Anexo IV do Edital

ESTUDO TÉCNICO PRELIMINAR 92/2020

1. INFORMAÇÕES BÁSICAS

Número do processo: 23090.021643/2020-82

2. DESCRIÇÃO DA NECESSIDADE

Contratação de Certificados Digitais e-CPF e e-CNPJ

Contratação de empresa especializada na prestação de serviços de emissão de certificados digitais do tipo A3 e Token Criptográfico (dispositivos eletrônicos geradores de senhas temporárias). Esses serviços são: a renovação e emissão de certificados digitais do tipo A3, e-CPF, padrão ICP-Brasil, com validade de 36 meses e sem fornecimento do Token Criptográfico; e a emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, padrão ICP-Brasil, com fornecimento de Token criptográfico, com validade de 36 meses.

Os certificados digitais e Tokens são necessários para atender a ação “Uso de Recursos Criptográficos em Segurança da Informação e Comunicações” da meta 101 do PDTIC 2017-2020 (Criar e revisar as normas de Segurança da Informação da UFLA). Essa meta está alinhada à demanda “Melhoria da segurança da informação e comunicação da UFLA em conformidade com as legislações vigentes”, incluída como a “Necessidade 90” do “Plano de Tecnologia da Informação e Comunicação 2017-2020” (PDTIC 2017-2020).

3. ÁREA REQUISITANTE

Área requisitante	Responsável
Diretoria de Gestão de Tecnologia da Informação	Erasmo Evangelista de Oliveira

4. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

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: COMPRASNET.
5	Autenticação por meio de certificado digital no sistema: WORKFLOW - TERMO DE OUTORGA.
6	Autenticação por meio de certificado digital no sistema da Receita Federal do Brasil.
Identificação das necessidades tecnológicas	
1	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 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 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 Economia, do Planejamento 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, ComprasNet, Receita Federal). 1.8. Os certificados digitais deverão ser compatíveis com os tokens modelo: Token StarSign USB – G&D Burti, StarSign Crypto – USB-Token S, SafeNet iKey 2032 e SafeNet Token 5100/5110, já existentes na UFLA.
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. 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 123 do Comitê

Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017).
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 Economia, do Planejamento 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, 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 de emissão 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, 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 token criptográfico.
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, através 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.
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. 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 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 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-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, da Economia, 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 ICPBrasil 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 de emissão 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 ICPBrasil. 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.
3.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).
3.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).
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).
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.
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.
3.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.
3.2.18. Possuir indicador luminoso de estado do dispositivo.
3.2.19. Assinar dados digitalmente em até 10 (dez) segundos.
3.2.20. O token criptográfico deverá possuir certificação do INMETRO.
3.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura.
3.3. Funcionalidades
3.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.
3.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label).
3.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.
3.3.4. Permitir criação de senhas com caracteres alfanuméricos.
3.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.
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.
3.3.7. 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.
3.3.8. Permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key).

	3.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). 3.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. 3.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores). 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. 3.3.13. Implementar mecanismo de autenticação tipo challenge-response. 3.3.14. Forçar a troca da senha padrão no primeiro acesso. 3.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos. 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. 3.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. 3.4. Software 3.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita: 3.4.1.1. gerenciamento do dispositivo; 3.4.1.2. exportação de certificados armazenados no dispositivo; 3.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; 3.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; 3.4.1.5. visualização de certificados armazenados no dispositivo; 3.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; 3.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso. 3.4.2. Deverá ser disponibilizado portal para download de drivers/Softwares de forma ilimitada e gratuita. 3.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.
Demais requisitos necessários e suficientes à escolha da solução de TIC	
1	O serviço de certificação presencial e validação de documentos de cada certificado deverão ser prestados 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. 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. Em hipótese alguma os servidores da Contratante se deslocarão para outra cidade para obter o serviço. Tal exigência visa à 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, ainda que a empresa custeie as referidas despesas.

2 A Contratante comunicará à Contratada, via e-mail a ser designado para esse fim, identificação de servidores autorizados a receber certificados digitais. Essa forma de comunicação poderá ser substituída, caso a Contratada possua sistema próprio de abertura de chamados que permita à UFLA enviar os nomes de tais servidores.

3 A Contratada deverá disponibilizar um canal de comunicação (telefone, e-mail ou sistema de abertura de chamados) para 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.

4 A Contratada deverá disponibilizar, via telefone, e-mail ou sistema de abertura de chamados, uma data e um horário para a validação presencial em seu posto de atendimento.

