Estudo Técnico Preliminar 39/2025

1. Informações Básicas

Número do processo: 64024.002124/2025-09

2. Descrição da necessidade

Contratação de Certificados Digitais e-CPF
O certificado digital é uma assinatura eletrônica que utiliza chaves criptográficas para confirmar a identidade de uma pessoa física (e-CPF).
O comando do 25º Batalhão de Caçadores, têm a necessidade de utilizar os certificados digitais para reforçar a segurança da informação e garantir um acesso mais seguro a diversos sistemas estruturantes da administração pública federal, tais como: Sistema de Concessão de Diárias e Passagens (SCDP); Sistema Integrado de Administração de Pessoal (SIAPE); Sistema de Gestão de Pessoas (SIGEPE), Sistema Integrado de Administração Financeira (SIAFI), Portal de Compras do Governo Federal - compras.gov.br, Receita Federal, entre outros. É importante ressaltar que é obrigatória a utilização do certificado digital no acesso aos sistemas estruturantes do governo citados anteriormente.

Motivação / Justificativa

O presente documento tem por objetivo justificar a necessidade de aquisição de um novo certificado digital para o Comandante e Subcomandante do 25º Batalhão de Caçadores, tendo em vista que o dispositivo atual (token) apresentou falha e não está mais em funcionamento. A ausência de um certificado digital ativo impossibilita o acesso aos sistemas essenciais para a gestão da Organização Militar (OM), impactando diretamente o desempenho das atividades administrativas e operacionais da unidade.

A aquisição do certificado digital está em conformidade com as disposições da Lei nº 14.133/2021, que rege as contratações públicas. O artigo 74, inciso I, da referida lei estabelece que a administração pública poderá realizar a contratação direta por dispensa de licitação em situações de emergência ou de caráter indispensável à manutenção das atividades institucionais. Neste caso, a aquisição do certificado digital se justifica pela necessidade de garantir a continuidade dos serviços administrativos e operacionais do batalhão.

O Comandante da OM desempenha funções essenciais que demandam acesso a diversos sistemas informatizados da Administração Pública, tais como:

- Sistema de Concessão de Diárias e Passagens (SCDP);
- Sistema Integrado de Administração de Pessoal (SIAPE);
- Sistema de Gestão de Pessoas (SIGEPE);
- Sistema Integrado de Administração Financeira (SIAFI);
- Portal de Compras do Governo Federal - compras.gov.br, Receita Federal
- **Demais sistemas do Exército Brasileiro que exigem autenticação digital.**

A ausência do certificado digital inviabiliza a assinatura eletrônica de documentos, a realização de transações administrativas e o cumprimento de prazos institucionais, comprometendo a eficiência e legalidade dos atos administrativos.

Caso a aquisição do novo certificado digital não seja realizada de forma célere, haverá impactos negativos significativos, tais como:

- Impossibilidade de gestão eficaz dos sistemas informatizados;
- Atrasos na tramitação de documentos e processos administrativos;
- Comprometimento das atividades estratégicas do batalhão;

- Risco de descumprimento de prazos legais e normativos.

Diante do exposto, a aquisição de um novo certificado digital para o Comandante do [Nome do Batalhão] se faz necessária e urgente, a fim de garantir a continuidade das atividades institucionais, preservar a eficiência administrativa e assegurar a conformidade com as normas vigentes. Recomenda-se, portanto, a tramitação do processo de aquisição em caráter prioritário, com base na Lei nº 14.133/2021.

3. Área requisitante

Área Requisitante	Responsável
Seção de Informática	Victor Brito Portela

4. Necessidades de Negócio

Identificação das necessidades de negócio

1 Autenticação por meio de certificado digital no sistema estruturante do governo: SCDP.
2 Autenticação por meio de certificado digital no sistema estruturante do governo: SIAPENET.
3 Autenticação por meio de certificado digital no sistema estruturante do governo: SIAFI.
4 Autenticação por meio de certificado digital no sistema estruturante do governo: Compras.gov.br.
5 Autenticação por meio de certificado digital no sistema da Receita Federal do Brasil.
6 Autenticação por meio de certificado digital nos demais sistemas estruturantes do governo, além dos retrocitados.

