

Estudo Técnico Preliminar 42/2024

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.

Adicionalmente, a Polícia Federal, como órgão da administração pública, atua em todos os Estados do País por meio de suas Superintendências Regionais (SRs). Cada SR é uma Unidade Gestora (UG) com competência para planejar, dirigir, supervisionar, coordenar, orientar, fiscalizar e avaliar a execução das atividades relacionadas à atuação da PF. Os Ordenadores de Despesas (ODs), municiados por dados do sistema, tomam decisões que visam à alocação eficiente e eficaz dos recursos públicos. Para isso, acessam o sistema SIAFI para autorizar pagamentos, gerenciar ordens de pagamento, consultar saldos e desempenhar outras responsabilidades inerentes à função.

Em todas as Unidades Gestoras (UG) da PF, o sistema SIAFI é utilizado pelos servidores da área de contratos para gerenciar contas de contratos e garantias, registrar instrumentos contratuais firmados pela União com fornecedores e realizar baixas em saldos de contratos.

Também é utilizado pelos servidores das áreas de execução orçamentária e financeira para atividades como pagamento de faturas autorizadas pelo OD, emissão de empenhos, recolhimento de impostos e pagamento de diárias. Os gestores financeiros e seus substitutos em cada UG também utilizam o sistema para gerir adequadamente os recursos públicos da unidade e conduzir atividades relacionadas ao encerramento do exercício financeiro.

O sistema SIAFI desempenha um papel essencial na Administração Pública, fornecendo informações gerenciais confiáveis e precisas para todos os níveis da Administração. Seu acesso seguro contribui para minimizar riscos de invasões no sistema e eventuais prejuízos ao erário.

As atribuições do Sistema de Contabilidade Federal no âmbito da Polícia Federal são exercidas pelo Serviço de Contabilidade (SECONT), conforme estabelecido nas Portarias nº 115/2010-MJ e nº 1/2014-MJ. Os servidores da área de contratos e de execução orçamentária e financeira seguem os normativos mencionados, bem como o Manual SIAFI (Link: Manual SIAFI (tesouro.gov.br)) e as orientações da SECONT/CGOF/DLOG/PF.

Seguindo essa lógica, o acompanhamento contábil e de custos das Unidades Gestoras da Polícia Federal é realizado por meio dos processos de conformidade contábil e de custos da Unidade Gestora. Cada unidade renova seu processo anualmente. Para ser tramitado é essencial que o referido processo seja alimentado com os dados disponibilizados no sistema SIAFI.

As atribuições do SECONT/CGOF/DLOG/PF estão previstas na Instrução Normativa nº 270/2023-DG/DPF, que define as competências específicas das unidades centrais e descentralizadas da Polícia Federal, bem como no Decreto nº 6.976/2009, que dispõe sobre o Sistema de Contabilidade Federal e estabelece outras providências.

O uso de certificados digitais emitidos por autoridade certificadora de governo por parte de operadores, ou seja, usuários que possuem perfil de acesso que não seja exclusivamente de consulta, no âmbito da Administração Pública, será essencial para o acesso ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) a partir de 31/10/2024, conforme comunicado do Tesouro Nacional (STN) por meio do documento SEI 36275168. O STN, como órgão central do Sistema de Contabilidade Federal, é responsável por gerenciar o sistema SIAFI e tem implementado recentemente ações voltadas ao aprimoramento da segurança das credenciais de acesso dos servidores envolvidos nas diversas funções operacionais do sistema.

A ausência dos certificados mencionados resultaria em dificuldades de acesso ao sistema SIAFI por parte dos servidores da Polícia Federal, acarretando uma série de contratemplos administrativos e gerando riscos de interrupção de serviços que dependem desse acesso. Em outras palavras, todos os serviços que requerem pagamentos com recursos públicos da unidade seriam afetados.

