



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE LAVRAS
PRÓ-REITORIA DE PLANEJAMENTO E GESTÃO



ANEXO I DO TERMO DE REFERÊNCIA

ESTUDO TÉCNICO PRELIMINAR

DADOS DO PROCESSO

Oficialização da demanda (DOD):	Documento 23090.041246/2018-11
Objeto:	Contratação de empresa especializada na prestação de serviços de emissão de certificados digitais do tipo A3, e-CPF, padrão ICP-Brasil, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, padrão ICP-Brasil, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.
Portarias de designação:	Nº 38, de 1º de março de 2019 – Pró-Reitoria de Planejamento e Gestão
Equipe de Planejamento	Clayton Ferreira Santos, Bruno da Silva Gonçalves e Miriam Rosa Silva.

NORMATIVOS QUE DISCIPLINAM OS SERVIÇOS A SEREM CONTRATADOS

Instrução Normativa nº 1, de 4 de abril de 2019;
Instrução Normativa nº 202, de 18 de setembro de 2019;
Instrução Normativa SEGES/MP nº 5, de 26 de maio de 2017;
Lei nº 8.666, de 21 de junho de 1993;
Instrução Normativa nº 3, de 20 de abril de 2017;
Lei nº 10.520, de 17 de julho de 2002;
Decreto nº 9.507, de 21 de setembro de 2018;
Decreto nº 5.450, de 31 de maio de 2005;
Decreto nº 7.892, de 23 de janeiro de 2013.

REFERÊNCIA AO PDI/PDTIC DA UFLA

A demanda de aquisição dos Certificados Digitais e-CPF e e-CNPJ, do tipo A3, está prevista no PDTIC 2017-2020, listada como Necessidade 97 (Serviços de emissão de certificados digitais padrão ICP-Brasil), Meta 134 (serviços de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, padrão ICP-Brasil, com e sem fornecimento de dispositivo físico de armazenamento), com execução prevista para o segundo semestre de 2019.

1 – INTRODUÇÃO

A presente análise tem por objetivo identificar e analisar os cenários para o atendimento da demanda, bem como demonstrar a viabilidade técnica e econômica da contratação de empresa especializada na prestação de serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão

de certificados digitais do tipo A3, e-CPF e e-CNPJ, padrão ICP-Brasil, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos, bem como fornecer informações necessárias para subsidiar o respectivo processo.

2 – DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Contratação de empresa especializada para prestação de serviços de renovação de Certificados Digitais do tipo A3, e-CPF, compatíveis com a infraestrutura de chave pública ICP-Brasil, sem fornecimento de mídias criptográficas portáteis para armazenamento - emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, compatíveis com a infraestrutura de chave pública ICP-Brasil, com fornecimento de mídias criptográficas portáteis para o armazenamento dos certificados digitais utilizados pelos servidores da UFLA, que permitam o acesso aos diversos sistemas da Administração Pública Federal (Sistema de Concessão de Diárias e Passagens - SCDP, Sistema de Integrado de Administração de Pessoal – SIAPE, Sistema Integrado de Administração Financeira - SIAFI, Receita Federal, Portal de Compras – Comprasnet, Receita Federal), conforme especificações e condições estabelecidas no presente Estudo Preliminar.

3 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES

Necessidades de Negócio da Área Requisitante

Id	Funcionalidades	Envolvidos
1.	Autenticação por meio de certificado digital no sistema estruturante do governo: SCDP	PROPLAG, PRGDP, PROEC, DCOF, PRG, PRPG, PROINFRA, PRP, PRAEC, DRCA, AUDITORIA, REITORIA, DIPS, DRI, DICON, DIREC, DGM, DEPARTAMENTOS DIDÁTICOS, DGTI, DMP, PROGRAMA DE PÓS-GRADUAÇÃO
2.	Autenticação por meio de certificado digital no sistema estruturante do governo: SIAPENET	PRGDP, DGTI
3.	Autenticação por meio de certificado digital no sistema estruturante do governo: SIAFI	DCOF, PROPLAG, AUDITORIA, PRPG
4.	Autenticação por meio de certificado digital no sistema estruturante do governo: COMPRASNET	DGM, PROPLAG, DCOF
5.	Autenticação por meio de certificado digital no sistema: WORKFLOW - TERMO DE OUTORGA	PRP, PRG, DIREC, DEPARTAMENTOS DIDÁTICOS, PROGRAMA DE PÓS-GRADUAÇÃO
6.	Autenticação por meio de certificado digital no sistema da Receita Federal do Brasil	PRGDP

Identificação das necessidades tecnológicas

<p>1. Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.</p>	<p>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);</p> <p>1.2. Nível: A3;</p> <p>1.3. Validade: 3 (três) anos, contados a partir da data do aceite definitivo do certificado.</p> <p>1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2;</p> <p>1.5. Tipo: e-CPF.</p> <p>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, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros;</p> <p>1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal);</p> <p>1.8. Os certificados digitais deverão ser compatíveis com os tokens modelo: token StarSign USB – G&D Burti, StarDign Crypto – USB-Token S, SafeNet iKey 2032 e SafeNet Token 5100/5110 já existentes na UFLA.</p>
<p>2. Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.</p>	<p>2.1. Certificado</p> <p>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);</p> <p>2.1.2. Nível: A3;</p> <p>2.1.3. Validade: 3 (três) anos, contados a partir da data do aceite definitivo do certificado.</p> <p>2.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2;</p> <p>2.1.5. Tipo: e-CPF.</p> <p>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, do Planejamento e da Defesa, Procuradoria Geral da Fazenda</p>

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, ComprasNet, Receita Federal).

2.2. Dispositivo Físico de armazenamento

2.2.1. Dispositivo Físico de armazenamento (token criptográfico), 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 do aceite definitivo do certificado.

2.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior.

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

2.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

2.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.

2.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas.

2.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3).

2.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas.

2.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.

2.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits.

2.2.12. Possuir carcaça resistente à água e à violação.

2.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).

2.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).

2.2.15. 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).

2.2.16. 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.

2.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, 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;

2.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.

2.2.18. Possuir indicador luminoso de estado do dispositivo.

2.2.19. Assinar dados digitalmente em até 10 (dez) segundos.

2.2.20. O token criptográfico deverá possuir certificação do INMETRO.

2.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura.

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 token criptográfico mediante a utilização de PUK (Pin Unlock Key).

2.3.9. ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores).

2.3.10. suportar os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome.

