Estudo Técnico Preliminar 7/2024

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

2.1 Contratação de serviço de certificação digital e-CPF dentro das especificações e normas ICP-Brasil

2.2 O certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em uma rede de computadores. O processo de certificação digital utiliza procedimentos lógicos e matemáticos para assegurar confidencialidade, integridade das informações e confirmação de autoria.

2.3. Todas as transações eletrônicas assinadas digitalmente têm validade jurídica garantida pela Medida Provisória n° 2.200/01 que institui a ICP-Brasil para a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica e das aplicações que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

2.4. A utilização da certificação digital busca garantir a segurança necessária para a virtualização de procedimentos que hoje são feitos de forma presencial, como a assinatura de documentos, além de simplificar os procedimentos, reduzir a burocracia, possibilitar a diminuição de custos e celeridade processual.

2.5 Os certificados serão utilizados pelos servidores da UFMG para emissão do diploma digital, e acesso aos diversos sistemas estruturantes da Administração Pública Federal, que exigem a certificação digital para determinados perfis (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, entre outros), garantindo os princípios de segurança da informação (autenticidade, confidencialidade e integridade) dos atos públicos da Administração.

3. Área requisitante

Área Requisitante	Responsável
DTI/DPS- DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO /DIVISÃO DE PROCESSOS E SEGURANÇA	SADALLO ANDERE NETO

4. Necessidades de Negócio

4.1 Permitir o acesso a todos os sistemas estruturantes da administração pública federal que exijam certificado digital para acesso.

4.2 Ser utilizado nos serviços eletrônicos dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Economia, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios dentre outras instituições.

4.2 Ser emitido em todas as capitais brasileiras.

4.3 Ter validade de 3 (três) anos e fornecer assistência técnica compatível com a solução contratada.

5. Necessidades Tecnológicas

5.1. Certificado emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil;

5.2 Conter nível A3;

5.3 A solução deverá ser compatível com os sistemas operacionais de computadores desktops, notebooks e dispositivos móveis.

5.3.1 Permitir gerenciar os dispositivos autorizados e assinar digitalmente documentos por meio de celular ou tablet utilizando sistema operacional Android ou iOS;

5.3.2 Ser compatível com os sistemas operacionais Linux, Windows 7, Windows 10 e superiores;

5.3.3 Possuir compatibilidade com os navegadores WEB: Microsoft Edge, Mozilla Firefox e Google Chrome;

5.4 Ser protegido por senha;

5.6 O processo de emissão do certificado nas autoridades de registro deverá estar em conformidade com as orientações do Instituto Nacional de Tecnologia da Informação - ITI, quanto aos procedimentos e documentos exigidos.

5.7 Gerar apenas um certificado e permitir a utilização em múltiplos dispositivos móveis a escolha do usuário.

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

Requisitos de Capacitação, Ambientais, Culturais e Sociais

1. A solução deverá prover de manual de operações em língua portuguesa, contendo linguagem clara objetiva, preferencialmente em formato eletrônico;
2. As mensagens e avisos emitidos pela solução deverão ser em língua portuguesa;
3. Observar no que couber o disposto na IN SLTI/MP nº 1, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional
4. Os produtos devem ser acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento e permita o descarte sustentável;
5. Cabe exclusivamente à Contratada remover às suas expensas todo o material que for constatado dano em decorrência de transporte ou acondicionamento, providenciando a substituição do mesmo, assim como o descarte sustentável dos resíduos. Conforme previsto no inciso IV do artigo 5º da Instrução Normativa nº 1, de 19/01/2010-SLTI/MPOG, os equipamentos ofertados não deverão conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs);
6. Observar os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares; Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.
7. A CONTRATADA deverá obedecer às normas técnicas, de saúde, de higiene, conforto e de segurança do trabalho, de acordo com as normas do Ministério do Trabalho e Emprego. Deverá prever soluções inovadoras na prestação de serviços de excelência, que resultem em sustentabilidade e eficiência.
8. Comprovar e manter durante toda a vigência do contrato, sob pena de rescisão contratual, as seguintes condições:
9. Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pelo Ministério do Trabalho e Emprego, por meio da Portaria nº 540/2004.
10. Não ter sido condenada, a CONTRATADA ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro;
11. Adotar boas práticas de otimização de recursos/redução de desperdícios/menor poluição, como: - Racionalização do uso de substância potencialmente tóxicas/poluentes. - Substituição de substâncias tóxicas por outras atóxicas ou de menor toxicidade. - Racionalização/economia no consumo de energia, especialmente elétrica, água e papel. - Treinamento

