

Estudo Técnico Preliminar 6/2025

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

A Diretoria de Tecnologia da Informação e Comunicação (DTI/PF) é responsável pela especificação e padronização do parque computacional e tecnológico da Polícia Federal, desenvolvendo metodologias de trabalho e agregando conhecimento técnico para difusão entre as descentralizadas, inclusive por meio de intercâmbio com outras instituições.

Os sistemas e serviços corporativos de Tecnologia da Informação e Comunicação exigem a utilização de mecanismos digitais de verificação de identidade de usuários, bem como da autenticidade e da originalidade de documentos digitais. Tais mecanismos são normalmente implementados por meio de serviços de autoridades certificadoras digitais.

Deseja-se contratar a emissão de novos certificados digitais do tipo A1 para uso nos servidores de aplicações, possibilitando a verificação da identidade desses equipamentos junto aos usuários dos sistemas corporativos, prevenindo a ocorrência de ataques e fraudes que possam comprometer a prestação de serviços e a imagem institucional da PF.

Além dos certificados de máquina do tipo A1, existe grande demanda na PF pela emissão de certificados digitais pessoais do tipo A3, os quais são utilizados principalmente para a autenticação da identidade dos usuários nos acessos aos sistemas e para realizar a assinatura de documentos digitais, que necessitem de validade legal.

São exemplos de aplicações que demandam a utilização de certificados digitais o sistema PJe, do Poder Judiciário, e o SIAFI, da Secretaria do Tesouro Nacional.

Com a utilização de certificados digitais é possível criar mecanismos para verificar a identidade de máquinas que disponibilizam serviços informatizados, assim como permitir que os portadores de certificados realizem a assinatura digital e a criptografia de documentos e e-mails.

Por fim, os serviços de autoridade certificadora também englobam a emissão de certificados de carimbo de tempo. A demanda por esse tipo de serviço se justifica pela necessidade de se estabelecer mecanismos de comprovação do momento exato da criação de determinados arquivos digitais que são utilizados como evidências em processos criminais, garantindo assim a cadeia de custódia da evidência.

Atualmente, os serviços de certificação digital na PF são prestados pela empresa VALID CERTIFICADORA DIGITAL LTDA por meio do Contrato nº 15/2022, vigente desde 30/12/2022. No entanto, o volume e a qualidade dos serviços têm se mostrado insuficientes para atendimento das demandas da Polícia Federal, em particular para os certificados digitais pessoais A3, conforme atestam os Despachos SEI 29181406 e 29949816.

Deve ser considerado ainda que durante a pandemia da Covid-19 foram feitas alterações nas regulamentações seguidas pelas entidades (Autoridades Certificadoras e Autoridades de Registro) vinculadas à ICP-BRASIL, passando a ser possível a emissão de certificados digitais pessoais por meio de videoconferência além do mecanismo anteriormente vigente que tornava obrigatória a presença física do titular em uma Autoridade de Registro, devendo o contrato estabelecer parâmetros de serviço específicos para essa modalidade de atendimento.

A PF possui diversos serviços disponibilizados aos usuários externos através da rede Internet e os dados trafegados nos acessos muitas vezes contêm informações privadas, tanto de usuários, quanto do própria PF. Desta forma, existe a necessidade da utilização de mecanismos de segurança na comunicação entre os usuários e a Polícia Federal. A certificação digital é um tipo de mecanismo de segurança de identificação que permite que operações eletrônicas dos mais diversos tipos sejam feitas considerando a integridade, a autenticidade, a confidencialidade e o não repúdio dessas transações. A autenticidade garante a autoria de um documento, o acesso legítimo a um sistema, entre outros. A integridade garante que as informações não foram alteradas sem a devida autorização. A confidencialidade garante que as informações privativas não serão acessadas por terceiros. O não-repúdio impede que o autor do documento ou da autenticação do sistema conteste a sua validade negando sua autoria.

O certificado digital é amplamente usado, tanto no setor público quanto no privado, e constitui uma forma de garantir ao usuário a autenticidade das informações acessadas, além de assegurar que todos os dados disponibilizados estão protegidos contra

acesso indevido ou adulteração do seu conteúdo. Seguindo a tendência de grandes instituições privadas, os órgãos governamentais, sentindo necessidade de impor agilidade, facilidade e custos mais baixos aos seus serviços, criam Portais Institucionais e abrem seus sistemas de informação e serviços para a Internet. Uma das formas de manter a segurança na comunicação e a confiança dos usuários nesses Portais é através da implementação de uma base de certificados digitais.