5. Necessidades Tecnológicas

Identificação das necessidades tecnológicas
Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.
1.1. 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).
1.2. Nível: A3.
1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2.
1.5. Tipo: e-CPF.
1.6. 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 Gestão e da Inovação em Serviços Públicos, do Planejamento e Orçamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios, entre outros.
1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, Compras.gov.br, Receita Federal, entre outros).

Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico para armazenamento do certificado, com validade por 3 anos.
2.1. Certificado
2.1.1. 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).
2.1.2. Nível: A3.
2.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
2.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2.
2.1.5. Tipo: e-CPF.
2.1.6. 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 Gestão e da

Inovação em Serviços Públicos, do Planejamento e Orçamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros.
2.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, Compras.gov.br, Receita Federal, entre outros).
2.2. Dispositivo físico de armazenamento
2.2.1. Dispositivo físico de armazenamento, em modelo homologado conforme padrão ICP- Brasil e constante na lista de homologação atual, disponível no site do Instituto Nacional de Tecnologia da Informação (ITI).
2.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
2.2.3. Ser aderente às normas do Comitê Gestor da ICP-Brasil.
2.2.4. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.
2.2.5. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.
2.2.6. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas.
2.2.7. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3).
2.2.8. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas.
2.2.9. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.
2.2.10. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits.
2.2.11. Possuir carcaça resistente à água e à violação.
2.2.12. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).

2.2.13. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).
2.2.14. 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).
2.2.15. 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.
2.2.15.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidadesexistentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE.
2.2.16. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.
2.2.17. Possuir indicador luminoso de estado do dispositivo.
2.2.18. Assinar dados digitalmente em até 10 (dez) segundos.
2.2.19. O dispositivo físico de armazenamento deverá possuir certificação do INMETRO.
2.3. Funcionalidades
2.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.
2.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label).
2.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.
2.3.4. Permitir criação de senhas com caracteres alfanuméricos.
2.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.
2.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 2459.
2.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução. Apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo.
2.3.8. Permitir inicialização e reinicialização do dispositivo físico de armazenamento do certificado mediante a utilização de PUK (Pin Unlock Key).
2.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores), Linux (kernel 2.4, 2.6 e superiores) e Mac OS (10.0 e superiores).
2.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome.
2.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4,2.6 e superiores).
2.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo.
2.3.13. Implementar mecanismo de autenticação tipo challenge-response.

2.3.14. Forçar a troca da senha padrão no primeiro acesso.
2.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos.
2.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida.
2.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do dispositivo físico de armazenamento.
2.4. Software

2.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:
2.4.1.1. gerenciamento do dispositivo;
2.4.1.2. exportação de certificados armazenados no dispositivo;
2.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;
2.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;
2.4.1.5. visualização de certificados armazenados no dispositivo;
2.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;
2.4.1.7. reutilização de dispositivos bloqueados, por meio de apagamento total dos dados armazenados e geração de nova senha de acesso.
2.4.2. Deverá ser disponibilizado portal para download de drivers/softwares de forma ilimitada e gratuita.
2.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.
Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.
3.1. Certificado
3.1.1. 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).
3.1.2. Nível: A3.
3.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
3.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2.
3.1.5. Tipo: e-CPF.
3.1.6. 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 Gestão e da Inovação em Serviços Públicos, do Planejamento e Orçamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros.
3.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, Compras.gov.br, Receita Federal, entre outros).

Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de dispositivo físico para armazenamento do certificado, com validade por 3 anos.
4.1. Certificado
4.1.1. 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).
4.1.2. Nível: A4.
4.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
4.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2.
4.1.5. Tipo: e-CPF.
4.1.6. 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 Gestão e da Inovação em Serviços Públicos, do Planejamento e Orçamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros.
4.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, Compras.gov.br, Receita Federal, entre outros).
4.2. Dispositivo físico de armazenamento
4.2.1. Dispositivo físico de armazenamento, em modelo homologado conforme padrão ICP- Brasil e constante na lista de homologação atual, disponível no site do Instituto Nacional de Tecnologia da Informação (ITI).
4.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado.
4.2.3. Ser aderente às normas do Comitê Gestor da ICP-Brasil.
4.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.
4.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.
4.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas.
4.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3).
4.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas.