/capacitação periódicos dos empregados sobre boas práticas de redução de desperdícios/poluição. - Reciclagem /destinação adequada de resíduos gerados na prestação de serviços.
12. A vigência do Contrato será de 24 (vinte e quatro meses) meses, podendo ser prorrogado por interesse da Contratante.
13. A licitante deverá ter pleno conhecimento das condições necessárias para a prestação do serviço.

Requisitos Legais

1. A presente contratação deverá observar as seguintes leis e normas:
2. Medida Provisória 2.200-2, de 24.08.2001, que criou o sistema nacional de Certificação Digital da ICP-Brasil e que regulamentou a utilização dos documentos eletrônicos no Brasil, criando a ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira, sistema que administra e gerencia a emissão de certificados digitais no país. A ICP-Brasil é mantida pelo ITI Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Presidência da República.
3. Decreto nº 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.
4. Portaria nº 330, de 06 de abril de 2018 do Ministério da Educação, que regulamentou a emissão de diplomas digitais nas Instituições de Ensino Superior pertencentes ao sistema federal de ensino.
5. Lei nº 14.133, de 1º de abril de 2021, estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.
6. Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;
7. Decreto nº 9.637,de 26 de dezembro de 2018: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, dispõe sobre a governança da segurança da informação;
8. Decreto nº 7.174/2010: regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
9. Decreto n° 7.579/2011:dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo Federal;
10. Decreto nº 11.129, de 11 de julho de 2022: Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.
11. Instrução Normativa SLTI/MP nº 05, de 27 de junho de 2014: dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral e suas alterações;
12. Instrução Normativa SEGES/MP n° 05, de 26 de maio de 2017: dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;
13. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
14. Instrução Normativa nº 6, de 11 de agosto de 2017 do Instituto Nacional de Tecnologia da Informação – ITI que dispôs sobre a validação de solicitação de certificados para servidores públicos da ativa e militar da união.
15. Medida Provisória 2.200-2, de 24.08.2001, que criou o sistema nacional de Certificação Digital da ICP-Brasil e que regulamentou a utilização dos documentos eletrônicos no Brasil, criando a ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira, sistema que administra e gerencia a emissão de certificados digitais no país. A ICP-Brasil é mantida pelo ITI Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Presidência da República.
16. **Requisitos Temporais**
17. O certificado deverá possuir validade de 3 (três) anos, contados a partir da data de sua emissão.
18. **Requisitos de Manutenção e Garantia**
19. O prazo de garantia de correção e atualização do objeto, motivadas por falhas técnicas e mudanças originadas de diretrizes ICP-Brasil, é de 36 (trinta e seis) meses, contado da data de recebimento dos certificados pela CONTRATANTE.
20. A CONTRATADA deverá manter central de atendimento para a abertura de chamados pelo menos no horário das 08h00min às 18h00min, de segunda a sexta-feira, exceto feriados;
21. A central deverá ser acionada por telefone ou pela internet.