De acordo com as melhores práticas em tecnologia da informação, os dados e as informações devem receber um nível adequado de proteção que considere o potencial de impacto causado pela perda de integridade ou de sigilo. Considerando a importância dos sistemas de informação sob responsabilidade da PF, faz-se necessária a manutenção dos certificados digitais para servidores web onde estão hospedados os Portais e serviços disponíveis na internet pela Polícia Federal.

Considerando, portanto, as necessidades da Polícia Federal, a presente contratação se destina a:

1. Permitir a emissão de certificados digitais de máquina (A1) suficientes para todos os serviços e sistemas informatizados da PF, que são disponibilizados para os públicos interno e externo, considerando inclusive a emissão de certificados do tipo wildcard para os domínios pf.gov.br e dpf.gov.br em cadeia de certificação internacional;
2. Permitir a emissão de certificados digitais pessoais (A3) para todos os servidores da PF e para as pessoas jurídicas (CNPJs) integrantes da instituição, considerando eventualmente o fornecimento das mídias (tokens ou smartcards) nas quais esses certificados serão armazenados, e ainda o modelo de fornecimento de certificado "em nuvem" sem token físico (cuja validação do uso é feita através do smartphone);
3. Permitir a emissão de certificados de carimbo de tempo para todos os arquivos que poderão consistir em evidências digitais a serem utilizadas em investigações, como, por exemplo, os laudos produzidos no Sistema de Criminalística (SISCRIM);

3. Área requisitante

Área Requisitante	Responsável
DISEG/CGTI/DTI/PF	Bruno Werneck Pinto Hoelz

4. Necessidades de Negócio

Conforme previsto na IN nº 94 de 23/12/22, o Estudo Técnico Preliminar da Contratação deve definir e especificar as necessidades de negócio e tecnológicas, e os requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

Necessidade 1: Garantir a confidencialidade, integridade e segurança das informações disponibilizadas pelos diversos sistemas e aplicações da Polícia Federal aos seus clientes internos e externos. Funcionalidade: Contratação de serviço de emissão de certificados digitais A1 padrão ICP-Brasil para servidores, de forma a garantir a segurança do meio de comunicação (e-CNPJ e site).

Necessidade 2: Garantir a confiabilidade, integridade, autoria e não repúdio das informações e documentos gerados e mantidos em meio digital pela Polícia Federal. Funcionalidade: Contratação de serviço de emissão de certificados digitais A3 sob a cadeia ICP-Brasil (e-CPF).

Necessidade 3: Garantir a temporalidade e veracidade dos documentos eletrônicos assinados digitalmente. Funcionalidade: Contratação de serviço de emissão de carimbos de tempo de forma a atestar que uma determinada informação digital existia em uma determinada data e hora do passado.

5. Necessidades Tecnológicas

Necessidade	ID	Requisito
1	1	O certificado deve estar sob a cadeia ICP-Brasil e em plena conformidade com os requisitos nela estabelecidos.
1	2	O certificado deve possuir prazo de validade mínimo de 1 (um) ano.
1	3	A AC deve permitir a verificação do status do certificado, identificando os vencidos e revogados.
2	1	O certificado deve estar sob a cadeia ICP-Brasil e em plena conformidade com os requisitos nela estabelecidos.
2	2	O certificado deve possuir prazo de validade mínimo de 3 (três) anos.
2	3	O certificado deve ser armazenado em mídia digital (token ou smart card) ou em nuvem.
2	4	A mídia de armazenamento deve ser compatível com os sistemas operacionais Windows e Linux, além de compatibilidade com os navegadores Mozilla Firefox e Internet Explorer.
3	1	A autoridade de carimbo de tempo (ACT) deve operar sob a cadeia ICP-Brasil, sendo credenciada pelo ITI – Instituto Nacional de Tecnologia da Informação.
3	2	A ACT deve permitir identificação e registro de todas as ações executadas.
3	3	A ACT deve ser gerenciada pelos SAS (Sistemas de Auditoria e Sincronismo) do tempo geridos pelo ITI e possuir alvará vigente emitido a fim de garantir que a precisão do sincronismo do seu relógio esteja de acordo com o relógio do SAS.
4	1	O certificado deve estar sob a cadeia ICP-Brasil e em plena conformidade com os requisitos nela estabelecidos.
4	2	O certificado deve possuir prazo de validade mínimo de 1 (um) ano.
4	3	O certificado deve ser armazenado em mídia digital (token ou smart card) ou em nuvem.
4	4	A mídia de armazenamento deve ser compatível com os sistemas operacionais Windows e Linux, além de compatibilidade com os navegadores Mozilla Firefox e Internet Explorer.