	<p>2.3.11. possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores).</p> <p>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.</p> <p>2.3.13. implementar mecanismo de autenticação tipo challenge-response.</p> <p>2.3.14. forçar a troca da senha padrão no primeiro acesso.</p> <p>2.3.15. bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos.</p> <p>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.</p> <p>2.3.17. bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico.</p> <p>2.4. Software</p> <p>2.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:</p> <p>2.4.1.1. gerenciamento do dispositivo;</p> <p>2.4.1.2. exportação de certificados armazenados no dispositivo;</p> <p>2.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;</p> <p>2.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;</p> <p>2.4.1.5. visualização de certificados armazenados no dispositivo;</p> <p>2.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;</p> <p>2.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.</p> <p>2.4.2. Deverá ser disponibilizado portal para download de drivers/Softwares de forma ilimitada.</p> <p>2.4.3. Garantia de 3 (três) anos, contada a partir do aceite definitivo dos produtos.</p>
<p>3. Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.</p>	<p>3.1. Certificado</p> <p>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);</p>

- 3.1.2. Nível: A3;
- 3.1.3. Validade: 3 (três) anos, contados a partir da data do aceite definitivo do certificado.
- 3.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2;
- 3.1.5. Tipo: e-CNPJ;
- 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, do Planejamento 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, ComprasNet, Receita Federal).
- 3.2. Dispositivo Físico de Armazenamento**
- 3.2.1. Dispositivo Físico de armazenamento (Token criptográfico), 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)
- 3.2.2. Validade: 3 (três) anos, contados a partir da data do aceite definitivo do certificado.
- 3.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior.
- 3.2.4. Ser aderente às normas do Comitê Gestor da ICP-Brasil.
- 3.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.
- 3.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.
- 3.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas.
- 3.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3).
- 3.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas.
- 3.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.
- 3.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits.
- 3.2.12. Possuir carcaça resistente à água e à violação.

<p>3.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).</p> <p>3.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).</p> <p>3.2.15. 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).</p> <p>3.2.16. 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.</p> <p>3.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, 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;</p> <p>3.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.</p> <p>3.2.18. Possuir indicador luminoso de estado do dispositivo.</p> <p>3.2.19. Assinar dados digitalmente em até 10 (dez) segundos.</p> <p>3.2.20. O token criptográfico deverá possuir certificação do INMETRO.</p> <p>3.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura.</p> <p>3.3. Funcionalidades</p> <p>3.3.1. permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.</p> <p>3.3.2. permitir personalização eletrônica através de parâmetro identificador interno (label).</p> <p>3.3.3. permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.</p> <p>3.3.4. permitir criação de senhas com caracteres alfanuméricos.</p> <p>3.3.5. permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.</p> <p>3.3.6. 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.</p> <p>3.3.7. armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados</p>
--

<p> 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. </p> <p> 3.3.8. permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key). </p> <p> 3.3.9. ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). </p> <p> 3.3.10. suportar os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. </p> <p> 3.3.11. possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores). </p> <p> 3.3.12. possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo. </p> <p> 3.3.13. implementar mecanismo de autenticação tipo challenge-response. </p> <p> 3.3.14. forçar a troca da senha padrão no primeiro acesso. </p> <p> 3.3.15. bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos. </p> <p> 3.3.16. 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. </p> <p> 3.3.17. bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. </p> <p> 3.4. Software </p> <p> 3.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita: </p> <p> 3.4.1.1. gerenciamento do dispositivo; </p> <p> 3.4.1.2. exportação de certificados armazenados no dispositivo; </p> <p> 3.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; </p> <p> 3.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; </p> <p> 3.4.1.5. visualização de certificados armazenados no dispositivo; </p> <p> 3.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; </p>

	<p>3.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.</p> <p>3.4.2. Deverá ser disponibilizado portal para download de drivers/Softwares de forma ilimitada.</p> <p>3.4.3. Garantia de 3 (três) anos, contada a partir do aceite definitivo dos produtos.</p>
--	---

DEMAIS REQUISITOS DA CONTRATAÇÃO

1.	<p>O serviço de certificação presencial e validação de documentos de cada certificado deverá ser prestado no município de Lavras. Para fins da presente contratação, o local em que a Contratada prestará o serviço será aqui denominado “Posto de Atendimento”. Considerando que o serviço de certificação digital é essencial para o funcionamento das atividades da Instituição, é fundamental que ele esteja disponível sempre que houver demanda por parte da Contratante, observados os prazos descritos nos itens 8 e 9 desta tabela. <u>Ressalta-se que a Contratante não disponibilizará estrutura física, recursos materiais ou humanos para a execução do serviço, sendo tais de responsabilidade exclusiva da Contratada.</u> Em hipótese alguma, os servidores da Contratante se deslocarão para outra cidade para obter o serviço, ainda que a empresa custeie as despesas de deslocamento. Tal exigência visa a economicidade para a Administração, evitando custos com diárias e despesas com locomoção para os servidores se deslocarem a outras cidades para realizar a validação presencial dos documentos, bem como o comprometimento da carga horária de trabalho, custeada pelo contribuinte.</p>
2.	<p>A Contratante comunicará à Contratada, via e-mail a ser designado para esse fim, a identificação de servidores autorizados a receber certificados digitais. Essa forma de comunicação poderá ser substituída, caso a Contratada possua sistema próprio que permita à UFLA enviar os nomes de tais servidores.</p>
3.	<p>A Contratada deverá disponibilizar portal web de cadastramento prévio e agendamento, em que seja suficiente um único comparecimento do servidor da UFLA ao posto de atendimento para que o certificado seja emitido. Para casos em que for necessário mais de um comparecimento do servidor, devido a problemas alheios à vontade da Contratada, ela deverá apresentar justificativa à Contratante.</p>
4.	<p>A Contratada deverá disponibilizar agenda em seu portal web para que o servidor da UFLA escolha a data para a validação presencial em seu posto de atendimento. O agendamento também poderá ser realizado por telefone.</p>
5.	<p>A Contratada deverá disponibilizar Posto de Atendimento para validação presencial e emissão do certificado, cujo horário de funcionamento seja, ao menos, das 8 (oito) às 17 (dezessete) horas, de segunda à sexta-feira, exceto feriados. No caso do cadastramento prévio a ser solicitado pelo servidor da UFLA, que será realizado por telefone ou pela internet, os horários a serem disponibilizados pela empresa também deverão ser, pelo menos, os supracitados.</p>
6.	<p>No momento do cadastramento, a Contratada deverá fornecer ao servidor da UFLA uma lista com todos os documentos necessários para a emissão do certificado, a fim de evitar a necessidade de mais de um comparecimento do servidor ao posto de atendimento para a</p>