5 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, e-mail ou sistema de abertura de chamados, os horários a serem disponibilizados pela empresa também deverão ser, pelo menos, os supracitados.

6 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 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 consequências.

8 A Contratada deverá realizar a validação presencial para emissão dos certificados em, no máximo, 7 (sete) dias úteis após o contato para agendamento pelo servidor da UFLA.

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:
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 Os requisitos de sustentabilidade ambiental não se aplicam à esta contratação. No entanto, em relação à especificação dos dispositivo físico de armazenamento a serem licitados, existem pré-requisitos de que os mesmos sejam certificados pelo INMETRO.

5. LEVANTAMENTO DE MERCADO

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 demanda.

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.

É importante destacar que será utilizado o mesmo valor médio estimado para o ITEM 1 na composição dos dois cenários, uma vez que ele é o mesmo item para os dois cenários, por se tratar de renovação.

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.

IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	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.
2	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, acompanhado de leitora de cartão.

REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS - Solução Certificado em Nuvem - Essa solução precisa de rede de internet estável, tanto para o computador, quanto para o dispositivo móvel previamente autorizado. Além disso, é necessária 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. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução 1 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 token USB, 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.

A solução 2 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 venha acompanhada de uma leitora de smart cards, que se trata do equipamento responsável por fazer a gravação e a leitura dos certificados digitais que ficam armazenados dentro dos smart cards. 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.

Os certificados digitais armazenados em cartão e em token USB 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 USB e o cartão é que o token USB 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.

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

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

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.

Foi realizado o levantamento da demanda de certificado digital, com e sem dispositivo de armazenamento, com os servidores docentes e técnico-administrativos da UFLA, do dia 29 de julho

de 2020 ao dia 10 de agosto de 2020, por meio de questionário eletrônico. O levantamento de demanda foi divulgado por meio de e-mail institucional e também no sítio eletrônico da UFLA. Foram identificadas **20** demandas para renovação de certificados com validade até o fim de 2021. O levantamento também apontou a necessidade de emissão de **79** novos certificados digitais e-CPF, com fornecimento de dispositivos físicos de armazenamento. Foi identificada também a necessidade de emissão de **2** novos certificados digitais e-CNPJ, com fornecimento de dispositivos físicos de armazenamento. Essa previsão para emissão dos certificados digitais e-CNPJ é uma estratégia de segurança para reposição, caso ocorra alguma perda ou dano com os certificados digitais e-CNPJ utilizados atualmente na instituição.

LEVANTAMENTO DE NECESSIDADE DE CERTIFICAÇÃO DIGITAL 2021		
UNIDADE ORGANIZACIONAL	**NOVOS TOKENS**	**RENOVAÇÃO DE TOKENS**
AUDITORIA INTERNA	0	0
ECA	2	2
EDITORA	1	0
ESCOLA DE ENGENHARIA	9	2
FCA	2	0
FCHEL	4	1
FCS	5	0
FCSA	2	0
FELCH	0	0
ICE	10	1
ICN	12	0
PÓS-GRADUAÇÃO	20	4
PRAEC	1	0
PRGDP	2	4
PROEC	0	1
PROGRAD	4	1
PROPLAG	5	1
PRP	0	1
PRPG	0	1
SECAD	0	1
TOTAL	**79**	**20**

Uma vez que a contratação vigente se encerrará em 8 de novembro de 2020, não sendo assim possível atender toda a demanda supracitada, 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.

ESTIMATIVA DE NECESSIDADE DE CERTIFICAÇÃO DIGITAL	
ITEM	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.	20
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.	79
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

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

A estimativa do valor da contratação e o cálculo do Custo Total de Propriedade, incluindo os dados e as memórias de cálculo para cada item encontram-se no Anexo I deste Estudo Técnico Preliminar (19.1.1 - Pesquisa de preços Tokens.pdf).