4	5	O certificado deve ser emitido por órgão de governo
---	---	---

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

Implementar altos níveis de segurança da informação que estabeleça solução tecnológica para realização de assinatura digital de documentos e transações entre sistemas através do uso de certificados digitais que atender o padrão ICP-Brasil.

7. Estimativa da demanda - quantidade de bens e serviços

Diversos sistemas, principalmente aqueles que contém informações sigilosas, são implementados de forma a exigir que seus usuários possuam um certificado digital, tais como o Sistema de Criminalística (SISCRIM), e-Pol, dentre outros. Devido à natureza das atividades executadas pela PF, principalmente aquelas relacionadas à segurança pública, faz-se necessário que os servidores do órgão possuam um certificado digital para acessar tais sistemas.

Sendo assim, verifica-se a necessidade da aquisição de certificados digitais para implementação em diversos sistemas disponibilizados pela PF e para os usuários que acessam sistemas que exigem o uso de certificados digitais, além da necessidade de assinatura digital de documentos relacionados à polícia judiciária.

Uma alteração proposta neste novo contrato, com relação ao contrato anterior, é sua duração. Os certificados digitais emitidos para pessoas físicas (e-CPF) tem validade comum de 3 anos, logo, é razoável exigir que a duração do contrato de serviço tenha pelo menos o mesmo prazo de validade, ou seja, 36 meses. A doutrina e jurisprudência do TCU (Acórdão nº 490/2012 do Plenário) autorizam essa vigência pois entendem ser possível, excepcionalmente, que a vigência dos contratos de prestação de serviços contínuos extrapole os 12 meses previstos da Lei de Licitações, desde que devidamente motivada pela Administração a vantajosidade para o interesse público. Além disso, a nova lei de licitações (Lei 14.133/21) alterou o prazo de duração dos contratos de serviços continuados para até 5 anos, conforme art. 105 e 106.

Em 19/10/2023 foi assinado o primeiro Termo Aditivo do contrato com acréscimo de 25% para os itens 02 (Certificados digitais A3 e-CPF com token, 3 anos), 03 (Certificados digitais A3 e-CPF sem token, 3 anos) e 06 (Certificados digitais A3 e-CPF em nuvem) considerando a alta demanda por esses itens.

Para estimar a quantidade de itens do contrato vigente nº 15/2022 com a empresa VALID, foi usada a média da quantidade de solicitações de itens do contrato anterior nº 16/2027 (SEI 5924770). Essa fórmula acabou se mostrando inadequada (SEI 29181406), considerando que já no segundo ano de contrato (2023) foi feito um termo aditivo para que fosse possível atender a demanda de solicitações de certificados.

Assim sendo, a soma total da quantidade de certificados A3 e-CPF do contrato deve atender a quantidade total de servidores da Polícia Federal. Um extrato do número

total de servidores da PF foi retirado do portal da Azure, totalizando 15.296. Além disso, a Portaria Nº 19.026-DG/PF, de 13 de fevereiro de 2025, autorizou a realização de concurso público para provimento de 1.000 cargos vagos do Órgão, resultando na expectativa de 16.296 servidores públicos. Como não é possível prever, com acurácia e assertividade, qual das opções de armazenamento de certificado (se em nuvem ou em token) terá maior adesão, propõe-se a aquisição do quantitativo total estimado para ambas as modalidades, resultando em 16.296 certificados digitais com armazenamento em token (Item 2) e 16.296 certificados digitais com armazenamento em nuvem (Item 4). Esse incremento serve como margem de segurança para assegurar que a modalidade de maior interesse não enfrente escassez, garantindo a disponibilidade necessária para todos os usuários.

A quantidade de certificados A1 para computadores (Item 1) deve ser mantido em 30, como no contrato atual. Esse quantitativo considera a quantidade anual de Certificados A1 emitidos, com adição de reserva técnica. Porém, como o novo contrato terá vigência de 3 anos ao invés de 1 ano e como esses certificados têm o prazo de validade de 1 ano, o novo contrato deverá prever a emissão de 90 certificados A1 durante toda sua vigência de 36 meses. Com relação ao tipo de certificado A1 para servidor (SSL/TLS), devem ser compatíveis com a infraestrutura da ICP-Brasil.