	conclusão do serviço.
7.	A Contratada deverá orientar o titular do certificado, durante a validação presencial, sobre as melhores práticas de uso, evitando assim, o mau uso de certificados digitais com seus respectivos dispositivos de armazenamento e suas conseqüências.
8.	A Contratada deverá realizar a validação presencial para emissão dos certificados em, no máximo, 7 (sete) dias úteis após o agendamento.
9.	Após a validação presencial do certificado, a Contratada terá, no máximo, 2 (dois) dias úteis para entregar o certificado ao servidor da UFLA.
10.	Até o quinto dia útil de cada mês, a Contratada enviará à Contratante, em forma digital, lista com os nomes dos servidores da UFLA que receberam certificados digitais no mês anterior, especificando: <ul style="list-style-type: none"> a) o tipo de serviço prestado e o tipo de serviço prestado, isto é: emissão de certificado digital, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação; emissão de certificado digital, e-CPF, com fornecimento de dispositivo físico de armazenamento; emissão de certificados, e-CNPJ, com fornecimento de dispositivo físico de armazenamento; b) data em que o serviço foi prestado.
11.	A quantidade de certificados a serem emitidos por agendamento será de apenas 01 (um) por atendimento, a critério da demanda da UFLA.
12.	Os dispositivos de armazenamento (tokens criptográficos) deverão ser novos, de primeiro uso e em perfeitas condições de utilização, de forma a permitir completa segurança por parte da Contratante, sob pena do não recebimento definitivo dos mesmos.
13.	A licitação será realizada por itens, uma vez que são independentes entre si. Desta forma, haverá melhor aproveitamento do mercado e ampliação da competitividade.

Demandas dos Potenciais Gestores	Envolvidos
A contratação já abrange a demanda de todos os setores da Instituição.	Setor Requisitante

ESTIMATIVA DA DEMANDA
<p>A utilização da certificação digital é fundamental para que os servidores da Universidade Federal de Lavras (UFLA) acessem os diversos sistemas da Administração Pública Federal (SCDP, SIAPE, SIAFI, Receita Federal e Comprasnet) que permitem o funcionamento das atividades institucionais.</p> <p>Após a realização de levantamento da demanda com os servidores docentes e técnico-administrativos para verificar a necessidade de renovação de certificados digitais, e- CPF, foram identificadas 46 demandas. Destas, 38 (trinta e oito) foram solicitadas para o ano de 2019 e 8 (oito) para ano seguinte (certificados com validade até novembro de 2020).</p> <p>O levantamento também apontou a necessidade de emissão de 43 (quarenta e três) certificados digitais e-CPF, com fornecimento de dispositivos físicos de armazenamento, para o ano</p>

de 2019.

Uma vez que a atual gestão da UFLA termina em maio de 2020 e o novo dirigente da instituição poderá modificar toda a equipe de gestão, a equipe de planejamento da contratação entendeu ser prudente estimar a demanda de emissões de certificados digitais, e-CPF e e-CNPJ, com fornecimento de dispositivos físicos de armazenamento, para o ano de 2020 considerando o número de cargos CD1, CD2, CD3, CD4, FG1, FG2 e FUC. O levantamento foi realizado no Portal da Transparência no dia 10 de maio de 2019 e apontou o quantitativo de 215 (duzentos e quinze).

Os certificados digitais de Pessoa Jurídica, e-CNPJ, da UFLA venceram em junho de 2019. Sendo assim, será necessário a aquisição de 2 (duas) unidade para atender os atuais reitor e vice-reitora. Porém, devido à possível mudança na Reitoria que ocorrerá em maio de 2020, também será necessário demandar mais 2 (dois) certificados e-CNPJ para atender aos novos reitor (a) e vice-reitor (a). Não será contratada a renovação do certificado e- CNPJ existente (emissão do certificado, sem fornecimento de dispositivo físico de armazenamento), já que a mídia criptográfica existente não é passível de renovação.

Uma vez que não há saldo em Ata de Registro de Preço ou Contrato para atender às demandas supracitadas, é fundamental proceder com a contratação de empresa especializada para a emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ. A impossibilidade de acesso aos Sistemas da Administração Pública Federal por parte dos servidores que utilizam a certificação digital poderá prejudicar fortemente as atividades administrativas da Instituição.

Apesar dos esforços da equipe de planejamento em levantar um quantitativo próximo à realidade, as incertezas acerca dos impactos da mudança de gestão na Universidade em relação aos ocupantes de cargos cuja utilização de certificados digitais é fundamental para o exercício da função, os quantitativos apresentados são meras estimativas. Por isso, não se constituem, em hipótese alguma, compromissos futuros para a UFLA, razão pela qual não poderão ser exigidos, nem considerados como valor para pagamento mínimo, podendo sofrer alterações de acordo com as necessidades da Contratante, sem que isso justifique qualquer indenização à Contratada.

Diante do supracitado, sugere-se que a licitação ocorra por meio de Registro de Preços. O Decreto nº 7.892, de 23 de janeiro de 2013, traz a seguinte redação em seu Art. 3º:

“O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

- I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
- II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
- III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
- IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.”

Entende-se, portanto, que a contratação em questão se insere nos incisos I, II e IV do referido

Decreto.

Devido às motivações já apresentadas que levaram a decisão por um Pregão SRP, foi descartada a possibilidade de se fazer uma dispensa de licitação, contratando-se com empresa pública. Além disso, ressalta-se a necessidade de o serviço ser prestado na cidade de Lavras, por questões de economicidade para a Administração, evitando custos com diárias e despesas com locomoção para os servidores se deslocarem a outras cidades para realizar a validação presencial dos documentos, bem como o comprometimento da carga horária de trabalho, custeada pelo contribuinte. Também, não é desejável que a Contratante disponibilize local, equipamentos e servidores para possibilitar a vinda de pessoal de empresa pública para executar o serviço nas dependências da Contratante. É fundamental que o serviço seja prestado com celeridade sempre que a Contratante tenha demandas, ainda que pontuais, observados os prazos definidos no presente documento. Por fim, demonstrou-se na sessão pública do Pregão nº 33/2019 que os preços ofertados pelas licitantes foram inferiores àqueles que constam no site de empresa pública.