4.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.
4.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits.
4.2.12. Possuir carcaça resistente à água e à violação.

4.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).
4.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).
4.2.15. 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).
4.2.16. 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.
4.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do dispositivo físico de armazenamento do certificado, 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.
4.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.
4.2.18. Possuir indicador luminoso de estado do dispositivo.
4.2.19. Assinar dados digitalmente em até 10 (dez) segundos.
4.2.20. O token criptográfico deverá possuir certificação do INMETRO.
4.3. Funcionalidades
4.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.
4.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label).
4.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.
4.3.4. Permitir criação de senhas com caracteres alfanuméricos.
4.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.
4.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 2459.
4.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução. Apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo, sendo que no caso de certificados emitidos para pessoas jurídicas, o titular é a pessoa física responsável pela empresa.
4.3.8. Permitir inicialização e reinicialização do dispositivo de armazenamento do certificado, mediante a utilização de PUK (Pin Unlock Key).

4.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores), Linux (kernel 2.4, 2.6 e superiores) e Mac OS (10.0 e superiores).
4.3.10. Suportar os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome.
4.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4,2.6 e superiores).
4.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo.
4.3.14. Implementar mecanismo de autenticação tipo challenge-response.
4.3.14. Forçar a troca da senha padrão no primeiro acesso.
4.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos.
4.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida.
4.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do dispositivo físico de armazenamento do certificado digital.
4.4. Software
4.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:
4.4.1.1. gerenciamento do dispositivo;
4.4.1.2. exportação de certificados armazenados no dispositivo;
4.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;
4.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;
4.4.1.5. visualização de certificados armazenados no dispositivo;
4.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;
4.4.1.7. reutilização de dispositivos bloqueados, por meio de apagamento total dos dados armazenados e geração de nova senha de acesso.
4.4.2. Deverá ser disponibilizado portal para download de drivers/softwares de forma ilimitada e gratuita.
4.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.

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

Identificação de demais requisitos necessários e suficientes à escolha da solução de TIC.

Permitir a mobilidade de autenticação por meio de certificados digitais, utilizando o menor número de dispositivos físicos e operações.
Não poderá ser obrigatório o uso de dispositivos pessoais dos servidores para realização das operações de autenticação por meio de certificados digitais.

7. Estimativa da demanda - quantidade de bens e serviços

EXERCÍCIO	PREVISÃO DE CERTIFICADOS A VENCER (ciclo de 3 anos)	PREVISÃO DE EMISSÃO DE NOVOS CERTIFICADOS
2025	10	10
Total Parcial	10	10
Total geral	10	

8. Levantamento de soluções

Solução 1: Certificação digital tipo A3 sem fornecimento de token
A solução 1 consiste apenas na disponibilização de certificado digital tipo A3, visando a reutilização dos tokens atualmente em uso.
Vantagens:
Mobilidade: devido ao uso de tokens USB, a presente solução apresentaria elevado nível de mobilidade, visto que o usuário poderá utilizar seu certificado em qualquer computador que possua o programa gerenciador de token, dispensando a necessidade de equipamentos/dispositivos extras;
Economia: devido à reutilização de tokens, não será necessário o dispêndio de recursos financeiros
para aquisição de novos dispositivos.
Desvantagens:
Quantidade insuficiente: somente em caso excepcional de uma demanda por uso obrigatório de certificado por todos os militares comprometerá a eficiência da solução 1;
Solução 2: Certificação digital tipo A3 de uso em nuvem
A solução 2 consiste no fornecimento de certificação digital tipo A3 em nuvem. Ou seja, o certificado digital do usuário será armazenado na nuvem do fornecedor, dispensando assim a necessidade de token ou cartão inteligente.
Vantagens:
Mobilidade: alto grau de praticidade e mobilidade, visto que o certificado estará disponível em qualquer lugar e a qualquer momento;
Maior praticidade: como não há necessidade de token ou cartão, não haverá mais problemas com usuários que perdem esses itens, nem ocorrerão problemas relacionados ao mal funcionamento do dispositivo, facilitando, portanto, a gestão e o suporte técnico.
Desvantagens:
Incerteza de compatibilidade: atualmente existem sistemas que não possuem suporte nativo a certificados em nuvem (também conhecido como certificado online). Como é possível que nem todos os sistemas que estão no âmbito das atividades desenvolvidas, no momento há grande grau de incerteza quanto à viabilidade do uso desse tipo de certificação. Por outro lado, ocorreria desperdício de recurso, uma vez que o Batalhão possui utilização de mídia token.