Não há necessidade de emissão de certificados A3 sem token, considerando que o valor do dispositivo do token atualmente é baixo e que incompatibilidades entre tokens de outros fabricantes podem prejudicar sobremaneira a emissão dos certificados.

Cumprando informar que nos últimos anos ocorreram demandas relacionadas à comunicação via assinatura digital de sistemas corporativos com outros órgãos, cite-se por exemplo, as demandas registradas nos processos SEI nº 08410.004652/2019-11 e 08201.000392/2021-95. Dessa forma, visando atender tais demandas é necessário adicionar ao objeto de contratação do presente Estudo Técnico Preliminar um quantitativo relacionado ao certificado do tipo e-CNPJ. A estimativa de quantitativo para os certificados do tipo A3 e-CNPJ (Item 5) considerou o número de Unidades Gestoras da Polícia Federal (que atualmente está em 32), com adição de uma reserva técnica de segurança de 8 unidades. Dessa forma, atinge-se a quantidade de 40 unidades desse tipo de certificado, como no contrato atual. Ainda, esse tipo de certificado pode possuir validade de até 3 anos ao invés de 1 ano, e serem disponibilizados de forma física. Assim sendo, o contrato deverá prever que esses certificados sejam emitidos com a validade de 3 anos com disponibilização de tokens criptográficos.

As visitas técnicas seguem sendo necessárias, mesmo com atendimento remoto, pela necessidade de atendimento aos dirigentes da Polícia Federal em suas respectivas unidades, priorizando o trabalho de gestão e supervisão que desempenham em suas lotações. O serviço de Autoridade Registradora, com a respectiva visita para validação de documentação (item 7), se justifica pela necessidade de atendimento aos dirigentes da Polícia Federal em suas respectivas unidades, de maneira que não necessitem se deslocar até a AR, priorizando o trabalho de gestão e supervisão que desempenham em suas lotações. De maneira semelhante ao Item 5, o quantitativo deste item foi calculado com base na quantidade de Unidades Gestoras da PF com adição de

reserva técnica, resultando em 42 unidades anuais, o que implica em 126 unidades totais.

Com relação ao carimbo de tempo (Item 3), a estimativa de quantitativo utilizou como referência a quantidade de emissões durante o período de vigência do atual contrato, adicionando uma reserva técnica. Considerando que a média anual de produção de documentos se mantenha ao longo dos próximos anos e que os usuários continuem consumindo mais de 60 mil carimbos de tempo por ano, somados à necessidade de mais de 160 mil carimbos de tempo reaplicados automaticamente pelo sistema em 2024 e quantidade prevista semelhante em 2026, com uma necessidade anual de carimbos de tempo de mais de 220 mil unidades. Aplicando uma reserva técnica de segurança de 10% (dez por cento), prevendo possível aumento da produção de documentos, estima-se a contratação de 250 mil carimbos de tempo por ano para atender às necessidades. Há, portanto, previsão de um quantitativo de 750 mil unidades desse item para os 36 meses de contrato.

Vale dizer que, dentre os tipos de certificados digitais do tipo A1 que a Polícia Federal utiliza para viabilizar os acessos seguros e criptografados aos serviços de TIC, temos os certificados do tipo *wildcard* o qual é um certificado de segurança SSL/TLS, que possibilita a proteção de subdomínios ilimitados dentro de um único domínio através do protocolo HTTPS, em apenas um único certificado. Esse tipo de certificado é indispensável para os serviços de correio eletrônico e serviços em nuvem contratados atualmente pela Polícia Federal. Não é possível a emissão desse tipo de certificado digital no escopo da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), portanto este tipo de certificado é a única exceção às premissas estabelecidas neste Estudo Técnico Preliminar com relação à necessidade de alinhamento ao padrão ICP-Brasil.

Com relação aos certificados *wildcard*, com validade de 1 ano, o novo contrato deverá prever a emissão de certificados *.pf.gov.br e *.dpf.gov.br durante toda a vigência do contrato. Como esse tipo de certificado tem a validade de 1 ano somente, a emissão de 2 certificados por ano totaliza 6 certificados em 3 anos.