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);
- 4. Permitir a emissão de certificados digitais necessários para assinatura de documentos no sistema SIAFI, que só poderá ser efetuada por certificados digitais emitidos pelos órgãos de governo, conforme Ofício-Circular nº 40/2024/SPO/SE/MJ (SEI 36275168).

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.

Necessidade 4: Garantir os acessos dos operadores ao sistema SIAFI, evitando riscos de interrupções nas atividades essenciais ao bom funcionamento da PF. Funcionalidade: Contratação de serviço de emissão de certificados digitais por órgão de governo.

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

Considerando as necessidades tecnológicas, os serviços de emissão de certificados digitais são divididos em duas categorias. A primeira que deve necessariamente ser emitida por órgãos de governo, e a segunda que não tem essa restrição.

Essa subcategorização existe em decorrência da exigência da STN para utilização do sistema SIAFI, o que implica na criação da categoria 1. Certificados digitais emitidos por órgão de governo. Para os demais certificados, no entanto, essa exigência não é aplicada e, para que não haja restrição de participação de outras empresas no processo, é criada a categoria 2. Certificados digitais gerais.

7.1. Certificados digitais emitidos por órgão de governo

A seguir a quantidade de usuários SIAFI que necessitam do certificado emitido por autoridade certificadora do governo para continuarem com acesso ao sistema. Essa tabela está em conformidade com o documento SEI 36766125:

USUÁRIOS SIAFI COM PERFIL DE EXECUTOR		
Código	Unidade Gestora	Quantidade de Usuários SIAFI
200334	COORDENACAO GERAL DE ADMINISTRACAO - CGAD	72
200336	CGOF/DLOG	18
200338	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - DF	14
200340	ACADEMIA NACIONAL DE POLÍCIA- DF	19
200342	DIRETORIA DE TECNOLOGIA DA INFORMACAO - DTI	23

200344	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- SE	13
200346	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - BA	13
200350	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - MG	25
200352	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - ES	17
200354	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - MS	23
200356	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - RJ	22
200358	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - AL	11
200360	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- SP	36
200364	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- PR	26
200366	DIVISAO DE POLICIA FEDERAL - FOZ DO IGUACU/PR	19
200370	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - SC	22
200372	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- RS	19
200374	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - MT	21

200376	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - GO	15
200378	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - RO	21
200380	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - AC	22
200382	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - AM	13
200384	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - RR	18
200386	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- PA	14
200388	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- MA	17
200390	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - PI	19
200392	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - CE	19
200394	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- RN	12
200396	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- PB	13
200398	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- PE	21
200402	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL - AP	12

200404	SUPERINTENDENCIA REG.DEP.POLICIA FEDERAL- TO	18
200406	DIRETORIA TECNICO-CIENTIFICA-DITEC/DPF	20
200615	DGP	11

TOTAL

678

A tabela apresentada anteriormente totaliza 678 (seiscentos e setenta e oito) usuários do SIAFI.

Em relação a lista de usuários do SIAFI com o perfil de EXECUTOR foi desconsiderado os **132** (cento e trinta e dois) ordenadores de despesas e gestores financeiros titulares e substitutos que já possuem o certificado digital concedido pelo SERPRO em decorrência da alteração na sistemática de autorização de pagamento no SIAFI no mês de abril de 2024.

Dessa forma, o quantitativo total de usuários que necessitarão da certificação digital cadastrados atualmente no SIAFI será de **546** (quinhentos e quarenta e seis).

O Serviço de Contabilidade (SECONT/CGOF/DLOG/PF) sugere a aquisição de mais **200** (duzentos) certificados para compor a reserva técnica com intuito de atender a novos operadores, gestores financeiros e ordenadores de despesas durante a vigência contratual.