ESTIMATIVA DE NECESSIDADE DE CERTIFICAÇÃO DIGITAL 2019/2020

ITEM	Ano 2019	Ano 2020	TOTAL
1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.	38	8	46
2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	43	215	258
3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	2	2	4

4 – ANÁLISE DE SOLUÇÕES

A solução será adquirida na forma de contratação de serviço e terá que contemplar a emissão de certificados do nível A3, e-CPF (com e sem fornecimento de dispositivo físico de armazenamento) e e-CNPJ (com fornecimento de dispositivo físico de armazenamento), com validade de 3 anos, em conformidade com o padrão ICP-Brasil, , conforme definido nos itens desta licitação.

Vale destacar que não é viável adquirir o certificado digital separadamente dos dispositivos físicos de armazenamento, pois seriam necessários dois processos para estudar a viabilidade tanto da aquisição do serviço quanto do bem. Além disso, as duas Atas de Registro de Preços, uma para bem e outra para serviço, deveriam estar perfeitamente sincronizadas em relação à vigência e quantitativos. Portanto, os custos do processo licitatório e do acompanhamento para a execução de

ambas as Atas elevariam os custos para a Administração. Ressalta-se ainda que, o padrão criptográfico do certificado digital não é compatível com qualquer tipo de dispositivo físico de armazenamento, portanto, ainda que se fizesse licitação para compra de bem (dispositivo físico de armazenamento), ao longo da vigência da Ata de Registro de Preços, o padrão criptográfico do certificado digital poderia mudar, impedindo a utilização dos dispositivos físicos de armazenamento e do serviço de certificação digital licitados.

A solução tem a possibilidade de ser ofertada de várias maneiras, mudando o meio de armazenamento físico do certificado digital, conforme será exposto a seguir.

O primeiro cenário analisado será com a utilização de *token criptográfico* como dispositivo físico de armazenamento (CENÁRIO 1).

Outra possibilidade, é usar um *smartcard* (cartão com um circuito de memória interno) como dispositivo físico de armazenamento que, para ser usado em um computador, é necessária a utilização de um dispositivo leitor de cartão. Essa alternativa será abordada no CENÁRIO 2.

Há ainda a opção de utilizar o armazenamento do certificado em nuvem, porém essa solução precisa de rede de internet estável, tanto para o computador, quanto para o dispositivo móvel previamente autorizado. Além disso, é necessário uma verificação de segurança de pelo menos dois níveis, isto é, por meio do uso de uma senha (PIN) utilizada pelo usuário e de uma segunda validação recebida através de um aplicativo em seu dispositivo móvel. Como essa solução necessita da utilização de bens privados dos usuários, isto é, dispositivos móveis e, até mesmo, dados móveis, uma vez que há regiões na área do campus universitário em que não há sinal de dados de internet ou este é instável, essa comissão descartou esse cenário da análise de viabilidade.

Por questão de segurança da informação, existe a tendência de ampliação da solução para atender a todos os servidores da instituição futuramente.

Por fim, não será necessário adequar o ambiente para contratação da solução em questão, uma vez que os serviços não serão prestados nas dependências da Contratante.

4.1 - IDENTIFICAÇÃO DAS SOLUÇÕES

SOLUÇÃO/CENÁRIO 1

Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de *token USB* como dispositivo físico de armazenamento.

Descrição do Cenário 1

A solução provê a emissão de certificado digital e-CPF, sem fornecimento de dispositivo físico de armazenamento (renovação) e o armazenamento de certificados digitais do tipo A3, e-CPF e e-CNPJ, em um USB token, dispositivo portátil em formato chaveiro capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas as chaves, estas estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do *token* (seu

hardware criptográfico), além de protegê-las de riscos como roubo ou violação. Para o acesso ao certificado digital, é necessária apenas a conexão do *token* USB a uma porta USB no periférico a ele conectado.

Possíveis fornecedores: Certisign, Serpro, Prodemge, Serasa Experian e BR Certificados.

Análise da Solução

1. Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública.

Não se aplica ao objeto.

2. Alternativas do mercado.

Descrição dos cenários 1 e 2 (token criptográfico e cartão+leitora). A alternativa de certificação em nuvem foi descartada, conforme exposto.

3. Existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016.

Não se aplica ao objeto.

4. Políticas, os modelos e os padrões de governo que se aplicam ao objeto.

4.1 Infraestrutura de Chaves Públicas Brasileira;

4.2 ICP-Brasil.

5. Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual.

Não será necessário adequar o ambiente para contratação da solução em questão, pois os serviços não serão prestados nas dependências da Contratante.

6. Diferentes modelos de prestação do serviço.

Descrição dos cenários abordados.

7. Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes.

Descrição dos cenários abordados.

8. Possibilidade de aquisição na forma de bens ou contratação como serviço.

O objeto será contratado na forma de serviço.

9. Ampliação ou substituição da solução implantada.

Possibilidade de ampliação futura da solução, por questões de segurança da informação.

PESQUISAS DE PREÇOS

Para a obtenção dos preços estimados para o Cenário 1, foi realizada pesquisa de preço no Painel de Preços e em mídia especializada, de acordo com o disposto na INSTRUÇÃO NORMATIVA Nº 3, DE 20 DE ABRIL DE 2017, em seu artigo 2º, incisos I e III, respectivamente:

INSTRUÇÃO NORMATIVA Nº 3, DE 20 DE ABRIL DE 2017

Art. 2º A pesquisa de preços será realizada mediante a utilização dos seguintes parâmetros:

- I - Painel de Preços, disponível no endereço eletrônico <http://paineldeprecos.planejamento.gov.br>;
III - Pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, desde que contenha a data e hora de acesso.”

ITEM 1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.

Para o item 1, foram encontrados os preços listados no quadro abaixo. Utilizou-se de forma combinada os preços obtidos no Painel de Preços e em mídia especializada e, em seguida, adotou-se a média das três cotações encontradas, obtendo-se o preço unitário estimado no valor de **R\$ 142,85**. A média foi utilizada, uma vez que os valores são próximos entre si.