Embora atualmente seja possível contratar certificados *wildcard* com validade de 1 ano, o CA/Browser Forum, que estabelece padrões e boas práticas para a emissão de certificados digitais, está em processo de revisão e posterior discussão do Ballot SC-081, que propõe a redução da validade desse tipo de certificado gradualmente até chegar a 47 dias, conforme a tabela a seguir:

Certificado emitido a partir de	Validade máxima (dias)
Atualmente	398
15/03/2026	200
15/03/2027	100
15/03/2029	47

No cenário de aprovação dessa proposta, as quantidades anuais necessárias desse item seriam alteradas, saindo de 1 emissão anual por domínio para aproximadamente 8 emissões anuais por domínio a partir de 15 de março de 2029. Ainda, os custos associados a essas emissões podem variar de maneira ainda imprevisível.

Além disso, existe um risco de que, ainda durante a vigência do contrato, a empresa certificadora deixe de poder emitir certificados *wildcard* com validade de 1 ano, como

originalmente previsto. Isso porque as novas regras passariam a valer independentemente dos acordos comerciais pré-existentes. Essa mudança criaria uma discrepância entre o que está contratado e o que será tecnicamente possível cumprir, exigindo renegociações para manter a continuidade do serviço sem prejudicar a segurança ou a operação.

Adicionalmente, a redução do prazo de validade dos certificados wildcard para apenas 47 dias tornará inviável a gestão manual desses ativos de segurança, exigindo automatização do processo de emissão de certificados.

Diante desse cenário apresentado, torna-se essencial a aplicação da matriz de alocação de riscos prevista nos artigos 22 e 103 da Lei nº 14.133/2021, garantindo uma alocação clara de responsabilidades entre as partes e a preservação do equilíbrio econômico-financeiro do contrato. O artigo 22 estabelece que a matriz de riscos deve definir a distribuição das responsabilidades entre a Administração e o Contratado, considerando eventos supervenientes que possam impactar a execução contratual. No caso da contratação de certificados digitais, a redução progressiva da validade, conforme proposto pelo CA/Browser Forum, representa um fator de risco que pode gerar aumento significativo no número de emissões anuais e consequente impacto financeiro. Para mitigar esse risco, a matriz de alocação de responsabilidades deve prever mecanismos para ajustes contratuais que garantam a continuidade da prestação do serviço, evitando onerar desproporcionalmente qualquer uma das partes.

Além disso, o artigo 103 da Lei nº 14.133/2021 reforça a necessidade de que os contratos administrativos contenham cláusulas que assegurem a manutenção do equilíbrio econômico-financeiro, especialmente em situações de alteração substancial das condições inicialmente pactuadas. Diante da possibilidade de que a empresa certificadora deixe de poder emitir certificados wildcard com validade de um ano, torna-se fundamental que o contrato preveja medidas para readequação dos termos contratuais, evitando descontinuidade no serviço e prejuízos à Administração Pública. Considerando que, caso se concretize a redução da validade proposta, as quantidades anuais necessárias desse tipo de certificado aumentariam consideravelmente o número atualmente necessário, a partir de março de 2029, esta EPC entende, s.m.j., que a alternativa mais viável para se evitar futuros acréscimos de quantitativos e possibilitar a execução fluida do contrato até o término de sua vigência, consideradas as possíveis prorrogações, é licitar e ter em seu contrato o quantitativo de até 93 (noventa e três) certificados, inicialmente contratados com o valor vigente, prevendo a emissão e o pagamento por demanda, limitando a demanda ao quantitativo estimado, adequado à validade vigente, necessário para atender a necessidade da administração nos respectivos períodos de emissão.

Portanto, a inclusão de uma matriz de alocação de riscos no contrato é essencial para permitir a revisão de prazos e valores, caso as novas regulamentações impactem a execução do contrato. Dessa forma, assegura-se que a Administração Pública possa manter a prestação do serviço de forma eficiente e segura, sem comprometer sua operação devido a fatores externos imprevisíveis ou previsíveis porém de consequências incalculáveis, uma vez que não é possível calcular o impacto no quantitativo de certificados, considerando que o que se tem até o momento é um cenário proposto de diminuição gradativa de validade até 2029 pendente de aprovação, e o impacto financeiro, considerando a ausência de preços para a emissão de certificados com as validades propostas. Ante todo o exposto, deverá ser previsto no Termo de Referência e no Termo de Contrato uma Matriz de Alocação de Riscos considerando o contexto de variação de validade dos Certificados do tipo Wildcard e

prevendo a alocação de riscos, no mínimo quanto a mudança de validade; risco de interrupção de serviço; impacto financeiro/revisão de preços e quantitativo à ser demandado conforme validade vigente.