9. Análise comparativa de soluções

ID	REQUISITOS	Solução 1	Solução 2
1	Aderente a ICP-Brasil	Atende	Atende
2	Emitido por AC credenciada na ICP-Brasil	Atende	Atende
3	Validade mínima de 3 anos	Atende	Atende
4	Segurança	Atende	Atende
5	Praticidade e mobilidade	Atende	Atende
6	Compatibilidade com os sistemas	Atende	Não Atende
7	Presunção de validade jurídica	Atende	Atende
8	Certificação digital tipo A3	Atende	Atende
9	Compatibilidade Windows 7, Windows 10 e versões superiores	Atende	Atende
10	Compatibilidade com arquiteturas 32 e 64 bits	Atende	Atende
11	Quantidade supre a demanda	Atende	Atende
12	Economicidade	Atende	Não atende

Tabela 4: Avaliação das soluções identificadas

Avaliação das Soluções Viáveis

Conforme observa-se na *Tabela 4: Avaliação das soluções identificadas*, a opção que atenderá todos os requisitos elencados no Documento de Oficialização da Demanda é a Solução 1: Certificação digital

tipo A3 sem fornecimento de token, mediante contratação de empresa especializada para fornecer serviço de certificação digital tipo A3, de acordo com as normas preconizadas pelo ICP-Brasil e nos moldes apresentados na Solução 1.

- Descrição da solução: consiste na contratação de empresa especializada na prestação de serviços de certificação digital A3 para o fornecimento de 1369 certificados tipo A3;
- Fornecedores da solução:
    - Mercado Privado: Certsign, Serasa, Soluti, Valid, entre outros.
    - Governo: Serpro.
- Quem utiliza e valor pago: Informação apresentada na análise de custos.
- Diferentes formas de contratação:
    - Fornecimento de Certificado sem token.
    - Processo Licitatório ou Dispensa com o Serpro.
- Requisitos da solução
    - Capacitação: A empresa contratada deverá ter capacidade técnica de atender as solicitações do órgão contratante, especialmente quanto aos seguintes aspectos:
        - Dirimir dúvidas técnicas referentes à instalação e utilização dos certificados digitais; e
        - Responder questionamentos referentes a questões contratuais.
    - Legais: Atendimento aos requisitos da ICP-Brasil.
    - Manutenção: Não há.
    - Temporais: A solução deve estar disponível a partir de 01/01/2024.
    - Segurança: Os da ICP-Brasil.
    - Sociais, ambientais e culturais:

- Os tutoriais, manuais e demais documentações que contenham as instruções para a emissão do certificado digital e seu armazenamento no token deverão ser escritos em língua portuguesa, com clareza e simplicidade, de forma que o usuário comum tenha capacidade de entender e seguir as instruções sem maiores necessidades de esclarecimento;
- O presente processo administrativo para contratação da solução pretendida é realizado em forma eletrônica. O objetivo da referida adoção é reduzir o número de cópias e impressões em papel e proporcionar maior celeridade ao trâmite processual;
- Os trâmites para execução do contrato, isto é, solicitação e emissão de certificado digital serão todos on- line, sem a necessidade de deslocamento para emissão dos certificados;
- Os documentos e relatórios deverão ser disponibilizados de forma eletrônica, evitando a confecção e transporte de mídias e/ou papel. Uma vez que não há entrega de qualquer material ou equipamento, a Equipe de Planejamento da Contratação não vislumbrou outras práticas de sustentabilidade ambiental aplicáveis na presente contratação.