ID	DADOS DA PESQUISA DE PREÇOS	VALOR UNITÁRIO DO ITEM
1	Identificação da Compra: Pregão Eletrônico Nº 22/2019 (SRP) Órgão: INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO ACRE Órgão Superior: MINISTERIO DA EDUCACAO Descrição do Item: EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FÍSICA Código do CATSER: 27219 Nome do Fornecedor: OBJECTTI SOLUCOES LTDA CNPJ/CPF: 11735236000192 Número da UASG: 158156 Data do Resultado: 05 de julho de 2019.	R\$ 103,55
2	Descrição: e-CPF A3 - Somente Certificado Certisign Certificadora Digital S.A CNPJ: 01.554.285/0001-75 Link: https://www.certisign.com.br/certificado-digital/ecpf Data e hora de acesso: 14 de outubro de 2019, às 18h15min.	R\$ 190,00
3	Descrição: e-CPF A3 - Somente certificado Companhia de Tecnologia da Informação do estado de Minas Gerais - PRODEMGE CNPJ: 16.636.540/0001-04 Link: https://wwws.prodemge.gov.br/certificados-digitais/e-cpf Data e hora de acesso: 14 de outubro de 2019, às 18h14min.	R\$ 135,00
TOTAL		R\$ 428,55
MÉDIA		R\$ 142,85

Atualmente, os certificados digitais existentes na UFLA estão armazenados em *tokens*, razão pela qual não é necessário o fornecimento de dispositivo físico de armazenamento para fazer a emissão-

renovação. Caberá a empresa licitante ofertar o seu preço, **para o Item 1**, considerando apenas a emissão do certificado, sem o fornecimento da mídia criptográfica.

ITEM 2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.

Para o item 2, utilizou-se os preços obtidos no Painel de Preços em seguida, adotou-se a média das três cotações encontradas, obtendo-se o preço unitário estimado no valor de **R\$ 156,99**. A média foi utilizada, uma vez que os valores são próximos entre si.

ID	DADOS DA LICITAÇÃO	VALOR UNITÁRIO DO ITEM
1	Identificação da Compra: Pregão Eletrônico N° 3/2019 (SRP) Órgão: Instituto Federal de Educação, Ciência e Tecnologia de Brasília - CAMPUS ESTRUTURAL INST. FED. DE BRASÍLIA Órgão Superior: MINISTÉRIO DA EDUCAÇÃO Descrição do Item: EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FÍSICA Código do CATSER: 27189 Nome do Fornecedor: JULIANA NASCIMENTO LANZOTTI CNPJ/CPF: 30.633.996/0001-33 Número da UASG: 152146 Data do Resultado: 30 de maio de 2019.	R\$ 185,98
2	Identificação da Compra: Pregão Eletrônico N° 22/2019 (SRP) Órgão: TRIBUNAL SUPERIOR ELEITORAL/SEC.ADM/DF Órgão Superior: JUSTICA ELEITORAL Descrição do Item: EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FÍSICA Código do CATSER: 27197 Nome do Fornecedor: DIGISEC - CERTIFICACAO DIGITAL EIRELI CNPJ/CPF: 18.799.897/0001-20 Número da UASG: 070001 Data do Resultado: 05 de setembro de 2019.	R\$ 188,95
3	Identificação da Compra: Pregão Eletrônico N° 04/2019 Órgão: ASSEMBLEIA LEGISLATIVA DE MATO GROSSO Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL Descrição do Item: EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA Código do CATSER: 27189 Nome do Fornecedor: INSTITUTO EUVALDO LODI CNPJ/CPF: 03986163000183 Número da UASG: 926668 Data do Resultado: 17 de junho de 2019.	R\$ 96,05
TOTAL		R\$ 470,98

MÉDIA	R\$ 156,99
--------------	-------------------

ITEM 3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.

Para o item 3, utilizou-se os preços obtidos no Painel de Preços e, em seguida, adotou-se a média das três cotações encontradas, obtendo-se o preço unitário estimado no valor de **R\$ 124,68**. A média foi utilizada, uma vez que os valores são próximos entre si.

ID	DADOS DA LICITAÇÃO	VALOR UNITÁRIO DO ITEM
1	<p>Identificação da Compra: Pregão Eletrônico N° 3/2019 (SRP) Órgão: INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA – CAMPUS ESTRUTURAL INSTITUTO FEDERAL DE BRASÍLIA Órgão Superior: MINISTERIO DA EDUCACAO Descrição do Item: EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURÍDICA Código do CATSER: 27197 Nome do Fornecedor: DIGISEC - CERTIFICACAO DIGITAL EIRELI CNPJ/CPF: 18.799.897/0001-20 Número da UASG: 152146 Data do Resultado: 30 de maio de 2019.</p>	R\$ 103,18
	<p>Identificação da Compra: Pregão Eletrônico N° 4/2019 (SRP) Órgão: ASSEMBLÉIA LEGISLATIVA DO MATO GROSSO Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL Descrição do Item: EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURIDICA Código do CATSER: 27197 Nome do Fornecedor: INSTITUTO EUVALDO LODI CNPJ/CPF: 03986163000183 Número da UASG: 926668 Data do Resultado: 17 de junho de 2019.</p>	R\$ 117,85
2	<p>Identificação da Compra: Pregão Eletrônico N° 40/2019 (SRP) Órgão: PREFEITURA MUNICIPAL DE DUQUE DE CAXIAS Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL Descrição do Item: EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURIDICA Código do CATSER: 27197 Nome do Fornecedor: ONLINE CERTIFICADORA LTDA CNPJ/CPF: 11587975000184 Número da UASG: 985833 Data do Resultado: 04 de outubro de 2019.</p>	R\$ 153,00
TOTAL		R\$ 374,03

MÉDIA	R\$ 124,68
--------------	-------------------

Custo Total de Propriedade: Análise para o “Cenário 1 – TOKEN”			
Item	Valor (R\$)		
	2019	2020	TOTAL
1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.	38 unidades x R\$ 142,85 = R\$ 5.428,30	8 unidades x R\$ 142,85 = R\$ 1.142,80	46 unidades x R\$ 142,85 = R\$ 6.571,10
2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	43 unidades x R\$ 156,99 = R\$ 6.750,57	215 unidades x R\$ 156,99 = R\$ 33.752,85	258 unidades x R\$ 156,99 = R\$ 40.503,42
3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	2 unidades x R\$ 124,68 = R\$ 249,36	2 unidades x R\$ 124,68 = R\$ 249,36	4 unidades x R\$ 124,68 = R\$ 498,72
TOTAL GERAL			R\$ 47.573,24

SOLUÇÃO/CENÁRIO 2	
Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de cartão como dispositivo físico de armazenamento . Acompanha leitora de cartão.	
Descrição do Cenário 2	
A solução provê a emissão de certificados digitais e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e o armazenamento de certificados digitais do tipo A3 em um smart card, ou seja, um hardware em formato estilo “cartão de crédito” capaz de armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas as chaves, estas estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do cartão (seu hardware criptográfico), além de protegê-las de riscos como roubo ou violação. Para o acesso ao certificado digital armazenado no cartão, é necessária que a solução acompanhe uma leitora de <i>smartcards</i> , que se trata do equipamento responsável por fazer a gravação e a leitura dos certificados digitais que ficam armazenados dentro dos Cartões Smart Card. A leitora de cartões possui uma interface USB, sendo responsável por realizar a troca de dados entre o smart card e o periférico a ele conectado.	
Possíveis fornecedores:	Certisign, Serpro, Prodemge, Serasa Experian e BR Certificados.