8. Levantamento de soluções

Solução 1: Processo manual de assinatura manuscrita de documentos impresso em papel.

Essa solução implica em continuar com assinatura manuscrita restringindo ao princípio de autoria de um documento, em que as assinaturas seguem um padrão, sendo semelhantes entre si e possuindo características pessoais e biométricas de cada indivíduo sendo feita em algo tangível, como o papel, que é responsável pela vinculação da informação impressa à assinatura.

Esse é o modelo fortemente adotado em vários órgãos públicos atualmente, mas que demanda grande consumo de papel, prejudicando aspectos de sustentabilidade e manutenção desses documentos em arquivo que necessitam de espaço físico para acondicionamento.

Essa solução implica em custos com impressão e papel.

Solução 2: Certificado digital

Contratação de serviço de autoridade certificadora para emissão de certificado digital com a finalidade de troca de informações por meio eletrônico de modo a garantir autenticidade, confiabilidade e integridade da autoria dos documentos produzidos sem a necessidade da impressão em papel e assinatura manuscrita.

Certificado digital: documento eletrônico capaz de garantir autoria de documentos eletrônicos, pessoas e máquinas; Token: hardware capaz de gerar e armazenar chaves criptográficas que compõem os certificados digitais, que darão confiabilidade e segurança, e serviço de emissão de carimbo de tempo que é um terceiro documento eletrônico que tem como objetivo de trazer uma determinada data e hora pela Autoridade de Carimbo do Tempo.

Esse é o modelo adotado e utilizado no Ministério do Planejamento, Ministério da Fazenda, Receita Federal do Brasil, Procuradoria Geral da Fazenda Nacional e órgãos do poder judiciário que estão utilizando certificação digital em larga escala.

A autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação, ela define e verifica quais autoridades certificadoras podem emitir certificação digital mediante Comitê Gestor da ICP-Brasil, tais como: SERPRO, CAIXA, SERASA EXPERIAN, RECEITA FEDERAL, CERTISIGN entre outros.

O custo deverá ser estimado quando da cotação de preços junto a possíveis fornecedores, após a elaboração do termo de referência. E o referido quantitativo necessário e se possível verificação de economia em escala.

9. Análise comparativa de soluções

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		

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

10. Registro de soluções consideradas inviáveis

Atualmente é inviável retornar à utilização de assinatura manuscrita, pois a garantia dos atributos de não-repúdio e integridade ficariam prejudicados em larga escala, haja vista que a análise de um documento, em que as assinaturas seguem um padrão, sendo semelhantes entre si e possuindo características pessoais e biométricas de cada indivíduo sendo feita em algo tangível, exige análise manual e não escalável.

Cumprir informar que a Polícia Federal emprega esforços para melhor servir o cidadão objetivando a entrega de serviços com alto nível de qualidade e segurança, portanto, a opção pela utilização de assinatura manuscrita, dentre as opções tecnológicas disponíveis, não atende os requisitos necessários.

11. Análise comparativa de custos (TCO)

Não se aplica, pois apenas 1 (uma) solução se mostrou viável não sendo possível realizar comparação com outra, conforme previsto na IN nº 94 de 23/12/22.

12. Descrição da solução de TIC a ser contratada

Após análise comparativa das soluções identificadas, a equipe de planejamento da contratação entende como viável a Solução 2 para o item de certificados digitais de órgão de governo e a Solução 2 para o item de certificados digitais gerais. Essas Soluções atendem às necessidades da Polícia Federal.

A empresa que fornece a solução contratada deverá atender aos seguintes requisitos:

- a) prestar o serviço de certificação digital contemplando todos os itens do objeto da contratação;
- b) obedecer aos requisitos estabelecidos pela ICP-Brasil, no que couber;
- c) permitir a validação documental e identificação presencial do titular do certificado digital em pelo menos todas as capitais do Brasil.