    - Sustentabilidade:

- Além dos critérios de sustentabilidade descritos acima, não foram encontrados requisitos aplicáveis a esta contratação no Guia Nacional de Contratações Sustentáveis, elaborado pela Câmara Nacional de Sustentabilidade da Consultoria Geral da União/Advocacia Geral da União.

- Atendimento aos padrões e modelos do Governo Eletrônico:

	Atende	Não atende	Não se aplica
ePing			X
eMag			X
ePwg			X
ICP-Brasil	X		
e-ARQ	X		
Design System			X

- Necessidade de adequação do ambiente para implantação e operação da solução:
  - Recursos materiais: não há
  - Recursos humanos: não há
  - Há a necessidade de ajustar o fluxo de solicitação e aprovação das solicitações dos usuários.
- Mecanismos de continuidade da solução:
  - Em caso de encerramento do contrato, as emissões urgentes poderão ser tratadas por meio de dispensa por valor, enquanto uma nova contratação é realizada.
- Critérios de comparação das soluções: conforme exposto no tópico “Análise de Possíveis Soluções”.

Confirmando que a solução viável para a demanda em tela é a Solução 1: Certificação digital tipo A3 sem fornecimento de token, portanto não há outra com a qual compará-la. No entanto, existem dois caminhos possíveis para a implementação dessa solução:

- iniciar procedimento licitatório para buscar a contratação com o mercado;
- contratar o serviço com o SERPRO.

Portanto, pelos motivos expostos, recomenda-se a adoção da Solução 1: Certificação digital tipo A3 sem fornecimento de token, sendo esta implementada por meio da contratação desse serviço com o SERPRO, ao custo estimado de R$ 359,80

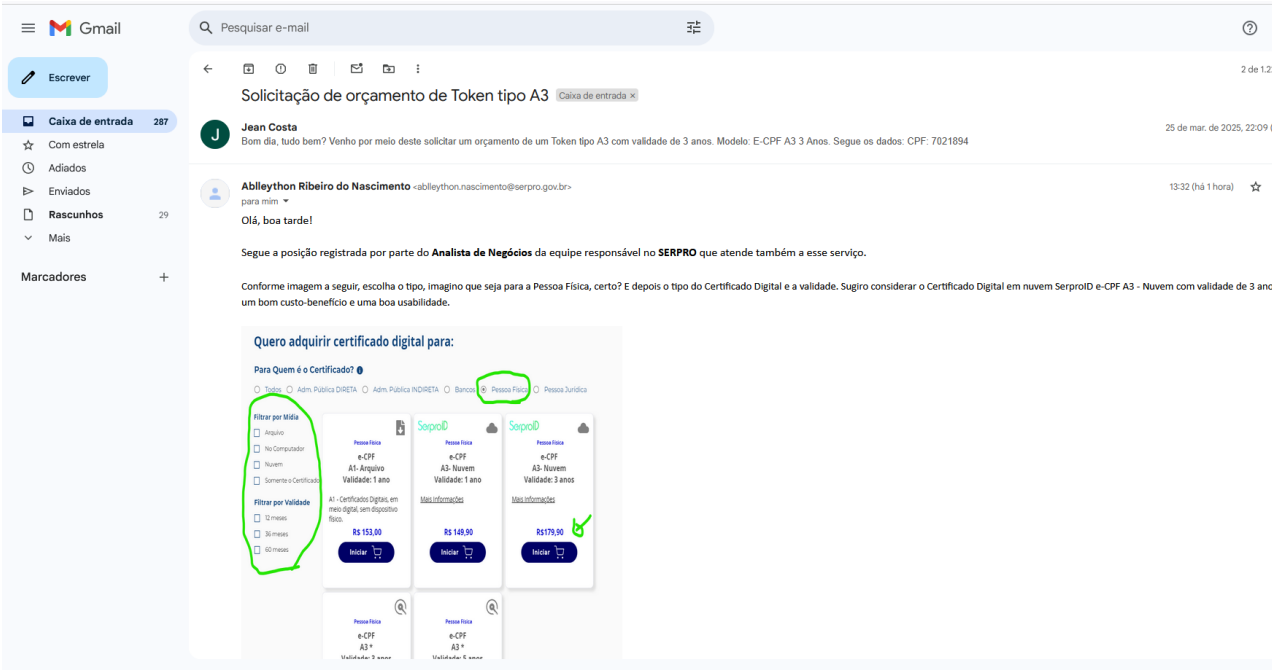
10. Registro de soluções consideradas inviáveis