ANÁLISE DA SOLUÇÃO

Os certificados digitais armazenados em cartão e token realizam exatamente as mesmas operações e possuem as mesmas funcionalidades, o que muda é a praticidade no uso de cada um deles. A principal diferença entre o token e o cartão é que o token não precisa da utilização de uma leitora, já que este se conecta diretamente à porta USB, padrão existente em qualquer computador. Já o cartão precisa de um dispositivo leitor de cartões USB para ser utilizado.

PESQUISAS DE PREÇOS

ITEM 1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.

Para o item 1, foram encontrados os preços listados no quadro abaixo. Utilizou-se de forma combinada os preços obtidos no Painel de Preços e em mídia especializada e, em seguida, adotou-se a média das três cotações encontradas, obtendo-se o preço unitário estimado no valor de **R\$ 142,85**. A média foi utilizada, uma vez que os valores são próximos entre si..

ID	DADOS DA PESQUISA DE PREÇOS	VALOR UNITÁRIO DO ITEM
1	Identificação da Compra: Pregão Eletrônico Nº 22/2019 (SRP) Órgão: Órgão Superior: Descrição do Item: EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA Código do CATSER: 27219 Nome do Fornecedor: OBJECTTI SOLUCOES LTDA CNPJ/CPF: 11735236000192 Número da UASG: 158156 Data do Resultado: 05 de julho de 2019.	R\$ 103,55
2	Descrição: e-CPF A3 - Só Certificado Certisign Certificadora Digital S.A CNPJ: 01.554.285/0001-75 Link: https://www.certisign.com.br/certificado-digital/ecpf Data e hora de acesso: 14 de outubro de 2019, às 18h15min.	R\$ 190,00
3	Descrição: e-CPF A3 - Somente certificado Companhia de Tecnologia da Informação do estado de Minas Gerais - PRODEMGE CNPJ: 16.636.540/0001-04 Link: https://www.prodemge.gov.br/certificados-digitais/e-cpf Data e hora de acesso: 14 de outubro de 2019, às 18h14min.	R\$ 135,00
TOTAL		R\$ 428,55
MÉDIA		R\$ 142,85

Atualmente, os certificados digitais existentes na UFLA estão armazenados em tokens, razão pela qual não é necessário o fornecimento de dispositivo físico de armazenamento para fazer a emissão-renovação. Caberá a empresa licitante ofertar o seu preço, **para o Item 1**, considerando apenas a emissão do certificado, sem o fornecimento da mídia criptográfica.

ITENS 2 E 3

Os preços referenciais para os itens 2 e 3 foram obtidos em mídias especializadas, de acordo com o disposto na INSTRUÇÃO NORMATIVA Nº 3, DE 20 DE ABRIL DE 2017, em seu artigo 2º, inciso III:

INSTRUÇÃO NORMATIVA Nº 3, DE 20 DE ABRIL DE 2017

“Art. 2º A pesquisa de preços será realizada mediante a utilização dos seguintes parâmetros:

.....

III - pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, desde que contenha a data e hora de acesso.”

Justificativa para pesquisa em mídia especializada

Não se encontrou no Painel de Preços contratações de certificação digital A3 armazenado em cartão.

Da mesma forma, não se obteve êxito em pesquisas com contratações similares de outros entes públicos, em execução ou concluídos nos 180 (cento e oitenta) dias anteriores à data da pesquisa de preço, conforme define o inciso II do artigo 2º da Instrução Normativa nº 3 de 20 de abril de 2017.

Diante do exposto acima, a pesquisa de preços para os itens 2 e 3 no Cenário 2 foi realizada apenas em mídia especializada, através dos sites das empresas Certisign Certificadora Digital S.A, Serasa Experian S.A e Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE.

ITEM 2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Cartão para armazenamento do Certificado e Leitora, com validade por 3 anos.

Para o item 2, foram encontrados os preços listados no quadro a seguir e, em seguida, adotou-se a média das três cotações, obtendo-se o preço unitário estimado no valor de **R\$ 354,67**. A média foi utilizada, uma vez que os valores são próximos entre si.

ID	DADOS DA PESQUISA DE PREÇOS	VALOR
1	Descrição: e-CPF A3 - Cartão+Leitora Certisign Certificadora Digital S.A CNPJ: 01.554.285/0001-75 Link: https://www.certisign.com.br/certificado-digital/ecpf Data e hora de acesso: 15 de outubro de 2019, às 8h03min.	R\$ 360,00

2	Descrição: e-CPF A3 - Kit Leitora Serasa Experian S.A CNPJ: 62.173.620/0001-80 Link: https://compra.certificadodigital.com.br/loja/#!/identificacao/e-CNPJ/0649/e-CNPJ-A3-36-MESES-CARTAO-E-LEITORA Data e hora de acesso: 15 de outubro de 2019, às 8h50min.	R\$ 415,00
3	Descrição:e-CPF A3 - Cartão e Leitora Companhia de Tecnologia da Informação do Estado de Minas Gerais - PRODEMGE CNPJ: 16.636.540/0001-04 Link: https://wwws.prodemge.gov.br/certificados-digitais/e-cpf Data e hora de acesso: 15 de outubro de 2019, às 8h06min.	R\$ 289,00
VALOR TOTAL		R\$ 1.064,00
VALOR UNITÁRIO MÉDIO		R\$ 354,67

ITEM 3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Cartão para armazenamento do Certificado e Leitora, com validade por 3 anos.

Para o item 3, foram encontrados os preços listados no quadro abaixo e, em seguida, adotou-se a média das três cotações, obtendo-se o preço unitário estimado no valor de **R\$ 434,00**. A média foi utilizada, uma vez que os valores são próximos entre si.