13. Estimativa de custo total da contratação

Valor (R\$): 2.776.562,70

Para estimativa do custo de cada item, considerou-se a Pesquisa de Preço realizada, conforme Nota Técnica (Anexo I). Estima-se que o valor da contratação em 3 anos será de R\$ 2.776.562,70, conforme detalhado na tabela abaixo:

	Certificados digitais (A1), 1 ano, para computador servidor	Certificados digitais (A3), 3 anos, c/ TOKEN	Carimbo de tempo (ACT) ICP-Brasil	* Certificados digitais (A3), 3 anos, em NUVEM	* Certificados digitais (A3), 3 anos, em TOKEN, e- CNPJ	* Certificados digitais A1 WILDCARD, 1 ano	Visita técnica para validação dos documentos dos solicitantes
Custo unitário estimado (R\$)	453,50	88,00	0,60	51,00	62,45	785,50	105,30
Quantidade total estimada	90	16296	750.000	16296	42	6	126
Valor total (R\$)	40.815,00	1.434.048,00	450.000,00	831.096,00	2.622,90	4.713,00	13.267,80

Valor total estimado	R\$ 2.776.562,70	
----------------------	------------------	--

14. Justificativa técnica da escolha da solução

A solução pretendida está alinhada à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a Lei 11.419/2006 e com a MP nº 2.200-2, que prevê que documentos eletrônicos assinados digitalmente com o uso de certificado digital emitidos no âmbito da ICP-Brasil tenham a mesma validade jurídica que os documentos em papel com assinaturas manuscritas.

Através de certificados digitais emitidos por autoridades certificadoras, é possível criar mecanismos para verificar a identidade de máquinas que disponibilizam serviços informatizados - utilizando certificados do tipo A1 e Carimbos de Tempo -, assim como permitir que os portadores de certificados realizem a assinatura digital e a criptografia de documentos e e-mails - utilizando certificados do tipo A3.

Atualmente os serviços de certificação digital são prestados pela empresa VALID CERTIFICADORA DIGITAL LTDA por meio do Contrato nº 15/2022, vigente desde 30/12/2022. No entanto, o volume e a qualidade dos serviços têm se mostrado insuficientes para atendimento das demandas da Polícia Federal, em particular para os certificados digitais pessoais A3, conforme atestam os Despachos SEI 29181406 e 29949816.

Deve ser considerado ainda que durante a pandemia da Covid-19 foram feitas alterações nas regulamentações seguidas pelas entidades (Autoridades Certificadoras e Autoridades de Registro) vinculadas à ICP-BRASIL, passando a ser possível a emissão de certificados digitais pessoais por meio de videoconferência além do mecanismo anteriormente vigente que tornava obrigatória a presença física do titular em uma Autoridade de Registro, devendo o contrato estabelecer parâmetros de serviço específicos para essa modalidade de atendimento.

Assim, torna-se necessária nova contratação de forma a permitir que a demanda por novos certificados seja atendida.

A partir da existência de um contrato de serviços, a Polícia Federal poderá demandar a emissão de novos certificados digitais do tipo A1. Os certificados A1 são utilizados nos servidores de aplicações para possibilitar a verificação da identidade da máquina pelos usuários dos sistemas institucionais, prevenindo ataques e fraudes que possam comprometer a prestação de serviços e a imagem institucional.

Além dos certificados de máquina do tipo A1, existe grande demanda na PF pela disponibilidade de certificados digitais pessoais A3. Os certificados pessoais A3 são principalmente utilizados para realizar a assinatura de documentos digitais, que possuem validade legal para todos os fins. Há previsão legal de que os certificados digitais sob a hierarquia ICP-Brasil, regulamentados pelo Instituto Nacional de Tecnologia da Informação, instituído pela Medida Provisória nº 2.200-2, sejam utilizados para que os documentos eletrônicos assinados digitalmente tenham a mesma validade jurídica que os documentos em papel com assinaturas manuscritas.

A contínua demanda por certificados A3 se justifica pela implantação e evolução de novos sistemas corporativos que lidam exclusivamente com documentos digitais, como é o caso dos sistemas SEI, e-POL e Sistema de Criminalística (SISCRIM), mas também devido a sistemas de outras instituições que demandam esse recurso, como os sistemas utilizados pelos Tribunais Federais.

Os sistemas que fazem parte da modernização da polícia judiciária, tal como o e-POL e o SISCRIM, exigem que os servidores públicos, bem como os documentos gerados por estes no curso dos inquéritos policiais, tenham a sua autenticidade comprovada. Essa comprovação é garantida mediante o uso de certificados digitais pessoais do tipo A3. Na maioria dos casos, esses certificados são gerados e armazenados em dispositivos, denominados tokens, para atender às normas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), criada pela Medida Provisória n. 2.200-2.

Os serviços de autoridade certificadora também englobam a emissão de certificados de carimbo de tempo. A demanda por esse tipo de serviço se justifica pela necessidade de se estabelecer mecanismos de comprovação de que determinado arquivo digital existia em determinada data e hora. Esses arquivos digitais devem ser utilizados como evidências em processos criminais, garantindo assim a cadeia de custódia da evidência.