Com isso, conforme apresentado no documento SEI 36765898, o **Serviço de Contabilidade propõe a aquisição de 746 (setecentos e quarenta e seis) certificados digitais emitidos por autoridade certificadora de órgão governamental.**

7.2. Certificados digitais gerais

Além disso, seguindo essa premissa de segurança, 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 (30/01/2024). Ao menos 30% (4.588) desses certificados e-CPF devem ser entregues em nuvem, para que sejam utilizados em dispositivos móveis (smartphones e tablets), algo que certificados em token físicos não possibilitam.

A quantidade de certificados A1 para computadores deve ser mantido em 30, como no contrato atual. 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.

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.

As visitas técnicas também não são mais necessárias, considerando que vai ser possível realizar a validação da documentação via vídeo conferência.

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 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. Assim sendo, o contrato deverá prever que esses certificados sejam emitidos com a validade de 3 anos.

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.

E por último, com relação ao carimbo de tempo, o novo contrato deverá prever a emissão da mesma quantidade de 250 mil unidades anuais, totalizando 750 mil unidades no período de 3 anos.

8. Levantamento de soluções

Considerando os requisitos básicos dessa demanda, as soluções são levantadas novamente se considerando as duas categorias de certificados digitais.

8.1. Certificados digitais emitidos por órgão de governo

A Subsecretaria de Planejamento e Orçamento comunicou à Polícia Federal, por meio do Ofício-Circular nº 40/2024/SPO/SE/MJ (36272949), as alterações na forma de autenticação de usuários do SIAFI, implementadas pela STN. Para aumentar a segurança e impedir utilizações indevidas ou desautorizadas, foram adotadas as seguintes medidas: exigência de certificado digital, fixação de IP de origem e habilitação do duplo fator de autenticação. Além disso, a assinatura de documentos no SIAFI só poderá ser realizada por meio de certificados digitais emitidos pelos órgãos de governo (SERPRO, RECEITA, DEFESA e PRESIDÊNCIA), conforme determinação do CETIR GOV.

Considerando essa exigência, e que apenas o SERPRO comercializa certificados digitais emitidos por governo, os certificados objeto desse processo devem obrigatoriamente ser adquiridos do SERPRO, sob pena de não serem compatíveis com as novas exigências impostas pelo STN, conforme Ofício mencionado.

A exigência comercial de certificados emitidos pelos órgãos de governo para atender as novas exigências impostas de segurança, limita a compra de certificados a apenas ao SERPRO, sendo possível a aquisição dos seguintes produtos disponibilizados no próprio sítio de Internet do SERPRO:



Solução 1: Certificados Digitais e-CPF A3, Administração Pública Direta em nuvem com validade de 1 ano.

Solução 2: Certificados Digitais e-CPF A3, SerproID, Administração Pública Direta em nuvem com validade de 3 anos.

8.2. Certificados digitais de outras autoridades certificadoras

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

9.1. Certificados digitais emitidos por órgão de governo

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		

9.2. Certificados digitais gerais

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

10.1. Certificados digitais emitidos por órgão de governo

Tendo em vista a restrição do SIAFI para apenas permitir acesso por uso de certificados emitidos pelos órgãos de governo para atender as novas exigências impostas de segurança, não foram considerados como soluções outras opções de certificados ICP-Brasil.

Qualquer certificado digital emitido por outra entidade diferentes de SERPRO, RECEITA, DEFESA e PRESIDÊNCIA não serão compatíveis com as exigências impostas pela STN conforme descrito no Ofício-Circular nº 40/2024/SPO/SE/MJ (36272949).

Nesse cenário, o SERPRO é um único dos órgãos de governo que comercializa a emissão de certificados digitais.

10.2. Certificados digitais emitidos por outras autoridade certificadoras

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.

Cumpre 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)

11.1. Certificados digitais emitidos por órgão de governo

A tabela a seguir considera a necessidade de 746 certificados digitais emitidos por órgão de governo. Na Solução 1, são considerados certificados com validade de 1 ano, e, na Solução 2, certificados com validade de 3 anos.