ID	DADOS DA LICITAÇÃO	VALOR
1	Descrição: e-CNPJ A3 - Cartão+Leitora Certisign Certificadora Digital S A CNPJ: 01.554.285/0001-75 Link: https://www.certisign.com.br/certificado-digital/ecnpj Data e hora de acesso: 15 de outubro de 2019, às 8h02min.	R\$ 418,00
2	Descrição: e-CNPJ A3 - Kit Leitora Serasa Experian SA CNPJ: 62.173.620/0001-80 Link: https://compra.certificadodigital.com.br/loja/#!/identificacao/e-CNPJ/0649/e-CNPJ-A3-36-MESES-CARTAO-E-LEITORA Data e hora de acesso: 15 de outubro de 2019, às 8h48min.	R\$ 515,00
3	Descrição:e-CNPJ A3 - Cartão e Leitora Companhia de Tecnologia da Informação do estado de Minas Gerais - PRODEMGE CNPJ: 16.636.540/0001-04 Link: https://wwws.prodemge.gov.br/certificados-digitais/e-cnpj Data e hora de acesso: 15 de outubro de 2019, às 8h00min.	R\$ 369,00
VALOR TOTAL		R\$ 1.302,00
VALOR UNITÁRIO MÉDIO		R\$ 434,00

Custo Total de Propriedade: Análise para o “Cenário 2 – Cartão+Leitora”			
ITEM	Valor (R\$)		
	2019	2020	TOTAL
1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.	38 unidades x R\$ 142,85 = R\$ 5.428,30	8 unidades x R\$ 142,85= R\$ 1.142,80	46 unidades x R\$ 142,85 = R\$ 6.571,10
2. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de cartão para armazenamento do Certificado e leitora, com validade por 3 anos.	43 unidades x R\$ 354,67 = R\$ 15.250,81	215 unidades x R\$ 354,67 = R\$ 76.254,05	258 unidades x R\$ 354,67 = R\$ 91.504,86
3. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de cartão para armazenamento do Certificado e leitora, com validade por 3 anos.	2 unidades x R\$ 434,00 = R\$ 868,00	2 unidades x R\$ 434,00 = R\$ 868,00	4 unidades x R\$ 434,00 = R\$ 1.736,00
TOTAL GERAL			R\$ 99.811,96

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

CERTIFICAÇÃO EM NUVEM

Essa solução precisa de rede de internet estável, tanto para o computador, quanto para o dispositivo móvel previamente autorizado. Além disso, é necessário uma verificação de segurança de pelo menos dois níveis, isto é, por meio do uso de uma senha (PIN) utilizada pelo usuário e de uma segunda validação recebida através de um aplicativo em seu dispositivo móvel. Como essa solução utilizaria bens privados dos usuários, isto é, dispositivos móveis e, até mesmo, dados móveis, uma vez que há regiões na área do campus universitário em que não há sinal de dados de internet ou este é instável, essa comissão descartou esse cenário da análise de viabilidade.

6 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

CENÁRIO/SOLUÇÃO	Estimativa (R\$)
1. Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de token criptográfico USB como	R\$ 47.573,24

dispositivo físico de armazenamento.	
2. Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento-renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de cartão como dispositivo físico de armazenamento. Acompanha leitora de cartão.	R\$ 99.811,96

6.1 - ANÁLISE COMPARATIVA DE CUSTOS

ITEM	VALOR UNITÁRIO ESTIMADO SOLUÇÃO/CENÁRIO 1	VALOR UNITÁRIO ESTIMADO SOLUÇÃO/CENÁRIO 2
1	R\$ 142,85	R\$ 142,85
2	R\$ 156,99	R\$ 354,67
3	R\$ 124,68	R\$ 434,00

COMPARATIVO DOS CUSTOS DE PROPRIEDADE (Cenários)

SOLUÇÃO 1 - Token	VALOR (R\$)	ANÁLISE
1. Emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação.	R\$ 142,85	A pesquisa de preço apontou que a emissão do certificado é a opção mais econômica quando comparada aos custos de emissão de um certificado em que seja necessário o fornecimento do dispositivo físico de armazenamento pela licitante. Provavelmente, o menor custo é explicado pela economia obtida com o token criptográfico já existente.
2. Emissão de certificados digitais do tipo A3, e-CPF, com fornecimento de Token USB como dispositivo físico de armazenamento.	R\$ 156,99	O certificado armazenado em token é a opção mais utilizada pela administração pública federal, tendo em vista que a pesquisa no painel de preço retornou apenas essa opção. Dispensa a utilização de interface de leitura, tornando-se, portanto, uma opção mais prática.
3. Emissão de certificados digitais do tipo A3, e-CNPJ, com fornecimento de Token USB como dispositivo físico de armazenamento.	R\$ 124,68	O certificado armazenado em token é a opção mais utilizada pela administração pública federal, tendo em vista que a pesquisa no painel de preço retornou apenas essa opção. Dispensa a utilização de interface de leitura, tornando-se, portanto, uma opção mais prática.

SOLUÇÃO 2 - Cartão + Leitora	VALOR (RS)	ANÁLISE
1. Emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação.	R\$ 142,85	A pesquisa de preço apontou que a emissão do certificado é a opção mais econômica quando comparada aos custos de emissão de um certificado em que seja necessário o fornecimento do dispositivo físico de armazenamento pela licitante. Provavelmente, o menor custo é explicado pela economia obtida com o token criptográfico já existente.
2. Emissão de certificados digitais do tipo A3, e-CPF, com fornecimento de cartão como dispositivo físico de armazenamento. Acompanha leitora de cartão.	R\$ 354,67	O certificado armazenado em cartão não é a opção mais utilizada na administração pública. Necessita de uma leitora de cartão para ser utilizado, o que pode explicar sua queda na preferência quando comparado a solução que utiliza o token. A pesquisa de preço apontou um valor estimado superior ao do dispositivo armazenado em token criptográfico.
3. Emissão de certificados digitais do tipo A3, e-CNPJ, com fornecimento de cartão como dispositivo físico de armazenamento. Acompanha leitora de cartão.	R\$ 434,00	O certificado armazenado em cartão não é a opção mais utilizada na administração pública. Necessita de uma leitora de cartão para ser utilizado, fato que pode explicar sua queda na preferência quando comparado a solução que utiliza o <i>token</i> . A pesquisa de preço apontou um valor estimado superior ao do dispositivo armazenado em token criptográfico.

