

Estudo Técnico Preliminar 27/2025

1. Informações Básicas

Número do processo: 01341.000980/2024-28

2. Descrição da necessidade

2.1. O presente Estudo Técnico Preliminar (ETP) tem como objeto analisar a viabilidade da contratação de do Serpro para a emissão de certificados digitais, Nível A3, para os servidores da CNEN.

2.2. Por questões de segurança cibernética e integridade das informações sensíveis, o acesso ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) passou a ser, desde 31 de outubro de 2024, exclusivamente realizado mediante autenticação com certificado digital ICP-Brasil, conforme diretrizes do Órgão Central de Sistemas Estruturantes do Governo Federal.

2.3. Essa medida atende às políticas nacionais de segurança da informação, conforme estabelecido no Decreto nº 10.748/2021, que institui a Estratégia Nacional de Segurança Cibernética (E-Ciber), reforçando o uso de mecanismos de autenticação forte para proteger ativos críticos da Administração Pública.

2.4. Diversos órgãos têm aderido à solução de solicitação de token pelo SOUGOV, um aplicativo com serviços de gestão de pessoas exclusivos para servidores públicos federais ativos, aposentados, pensionistas e anistiados políticos do poder Executivo Federal civil. Esse processo é mais dinâmico e evita retrabalhos, como ocorre com a atual contratação, na qual cada requisitante solicita suas demandas de forma isolada. Dessa forma, é possível centralizar e otimizar processos, conforme demonstrado no manual ([link](#)).

2.5. Essa solução envolve a contratação do Serpro, que é o único fornecedor que atendeu às especificações da AR MPDG – Autoridade de Registro do Ministério do Planejamento, Desenvolvimento e Gestão, responsável por essa gestão no âmbito do Governo Federal. Além de ser o único fornecedor que possui integração com a aplicação SOUGOV.

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Recursos Humanos	Leonardo Ferreira Bezerra

4. Necessidades de Negócio

4.1. Diversos sistemas estruturantes do Governo Federal — como SIAFI, SIAPE, SIAPE-Saúde, e-Social, Compras.gov.br, SEI e SouGov — exigem, atualmente, autenticação por meio de certificado digital ICP-Brasil,

como requisito de acesso e assinatura de atos administrativos eletrônicos. Essa exigência decorre da crescente adoção de modelos de governo digital, combinada com normas de segurança cibernética que visam garantir a identidade dos usuários e a inviolabilidade dos dados.

4.2. A contratação de certificados digitais com mídia criptográfica (tokens), emitidos conforme as especificações da ICP-Brasil, é necessária à continuidade das atividades institucionais da CNEN, uma vez que:

- Garante a autenticidade, integridade e não repúdio das operações realizadas em sistemas federais;
- Protege o acesso a sistemas com dados financeiros, previdenciários e sensíveis;
- Está alinhada com as exigências da Estratégia de Governo Digital (EGD) e da Estratégia Nacional de Segurança Cibernética (E-Ciber);
- Atende às normas da Lei nº 14.063/2020, que regulamenta o uso de assinaturas eletrônicas na Administração Pública.

4.3. O uso de certificados digitais tipo A3, armazenados em token criptográfico, agrega camadas adicionais de segurança, como autenticação multifator (token + PIN) e armazenamento seguro da chave privada, sendo uma medida recomendada para usuários com perfil de autorização crítica, como ordenadores de despesa, gestores de contrato e responsáveis por folha de pagamento.

5. Necessidades Tecnológicas

5.1. Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, em nuvem, com validade por 3 anos.

5.2. Certificado

5.2.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 65 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, de 9 de junho de 2009).

5.2.2. Nível: A3.

5.2.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.

5.2.4. Todos os certificados deverão ser emitidos sob a hierarquia V2.

5.2.5. Tipo: e-CPF.

5.2.6. Ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Fazenda, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros.

5.2.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal, entre outros).

5.2.8. Garantia de correção e atualização, motivadas por falhas técnicas e mudanças originadas de diretrizes ICP-Brasil, pelo período de 3 (três) anos, contados a partir da data do aceite definitivo do certificado. Caso a correção ou atualização exija emissão de novo certificado, a contratada deverá realizar, no prazo de até 7 (sete) dias úteis, contados da data de notificação, sem ônus adicional para a contratante.

5.3. Gerado e armazenado em nuvem da AC - autoridade certificadora

5.3.1. Com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica

5.3.2. Ser aderente às normas do Comitê Gestor da ICP-Brasil.

- 5.3.3. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.
- 5.3.4. Compatibilidade com o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).
- 5.3.5. Compatibilidade com o sistema operacional Microsoft Windows (2000 e versões superiores).
- 5.3.6. Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0 da Microsoft (Windows 2000 e versões superiores).
- 5.3.7. Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (. dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente.
 - 5.3.7.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE.
- 5.3.8. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3
- 5.3.9. Assinar dados digitalmente em até 10 (dez) segundos.