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Solução Viável 1	R\$ 107.520,98	R\$ 107.520,98	R\$ 107.520,98	R\$ 322.562,94
Solução Viável 2	R\$ 126.424,62	R\$ 0,00	R\$ 0,00	R\$ 126.424,62

Portanto, a Solução 2 (Certificados Digitais e-CPF A3, SerproID, Administração Pública Direta em nuvem com validade de 3 anos) é considerada como a solução mais vantajosa com relação aos custos.

11.2. Certificados digitais de outras autoridades certificadoras

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.
- d) para o item 1 (certificados digitais emitidos por órgão de governo), o certificado digital deve ser emitido pelo SERPRO.

13. Estimativa de custo total da contratação

Valor (R\$): 5.588.155,02

13.1. Certificados digitais emitidos por órgão de governo

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Solução Viável 2	R\$ 126.424,62	R\$ 0,00	R\$ 0,00	R\$ 126.424,62

Portanto, a estimativa é de contratar 746 (setecentos e quarenta e seis) certificados digitais e-CPF A3 SerproID, Administração Pública Direta em nuvem com validade de 3 anos. Essa contratação implicará num custo total de R\$ 126.424,62 (cento e vinte e seis mil, quatrocentos e vinte e quatro reais e sessenta e dois centavos).

13.2. Certificados digitais de outras autoridades certificadoras

Para estimativa do custo de cada item, foi feita pesquisa no sítio de empresas especializadas em prover soluções de certificado digital. As imagens capturadas durante a pesquisa fazem parte do Anexo I deste termo de referência. Estima-se que o valor da contratação em 3 anos será de R\$ 5.461.730,40, 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 (A1), 3 anos, em NUVEM, e-CNPJ	* Certificados digitais A1 WILDCARD, 1 anos
Custo unitário estimado (R\$)	399,00	374,90	0,04	294,90	379,90	2.199,00
Quantidade anual estimada	90	10708	750000	4588	40	6
Valor total (R\$)	35.910,00	4.014.429,20	30.000,00	1.353.001,20	15.196,00	13.194,00
Valor total estimado	R\$ 5.461.730,40					

Portanto, ao considerar os itens 1 e 2, a contratação implicará num custo total de R\$ 5.588.155,02.

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

Acerca do item 1, que se refere à emissão de certificados digitais por órgão de governo, observa-se, ao analisar os custos totais das duas soluções viáveis apresentadas, que a Solução Viável 2, que consiste na contratação de um serviço com validade de 3 anos em uma única vez, apresenta uma economia mais vantajosa. Isso porque enquanto a Solução Viável 1, com serviços de 1 ano renovados por três vezes, resulta em um custo de R\$ 322.562,94 ao longo de 3 anos, a Solução Viável 2 tem um custo total de apenas R\$ 126.424,62. Isso representa uma economia significativa, eliminando a necessidade de renovações anuais e seus custos associados, além de garantir estabilidade no fornecimento do serviço por todo o período, sendo, portanto, a alternativa mais econômica e eficiente.

Para o item 2, 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 documentos 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

Como apresentado neste estudo, a contratação está segmentada em dois itens distintos, conforme as necessidades específicas da administração. O primeiro item, que abrange certificados digitais emitidos por órgãos de governo conforme comunicado da STN (SEI 36275168), será contratado por contratação direta, em virtude da inviabilidade de competição. Isso se justifica pelo fato do SERPRO ser o único órgão de governo que comercializa o serviço demandado.

O segundo item 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.

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](#).

GABRIEL ARQUELAU PIMENTA RODRIGUES

Integrante Técnico



Assinou eletronicamente em 18/09/2024 às 18:08:23.

BRUNO WERNECK PINTO HOELZ

Integrante Requisitante



Assinou eletronicamente em 19/09/2024 às 10:30:59.

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 19/09/2024 às 11:20:07.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Preços Unitários - Certificados.docx (2.03 MB)