A Solução 2 não atende aos requisitos 6 e 12, visto que a certificação digital em nuvem pode apresentar incompatibilidade com alguns sistemas atualmente em uso no batalhão que não possuem suporte nativo a esse tipo de certificado. Assim, tem-se algum grau de incerteza quanto à viabilidade dessa solução.
Entende-se que, em um primeiro momento, será prudente adotar-se uma solução mais tradicional e manter essa solução mais inovadora para o futuro, quando a integração da solução com os sistemas estiver mais madura e difundida. No que se refere à economicidade, a solução 2 não atende, pois o Batalhão possui ainda um volume expressivo de tokens utilizáveis, que estão em atividade. Caso a solução 2 fosse adotada, haveria um descarte desnecessário desse material, ocasionando um prejuízo ao erário.

11. Análise comparativa de custos (TCO)

A única solução que atende plenamente as necessidades elicitadas pelo demandante é a Solução 1:.

Dessa forma, a análise de custo das soluções Certificação digital tipo A3 sem fornecimento de token ficará restrita a essa solução.
Em virtude da relativa simplicidade do objeto, o custo da solução resume-se, basicamente, ao custo do fornecimento dos certificados digitais A3.
Assim, foi efetuada a seguinte pesquisa:



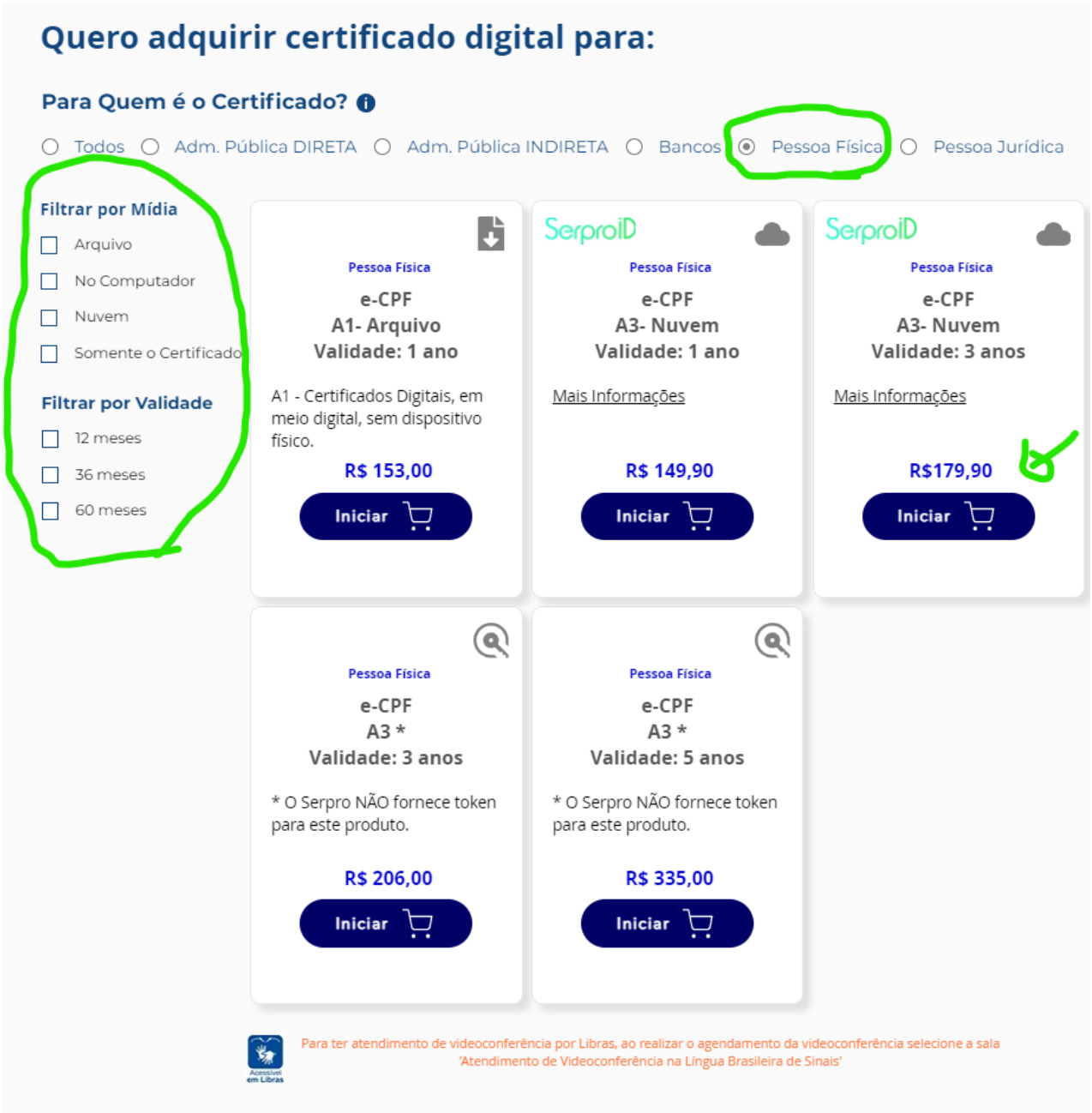


Tabela 5: Pregões para contratação de certificação digital A3 sem fornecimento de token

Preço médio unitário	
Certificação digital A3 sem fornecimento de token	R$ 169,47

Tabela 6: Preço médio unitário

No entanto, além da busca da solução no mercado, há também a possibilidade de realizar uma nova contratação com o SERPRO. (https://www.serpro.gov.br/menu/noticias/noticias-2020/emissao-certificado-digital-via-sigepe) , uma vez que o atual fornecimento de certificados digitais para a CGU já ocorre via Contrato 30/2020, destacando:

- Processo 100% online, ou seja, não há necessidade de deslocamento do servidor a um balcão de atendimento presencial;

- Maior segurança, visto que o SIGEPE registra a demanda via requerimento do servidor interessado em obter a certificação digital;
- Há a assinatura de um contrato que vigerá por determinada quantidade de meses;
- O pagamento é mensal, baseado na quantidade de certificados emitidos no mês;
- A validade do certificado digital A3 é de 3 anos;
- Há a exata opção que fornece certificado digital A3 sem token;
- Somente é possível a solicitação de emissão de certificados por meio do SIGEPE a servidores públicos.
- A instalação do certificado digital é feita pelo próprio usuário, sendo que o SERPRO disponibiliza instruções e ajuda interativa (https://certificados.serpro.gov.br/emissaosigepe/html/ e https://serpro.gov.br/menu/noticias/noticias-2020/como-solicitar-certificado-digital-pelo-sigepe);
- Há dois papéis: solicitante e aprovador;
- O aprovador de requerimento de certificado digital é definido pelo Órgão contratante.

Além dessas informações, foi obtida ainda uma proposta comercial do SERPRO (vide ANEXO II) para subsidiar a análise comparativa de custos com valor atualmente praticado por essa empresa.

Considerando essas informações obtidas, a contratação do serviço de certificação digital com o SERPRO apresenta-se vantajosa , principalmente pela integração com o SIGEPE e pelo menor preço oferecido.

Preço médio unitário	
Média de preço via Tabela 6	R$ 169,47

12. Descrição da solução de TIC a ser contratada

A solução escolhida como mais adequada para o pleno atendimento da demanda é a Solução 1: Certificação digital tipo A3 sem fornecimento de token.