5.4. Funcionalidades

- 5.4.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.
- 5.4.2. Permitir personalização eletrônica através de parâmetro identificador interno (label).

5.5. Software

- 5.5.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:
 - 5.5.1.1. Gerenciamento do dispositivo;
 - 5.5.1.2. Exportação de certificados armazenados no dispositivo;
 - 5.5.1.3. Importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;
 - 5.5.1.4. Importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;
 - 5.5.1.5. Visualização de certificados armazenados no dispositivo;
 - 5.5.1.6. Apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;
 - 5.5.1.7. Reutilização de dispositivos bloqueados, por meio de apagamento total dos dados armazenados e geração de nova senha de acesso.
- 5.5.2. Deverá ser disponibilizado portal para download de drivers/software de forma ilimitada e gratuita.
- 5.5.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.

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

- 6.1. A Solução a ser utilizada deverá conter todas as características para o cumprimento das funcionalidades, deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira - ICP Brasil/ITI; ser do tipo e-CPF com nível de autenticação A3 gerado e armazenado em nuvem, armazenamento fornecido pelo prestador de serviço, com possibilidade de identificar servidores do órgão, possuir validade de 03 anos (36 meses), contados a partir da data de validação /emissão do certificado; permitir a renovação por igual período e a utilização da assinatura de documentos eletrônicos, e-mails, acesso à aplicações, login em rede,

entre outras destinações, permitir acesso ao SIAPE, SIAFI e demais sistemas do governo ser aderente à Resolução nº 65, de 09 de junho de 2009, do Comitê Gestor da Infraestrutura de Chaves Públicas.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A demanda por certificados digitais na CNEN apresenta variação contínua, decorrente de fatores como:

- Mudança de perfil funcional, com servidores assumindo funções que exigem assinatura digital (ex: gestores, fiscais, ordenadores);
- Expiração dos certificados digitais já emitidos, com necessidade de renovação periódica;
- Reorganização administrativa e adesão crescente aos sistemas estruturantes que exigem autenticação com certificado digital (SEI, SIAFI, SouGov, etc.);
- Adicionalmente, no ano de 2025, temos o ingresso 150 de novos servidores aprovados no concurso realizado este ano.

7.2. Dessa forma, não é possível determinar com exatidão uma quantidade fixa de certificados a serem emitidos, uma vez que a demanda é dinâmica e condicionada à realidade administrativa de cada exercício.

7.3. Para embasar a estimativa, foi considerada a média anual de custos registradas desde o ano de 2020, conforme tabela constante na seção de estimativa de custos deste ETP. Essa média serve como parâmetro inicial para definição do valor global do contrato, sem estabelecer quantitativos obrigatórios, uma vez que a emissão será realizada sob demanda, conforme solicitação individualizada via sistema SouGov.

7.4. Essa abordagem está alinhada com o art. 11 da Instrução Normativa SEGES/ME nº 1/2019, que admite a estimativa com base em dados históricos ou projeções técnicas quando a demanda futura não puder ser dimensionada com precisão.

8. Levantamento de soluções

8.1 A solução será adquirida na forma de contratação de serviço e terá que contemplar a emissão de certificados do nível A3, e-CPF, em nuvem, com validade de 3 anos, em conformidade com o padrão ICP-Brasil, por unidade certificadora de governo.

8.2 Atualmente a CNEN efetua a contratação/compra de Tokens de forma individualizada e com abertura de processo para cada nova compra. Em temos gerais, as soluções propostas encontram-se discriminadas na tabela abaixo:

Solução	Descrição	Viabilidade
1. Modelo atual – Aquisição descentralizada de tokens físicos por cada unidade da CNEN	Cada unidade da CNEN realiza processo licitatório próprio para aquisição de tokens com certificados digitais. O processo inclui elaboração de termo de referência, aprovação de recursos, licitação, homologação, entrega e configuração.	Baixa viabilidade. Elevado custo operacional e burocrático. Redundância de processos, dificuldade de padronização e ineficiência administrativa. Inadequado para órgãos com múltiplas unidades, como a CNEN.
2. Solução SERPRO via SouGov – Requisição direta de certificado digital com token pelo aplicativo	A requisição do certificado e token é feita diretamente pelo servidor por meio do aplicativo SouGov , vinculado ao SERPRO. Um responsável institucional (perfil “aprovador”) valida o pedido. O processo é centralizado, padronizado e sem necessidade de processo licitatório para aquisição.	Alta viabilidade. Solução segura, eficiente e com apoio técnico do SERPRO. Reduz burocracia, elimina a necessidade de processos de compra e garante uniformidade entre as unidades da CNEN.

