatura,
                        status dos certificados: [{
                                informações: [{
                                        descrição
                                    }
                                ],
                                alertas: [{
                                        descrição
                                    }
                                ],
                                erros: [{
                                        descrição
                                    }
                                ],
                                tipo do certificado, // [A1, ...]
                                status, // [ VALIDO, INVÁLIDO ]
                                data de revogação, // nulo se não revogado
                                data hora da verificação, // data e hora da validação do
certificado
                                ICP - Brasil // booleano
                                status do certificado: {
                                    authorityKeyIdentifier,
                                    certificateIssuer: {
                                        c,
                                        cn,
                                        dn,
                                        e,
                                        email,
                                        formattedCn,
                                        l,
                                        o,
                                        ou: [],
                                        st
                                    },
                                    status, // [ VALIDO, INVÁLIDO ]
                                    data de revogação, // nulo se não revogado
                                    valido a partir de,
                                    valido até
                                },
                            }
                        ],
                        carimbo do tempo: {
                            informações: [{
                                    descrição
                                }
                            ],
                            alertas: [{
                                    descrição
                                }
                            ],
                            erros: [{
                                    descrição
                                }
                            ],
                            status, // [ VALIDO, INVÁLIDO ]
                            algoritmo da assinatura,
                            data e hora da assinatura, // Hora Legal Brasileira segundo
observatório nacional
```

```
                                timeStampAttributeCertificate: {
                                    holder: {
                                        authorityKeyIdentifier,
                                        certificateIssuer: {
                                            c,
                                            cn,
                                            dn,
                                            e,
                                            email,
                                            formattedCn,
                                            l,
                                            o,
                                            ou: [],
                                            st
                                        },
                                    },
                                    issuer: {
                                        authorityKeyIdentifier,
                                        certificateIssuer: {
                                            c,
                                            cn,
                                            dn,
                                            e,
                                            email,
                                            formattedCn,
                                            l,
                                            o,
                                            ou: [],
                                            st
                                        },
                                    },
                                    status, // [ VALIDO, INVÁLIDO ]
                                    data de revogação // nulo se não revogado
                                    valido a partir de,
                                    valido até
                                }
                            }
                        }
                    ]
                }
            }
        ]
    }
]
```