Serviços que Compõem a Solução			
Serviço	Quantitativo 2019 e 2020	Valor unitário estimado	Valor total estimado
1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.	46	R\$ 142,85	R\$ 6.571,10
2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	258	R\$ 156,99	R\$ 40.503,42

3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do Certificado, com validade por 3 anos.	4	R\$ 124,68	R\$ 498,72
CUSTO TOTAL ESTIMADO			R\$ 47.573,24

7 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Cenário	1	Descrição	Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de <i>token criptográfico</i> USB como dispositivo físico de armazenamento.
Serviços que Compõem a Solução			
Serviço			Estimativa
1. Emissão de Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - Renovação, com validade por 3 anos.			46 unidades x R\$ 142,85
Total			R\$ 6.571,10
2. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de <i>Token</i> criptográfico para armazenamento do Certificado, com validade por 3 anos.			258 unidades x R\$ 156,99
Total do item			R\$ 40.503,42
3. Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de <i>Token</i> criptográfico para armazenamento do Certificado, com validade por 3 anos.			4 unidades x R\$ 124,68
Total do item			R\$ 498,72
ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO			
R\$ 47.573,24			
Alinhamento em Relação às Necessidades de Negócio e Macro Requisitos Tecnológicos			
A contratação dos serviços está alinhada com a Necessidade 97 do PDTIC 2017-2020 (Serviços de emissão de certificados digitais padrão ICP-Brasil).			
Justificativa para o Parcelamento da Solução			
A solução mostra-se técnica e economicamente viável para o parcelamento em 3 itens, independentes entre si, conforme quadro do item 3.3. Desta forma, haverá melhor aproveitamento do mercado e ampliação da competitividade.			

8 – NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE INTERNO PARA EXECUÇÃO CONTRATUAL

Devido à forma de execução do serviço a ser contratado, não será necessário adequar o ambiente interno para contratação da solução em questão, pois os serviços não serão prestados nas dependências da Contratante.

9 – RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

Recurso Material

Não se aplica, pois o serviço será prestado pela Contratada em seu posto de atendimento, na cidade de Lavras. É responsabilidade exclusiva da Contratada a disponibilização de estrutura física, recursos materiais e recursos humanos necessários para a prestação do serviço. Portanto, **não há qualquer recurso material da Contratante envolvido.**

Quantidade	Não se aplica.	Disponibilidade	Não se aplica.
Ações para Obtenção do Recurso		Não se aplica.	
Responsáveis pela Obtenção do Recurso		Não se aplica.	

Recursos Humanos

Não se aplica, pois a empresa será responsável por disponibilizar todos os recursos humanos necessários para a prestação do serviço. Portanto, **não há qualquer recurso humano da Contratante envolvido.**

Formação	Não se aplica.
Atribuições	Não se aplica.

10 – DECLARAÇÃO DE VIABILIDADE

Com base nos elementos anteriores do presente documento de Estudos Preliminares realizado por esta Equipe de Planejamento, DECLARAMOS que:

É VIÁVEL a contratação proposta pela unidade requisitante.

NÃO É VIÁVEL a contratação proposta pela unidade requisitante.

A Equipe de Planejamento identificada abaixo chegou à conclusão acima em razão do(s) seguinte(s) motivo(s):

A solução possibilitará o acesso dos servidores da Instituição aos sistemas do governo federal que permitem o bom funcionamento das atividades institucionais. Em termo de economicidade, no caso do Item 1, o custo para a emissão/renovação do certificado digital, tendo o dispositivo físico

de armazenamento já existente é mais vantajoso do que o custo de emissão de um certificado em que é necessário que a empresa forneça o token criptográfico.

Ressalta-se que os certificados digitais armazenados em cartões e token realizam exatamente as mesmas operações e possuem as mesmas funcionalidades, o que muda é apenas a praticidade no uso de cada um deles. A principal diferença entre o *token* e o cartão é que o token não precisa da utilização de uma leitora, pois se conecta diretamente à porta USB, padrão existente em qualquer computador. Já o cartão precisa de um dispositivo leitor de cartões USB para ser utilizado. Essa característica faz com que exista uma tendência de preferência pelo armazenamento em *Token* USB.

Considerando a pesquisa de preço, optou-se por escolher o Cenário 1, cuja Solução é a “Licitação para serviços de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação e de emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, com fornecimento de token criptográfico USB como dispositivo físico de armazenamento”, uma vez que foram obtidos preços de referência, para todos os itens, inferiores àqueles obtidos tendo cartão com leitora como dispositivo físico de armazenamento. Ressalta-se ainda que o certificado armazenado em *token* possui maior praticidade quando comparado ao cartão, pois não necessita de interface de leitura. Além disso, o público usuário já está adaptado a esse tipo de solução que é a utilizada na instituição atualmente.

Vale destacar que a escolha pelo *token* criptográfico como o dispositivo físico de armazenado a ser disponibilizado pelos licitantes não limita a competitividade, uma vez que, segundo pesquisas de mercado, as empresas ofertam tanto o *token* como o cartão.

Equipe de Planejamento: Clayton Ferreira Santos, Bruno da Silva Gonçalves e Miriam Rosa Silva

11 – DO ACESSO ÀS INFORMAÇÕES CONTIDAS NOS PRESENTES ESTUDOS PRELIMINARES:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que:

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | As informações contidas nos presentes Estudos Preliminares DEVERÃO ESTAR DISPONÍVEIS para qualquer interessado, pois não se caracterizam como sigilosas. |
| <input type="checkbox"/> | As informações contidas nos presentes Estudos Preliminares ASSUMEM CARÁTER SIGILOSO, nos termos do Art. 23 da Lei nº 12.527/2011, e, portanto, deverão ter acesso restrito. |

12 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria PROPLAG nº38, de 01 de março de 2019.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC.

Integrante Técnico

Nome: Clayton Ferreira Santos

Matrícula/SIAPE: 1311618

Integrante Técnico

Lavras, 16 de outubro de 2019.

Integrante Requisitante

Nome: Miriam Rosa Silva

Matrícula/SIAPE: 1889156

Integrante Requisitante

Lavras, 16 de outubro de 2019.

Autoridade Competente

Nome: Erasmo Evangelista de Oliveira

Matrícula/SIAPE: 01307332

Autoridade Máxima da Área de TIC

Lavras, 16 de outubro de 2019.