9. Análise comparativa de soluções

9.1. A Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, responsável por assegurar a autenticidade, integridade e validade jurídica de documentos eletrônicos e transações digitais por meio de certificados digitais. Posteriormente, a Lei nº 14.063/2020, regulamentada pelo Decreto nº 10.543/2020, reforçou o uso obrigatório de certificados digitais no padrão ICP-Brasil para atos administrativos que exijam assinatura eletrônica qualificada, como é o caso das assinaturas digitais realizadas por servidores da CNEN em sistemas como o SEI, Compras.gov.br, entre outros.

9.2. No modelo atualmente adotado pela CNEN, cada unidade descentralizada realiza seus próprios processos licitatórios para aquisição de tokens criptográficos com certificados digitais, gerando uma multiplicidade de contratos, procedimentos administrativos e dificuldades logísticas. Essa abordagem se mostra ineficiente, burocrática e dissonante da estratégia de transformação digital da Administração Pública Federal.

9.3. Como alternativa, o Serviço Federal de Processamento de Dados (SERPRO) disponibiliza solução integrada por meio do aplicativo SouGov, que permite a requisição direta de certificados digitais e tokens pelos próprios servidores, com posterior validação por um responsável institucional (perfil “aprovador”). Essa solução é centralizada, segura, padronizada para toda a Administração Pública Federal e dispensa a abertura de processos licitatórios para aquisição individual de tokens, uma vez que o fluxo é internalizado no ecossistema do Governo Federal. Além disso, o SERPRO é a única entidade autorizada a operar essa solução integrada ao SouGov, sendo, portanto, inviável tecnicamente a contratação de outro fornecedor.

9.4. Nos termos do art. 74, inciso I da Lei nº 14.133/2021, e com base no entendimento pacífico da jurisprudência e da doutrina administrativa, está caracterizada a inexigibilidade de licitação, dada a inviabilidade de competição. A contratação do SERPRO, nesse caso, decorre não só da sua posição institucional como empresa pública vinculada ao Governo Federal (Lei nº 5.615/1970), mas também da natureza exclusiva da integração com o SouGov, solução essencial para a otimização do processo de emissão de certificados digitais no âmbito da CNEN.

10. Registro de soluções consideradas inviáveis

10.1. A viabilidade das soluções está descrita no item 8. Levantamento de soluções

11. Análise comparativa de custos (TCO)

11.1. A Análise Comparativa de Custos, também conhecida como Total Cost of Ownership (TCO), é uma abordagem que considera o custo total associado à aquisição, operação, manutenção e gestão de uma solução ao longo de seu ciclo de vida. No contexto da contratação de certificados digitais via tokens criptográficos, o TCO não se limita ao preço unitário dos dispositivos, mas engloba também custos administrativos, operacionais, riscos e impactos na eficiência da gestão.

11.2. A comparação do modelo atual de aquisição descentralizada com a solução integrada oferecida pelo SERPRO via aplicativo SouGov, pode ser observada na tabela abaixo:

Critério	Modelo atual	Nova solução: SERPRO via SouGov
Custo de aquisição	Contratos distintos por unidade acarretando variabilidade de preços.	Centralizado no SERPRO sendo um custo único.
Custos operacionais	Elevados: exigem licitação, instrução processual, gestão contratual descentralizada.	Mínimos: requisição direta no app SouGov com aprovação interna.
Renovação	Repetição integral do processo. Risco de descontinuidade.	Fluxo contínuo e automatizado com nova requisição no sistema.

Gestão e suporte	Dificuldade de padronização e duplicidade de esforços entre unidades.	Gestão centralizada. Suporte técnico do SERPRO.
Riscos operacionais	Alto risco de atraso, falhas contratuais ou aquisições duplicadas.	Redução significativa de riscos com plataforma nacional unificada.
Custos ocultos (TCO)	Altos: horas de servidores, tempo gasto com trâmites, controles locais.	Baixos: operação padronizada e eficiente.

11.3. Ao considermos a solução como um todo, o custo total (TCO) da solução via SERPRO é inferior quando considerados os ganhos operacionais, a eliminação de processos licitatórios e o ganho em eficiência administrativa.