Essa solução consiste em contratar, junto ao SERPRO, serviço de certificação digital A3, conforme especificações neste documento e quantitativos da seguinte tabela:

Objeto da solução escolhida			
Item	Descrição	Quantidade	Métrica
1	Certificação digital A3 sem fornecimento de token	10	Unidade

Tabela 8: Objeto da solução escolhida

A emissão dos certificados será 100% online, obedecendo, em linhas gerais, ao seguinte fluxo:

1. Mediante prévia orientação interna da contratante, o servidor será instruído a efetuar o requerimento de seu certificado digital via SIGEPE;
2. A requisição será aprovada por servidor da CGU designado;

3. Da aprovação ou negação de requerimento, um e-mail do SIGEPE será enviado ao servidor com os devidos esclarecimentos sobre a rejeição do requerimento ou instrução para consolidar a baixa do certificado digital .

A contratação da solução, via dispensa de licitação, nos termos do inciso IX, artigo 75, da Lei n° 14.133/2021, com o SERPRO, pessoa jurídica de direito público interno, apresenta-se interessante, principalmente pela integração com o SIGEPE.

O contrato será de 5 (cinco) anos, a fim de cobrir as emissões de certificados estimadas para os exercícios de 2024 a 2028.

Os pagamentos serão mensais, sendo cobrados os valores referentes apenas às quantidades efetivamente emitidas de certificados digitais naquele mês. Se não houver nenhuma emissão de certificado durante o mês, não haverá valor a ser faturado.

13. Estimativa de custo total da contratação

Valor (R$): 1.694,70

Para estimar o valor da contratação, foi realizada uma pesquisa de preços diretamente com o fornecedor via email *Tabela 5: Pregões para contratação de certificação digital A3 sem fornecimento de token, e considerando* o valor praticado no contrato em vigor e o valor da proposta comercial apresentada pelo SERPRO. Dessa forma o valor estimado é R$ 1.694,70, estabelecido com base no preço da proposta comercial do SERPRO.

14. Justificativa técnica da escolha da solução

Conforme explicitado neste Estudo Técnico Preliminar, a opção pela presente solução justifica-se por ser esta a única viável para o pleno atendimento aos requisitos da demanda do requisitante.

Além de atender aos requisitos da demanda e a compatibilidade de preços do mercado, verificou-se que a presente solução, que está implantada no batalhão, atende satisfatoriamente as necessidades desejadas. Ou seja, a solução é conhecida pela área técnica e não haverá necessidade de alteração e implantação de novos procedimentos.

Por ser de amplo uso, foi possível apurar os valores que estão sendo contratados pelo Poder Público referentes ao objeto de estudo.

Portanto, a solução: (i) atende aos requisitos elencados na demanda do requisitante; (ii) é amplamente utilizada no âmbito dos órgãos e entidades da Administração Pública; e (iii) permite uma estimativa mais precisa de seu custo.

Por esses motivos, a Solução 1: Certificação digital tipo A3 sem fornecimento de token foi escolhida, sendo recomendada a contratação direta, via dispensa de licitação, nos termos do inciso IX, artigo 75, da Lei n° 14.133/2021, com o SERPRO, pessoa jurídica de direito público interno, devido às vantagens identificadas ao longo deste ETP.

15. Justificativa econômica da escolha da solução

Diante da proposta apresentada pelo Serpro, a solução 1 apresenta menor custo por certificado, se comparada às demais cotações apresentadas na tabela 7 do item 11 - Análise comparativa de custos (TCO). Em complemento, a solução 1 favorecerá o reaproveitamento de tokens já em atividade e no ambiente do batalhão.

16. Benefícios a serem alcançados com a contratação

Garantir a continuidade de acesso aos diversos sistemas que exigem essa tecnologia de segurança e de autenticidade atendendo a demanda atual e futura, no âmbito da CGU.

17. Providências a serem Adotadas

Não existe necessidade de adequação do ambiente da CGU para viabilizar a execução contratual, uma vez que a solução está em uso atualmente.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Considerando as disposições constantes neste estudo, sobretudo, acerca das justificativas da necessidade de aquisição e do quantitativo estimado, esta equipe se posiciona pela VIABILIDADE da contratação.

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.

VICTOR BRITO PORTELA

Setor Requisitante

JOSE RIBAMAR DA COSTA JUNIOR

Fiscal Adm

ROGERIO ALEX AQUINO DE CASTRO

Ordenador de Despesas