Diante dos elementos apresentados, constatou-se que a Solução 2: “Contratação de serviço de autoridade certificadora para emissão de certificado digital com a finalidade de troca de informações por meio eletrônico de modo a garantir autenticidade, confiabilidade e integridade da autoria dos documentos produzidos sem a necessidade da impressão em papel e assinatura manuscrita” apresenta mais elementos que justifiquem a sua escolha como solução adequada para atender aos requisitos básicos desse estudo preliminar.

15. Justificativa econômica da escolha da solução

O custo operacional da Solução 1 considera a assinatura manual de documentos, não sendo compatível com o cenário tecnológico e a convergência digital vislumbrada no âmbito da administração pública federal. Além disso, o uso de certificados digitais automatiza e agiliza o processo de assinatura de documentos, reduzindo significativamente o tempo e o esforço necessários para a autenticação manual, o que, em larga escala, gera economia de recursos humanos e operacionais. Adicionalmente, o uso de certificados digitais diminui o risco de erros, aumenta a segurança das transações e promove maior confiabilidade jurídica, enquanto o processo manual está sujeito a falhas, retrabalho e maiores custos com logística e armazenamento de documentos físicos. A segurança aprimorada oferecida pelos certificados digitais também contribui para a proteção contra fraudes e acessos não autorizados, reduzindo riscos financeiros e reputacionais. Portanto, a contratação do serviço de emissão de certificados digitais aumenta a eficiência e também representa uma solução mais econômica e sustentável a longo prazo.

16. Benefícios a serem alcançados com a contratação

A contratação do serviço de certificado digital eleva os níveis de segurança da informação garantindo, dentre outros benefícios, a produção de documento digitais e a validação de sistemas fornecidos pela Polícia Federal reforçando aspectos relacionados a integridade e não-repúdio. Dessa forma, propiciando a entrega de serviços com maior agilidade e qualidade no ambiente de TIC. Assim, alguns dos benefícios são:

- **Segurança nas Transações Eletrônicas:** Certificados digitais garantem a autenticidade e a integridade das comunicações e transações online, protegendo contra fraudes;
- **Autenticação de Identidade:** Proporciona uma forma segura de verificar a identidade de usuários, dispositivos ou servidores, evitando acesso não autorizado;
- **Assinatura Digital:** Permite a assinatura de documentos eletrônicos com validade jurídica, substituindo a assinatura manuscrita em muitos casos. Essa assinatura também garante a integridade dos dados, já que qualquer modificação no conteúdo invalida a assinatura;
- **Redução de Custos Operacionais:** Automatiza e facilita processos que, de outra forma, exigiriam verificação manual ou documentos em papel, como assinaturas de contratos;
- **Facilidade na Automação de Processos:** Com o uso de certificados digitais, processos como a autenticação em sistemas podem ser automatizados, aumentando a eficiência.

17. Providências a serem Adotadas

Os itens será processado por meio de licitação, com o objetivo de garantir a ampla competitividade entre os potenciais fornecedores, visando à obtenção da proposta mais vantajosa, conforme os princípios da economicidade e eficiência.

Ainda, caso o Ballot SC-081 seja aprovado no CA/B Forum, com redução da validade de certificados wildcard para 47 dias a partir de 15 de março de 2029, passará a ser necessário que a emissão desse tipo de certificado se dê de maneira automatizada, já que a frequência de ocorrência desse processo tornará o processo manual inviável.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Considerando o estudo aqui apresentado, a contratação do serviço de emissão de certificados digitais é tida como viável, pois atende a demanda existente respeitando os princípios da economicidade e eficiência da administração pública.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

BRUNO WERNECK PINTO HOELZ

Integrante Requisitante



Assinou eletronicamente em 27/06/2025 às 15:42:52.

FREDERICO IMBROISI MESQUITA

Integrante Requisitante Substituto

GABRIEL ARQUELAU PIMENTA RODRIGUES

Integrante Técnico



Assinou eletronicamente em 27/06/2025 às 12:03:14.

Despacho: Aprovo o presente Estudo Técnico Preliminar

ADEMIR DIAS CARDOSO JUNIOR

Diretor de Tecnologia da Informação e Inovação DTI/PF - Autoridade Máxima de TIC



Assinou eletronicamente em 02/07/2025 às 14:24:04.