12. Descrição da solução de TIC a ser contratada

12.1. Prestação de serviços de certificação digital por meio da SEPRO, garantindo a segurança dos acessos, levando em consideração o diferencial negocial dos certificados e-CPF emitidos pelo SERPRO é a Autoridade de Registro (AR) integrada ao SOUGOV, que permite a realização dos processos de validação de identidade, autorização de emissão e emissão do certificado seja feita diretamente através deste aplicação, sem a necessidade de atuação de um Agente de Registro ou deslocamento físico do usuário para procedimento de validação presencial. A presente contratação será por inexigibilidade de licitação previsão no artigo 74 inciso I, uma vez que a SEPRO é recomendada por questões de segurança pela STN.

13. Estimativa de custo total da contratação

Valor (R\$): 14.038,38

13.1. Para a definição do valor estimado da contratação, foi utilizada a média histórica de despesas com certificados digitais nos últimos cinco anos (2020–2024), no valor de R\$ 13.179,63, conforme dados extraídos dos registros contábeis da CNEN:

ANO	VALOR TOTAL (R\$)
2020	11.625,14
2021	13.079,72
2022	12.451,65
2023	13.290,68
2024	15.450,96

13.2. Considerando a necessidade de atualização monetária para o exercício de 2025, foi aplicado o índice oficial do IGP-M acumulado em 2024 (6,54%), conforme tabela do IBGE, o que resulta em um valor estimado corrigido de R\$ 14.038,38, a ser considerado como estimativa orçamentária para a contratação.

14. Justificativa técnica da escolha da solução

14.1. O Serviço Federal de Processamento de Dados – SERPRO, inscrito no CNPJ/MF sob o no 33.683.111 /0001-07, sediado na SGAN Quadra 601 – Módulo V – Ed. Sede – CEP: 70.836-900, Asa Norte, Brasília/DF, declara, para os devidos fins, que tem exclusividade na prestação de serviços correlatos a PORTARIA No 236, de 08 de dezembro de 2014, que institui a política de segurança da informação do Sistema Integrado de Administração de Recursos Humanos (SIAPE/SIGEPE) e em seu Art. 3o, alínea VI, informa a exclusividade do SERPRO no desenvolvimento das funcionalidades do SIAPE/SIGEPE.

14.2. Por meio da exclusividade citada, desenvolveu o módulo eletrônico da Autoridade Registradora – AR MPDG – Autoridade de Registro do Ministério do Planejamento, Desenvolvimento e Gestão, para atendimento

ao novo modelo de emissão de certificado digital, constante no documento de Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil – DOC-ICP-05, aprovado pelo Comitê Gestor da ICP-Brasil, por meio da resolução no 117, de 20 de outubro de 2020, permitindo aos servidores e aos empregados públicos, vinculados ao Sistema de Gestão de Pessoal da Administração Pública Federal – SIGEPE, solicitar o certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil por meio do SIAPE/SIGEPE.

14.3. Para possibilitar o fluxo completo de emissão e gestão de certificados digitais, foi realizado o credenciamento e vinculação da AR MPDG – Autoridade de Registro do Ministério do Planejamento, Desenvolvimento e Gestão às Autoridades Certificadoras AC SERPRO RFB e AC SERPRO

15. Justificativa econômica da escolha da solução

15.1. O corrente modelo de aquisição é ineficiente em termos econômicos e de gerenciamento. Os preços são praticados conforme localidade de CNEN. Além disso, o processo de aquisição é lento e requer a abertura e encaminhamento de processos para aprovação.

15.2. O modelo proposto além de simplificar o processo, permitindo que os servidores que fazem parte do processo atual foquem em outras atividades, unifica o preço praticado para toda a CNEN.

16. Benefícios a serem alcançados com a contratação

16.1. Permitir o acesso seguro de servidores a sistemas governamentais e a emissão de assinaturas digitalmente confiáveis, conforme orientações da Secretaria do Tesouro Nacional-STN.

17. Providências a serem Adotadas

17.1. Considerando a solução proposta requer o uso da aplicação SouGov, os servidores terão que utilizar a aplicação, ou a página web, para efetuar as solicitações.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Esta equipe declara viável a contratação considerando o caráter de exclusividade da a empresa SERPRO.

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 FERNANDES VAZ RIBEIRO

Membro da comissão de contratação



Assinou eletronicamente em 08/08/2025 às 16:45:22.

FERNANDO ANTONIO VATER

Membro da comissão de contratação



Assinou eletronicamente em 11/08/2025 às 14:20:21.

LUIS FERNANDO GOMES JUNIOR

Membro da comissão de contratação



Assinou eletronicamente em 08/08/2025 às 16:56:16.

SANDRA REGINA LANZELLOTTI SAMPAIO

Membro da comissão de contratação



Assinou eletronicamente em 11/08/2025 às 13:52:00.