8.1 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução 1 - Token

Custo Total de Propriedade – Memória de Cálculo

Item	Descrição do Serviço	Quant	Valor Unitário Médio 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.	20	R$ 142,00	R$ 2.840,00
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.	79	R$ 330,55	R$ 26.113,45
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	R$ 325,00	R$ 650,00
Total Estimado Geral				**R$ 29.603,45**

Solução 2 - Cartão + Leitora

Custo Total de Propriedade – Memória de Cálculo

Item	Descrição do Serviço	Quant	Valor Unitário Médio 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.	20	R$ 142,00	R$ 2.840,00
2	Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de cartão criptográfico e leitor para armazenamento do Certificado, com validade por 3 anos.	79	R$ 381,00	R$ 30.099,00
3	Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de cartão criptográfico e leitor para armazenamento do Certificado, com validade por 3 anos.	2	R$ 474,33	R$ 948,66

Total Estimado Geral	**R$ 33.887,66**

8.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	2020	2021	2022	
Solução 1 - Token USB	R$ 29.603,45	-	-	R$ 29.603,45
Solução 2 - Cartão + Leitora	R$ 33.887,66	-	-	R$ 33.887,66

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A solução mostra-se técnica e economicamente viável para o parcelamento em 3 itens, independentes entre si. Desta forma, haverá melhor aproveitamento do mercado e ampliação da competitividade.

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, optou-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.

10. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não possui dependências.

11. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica. Objetivo da Estratégia de Governo Digital 2020 - 2022 (Revogou a Política de Governança Digital, instituída pelo Decreto nº 8.638, de 15 de janeiro de 2016).
Objetivo 15.4	Aprimorar a Segurança da Informação e Comunicação, por meio da governança dos riscos de TIC. Objetivo estratégico do Plano de Desenvolvimento Institucional (PDI) 2016 - 2020 da UFLA (Planejamento Estratégico Institucional).

ALINHAMENTO AO PDTIC 2017 - 2020			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A.90.101	6) Criação das Normas de Uso dos Recursos Criptográficos em Segurança da Informação e Comunicações	M.101	Criar e revisar as normas de Segurança da Informação da UFLA
A.97.134	1) Planejamento da contratação 2) Licitação	M.134	Contratar serviços de emissão de certificados digitais do tipo A3, eCPF e eCNPJ, padrão ICP-Brasil, com e sem fornecimento de dispositivo físico de armazenamento.

ALINHAMENTO AO PAC 2020 e 2021	
Item	**Descrição**
4246	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA (PAC 2020)
10	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA (PAC 2021)
4530	EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA (PAC 2020)
11	EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA (PAC 2021)
4531	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURIDICA (PAC 2020)

Entende-se que o objeto em questão não se trata de oferta digital de serviços públicos, sendo assim, não é necessário integração à Plataforma de Cidadania Digital, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016.

12. DESCRIÇÃO DA SOLUÇÃO A SER CONTRATADA

Cenário	Descrição
Solução 1	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.

A Solução 1 (Token) é a que apresentou maior vantajosidade econômica, segundo a Pesquisa de Preços realizada, em relação à Solução 2 (Cartão + Leitora). Além disto, o certificado armazenado em token dispensa a utilização de interface de leitura, tornando-se, portanto, uma opção mais prática. Bem como, o público usuário já está adaptado a esse tipo de solução que é a utilizada na instituição atualmente.

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 0006/2020 que os preços ofertados pelas licitantes foram inferiores àqueles que constam no site de empresa pública.

13. RESULTADOS PRETENDIDOS

Acesso aos sistemas da administração pública federal – Os sistemas estruturantes da administração pública federal exigem o certificado digital dos servidores que possuem função de gestor. Sem o certificado digital não é possível ter o acesso de gestor.

Aumentar a segurança da informação e comunicação – A geração da chave de criptografia, do certificado digital do tipo A3, oferece mais segurança para acessar os sistemas de informação. No certificado digital A3, a geração da chave é feita em um hardware separado, o que faz com que haja mais proteção dos dados.

14. PROVIDÊNCIAS A SEREM ADOTADAS

Não se aplica.

15. POSSÍVEIS IMPACTOS AMBIENTAIS

Não se aplica.

16. DECLARAÇÃO DE VIABILIDADE

Esta equipe de planejamento declara **viável** esta contratação com base neste Estudo Técnico Preliminar.

16.1. Justificativa da Viabilidade

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 a Solução 1, cuja descrição é “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 armazenamento 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.

17. RESPONSÁVEIS

FERNANDO ELIAS DE OLIVEIRA
Integrante Requisitante

PLÍNIO MÁRCIO BRAGA TORRES
Integrante Técnico

ERASMO EVANGELISTA DE OLIVEIRA
Autoridade máxima da área de TIC

LUIZ PAULO BRIANEZI VALIM
Autoridade Competente

Lista de Anexos

Atenção: alguns arquivos digitais enumerados abaixo podem ter sido anexados mesmo sem poderem ser impressos.

- Anexo I - 19.1.1 - Pesquisa de preços Tokens.pdf (1.36 MB)