7. Estimativa da demanda - quantidade de bens e serviços

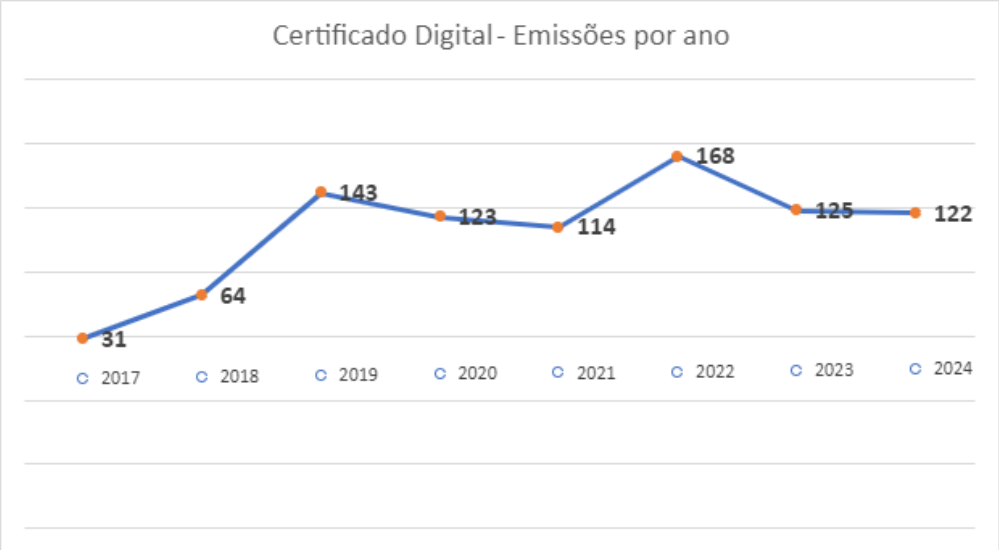
O certificado digital é destinado apenas aos servidores da UFMG cujas tarefas em sistemas de informação exijam tal mecanismo de segurança para autenticação.

Segundo o Portal da Transparência, em consulta realizada em 5 de junho de 2024, a Universidade Federal de Minas Gerais possui com 9.018 (nove mil e dezoito) servidores ativos.

Atualmente, 481 servidores da UFMG possuem certificado digital válido em uso para executar as tarefas típicas do cargo cuja utilização é fundamental para o adequado funcionamento da universidade, resultando em 5,34% dos servidores da UFMG com certificação digital custeada pela universidade.

Como descrito a seguir, há uma tendência de aumento deste quantitativo em decorrência der exigências dos próprios sistemas estruturantes da APF que, visando aumentar a segurança e mitigar riscos relacionados à segurança da informação, têm exigindo uso de certificado digital para acesso à sistemas e execução de tarefas para os quais o certificado não era exigido anteriormente.

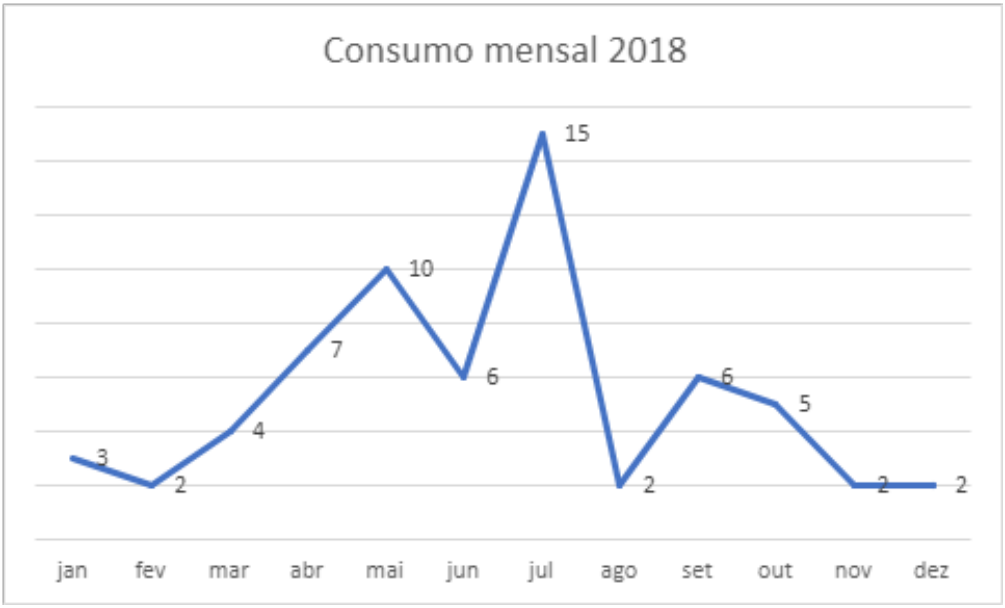
A seguir, detalha-se o padrão de consumo de certificados digitais na UFMG entre outubro de 2017 e maio de 2024.



Período de análise: out/2017-maio/2024 Fonte: Relatórios técnicos fornecidos pelas contratadas

Pode-se perceber a partir do gráfico anterior a tendência crescente no consumo de certificado digital para o ano de 2024, visto que, apenas nos primeiros cinco meses houve um consumo similar ao consumo total do ano de 2023.

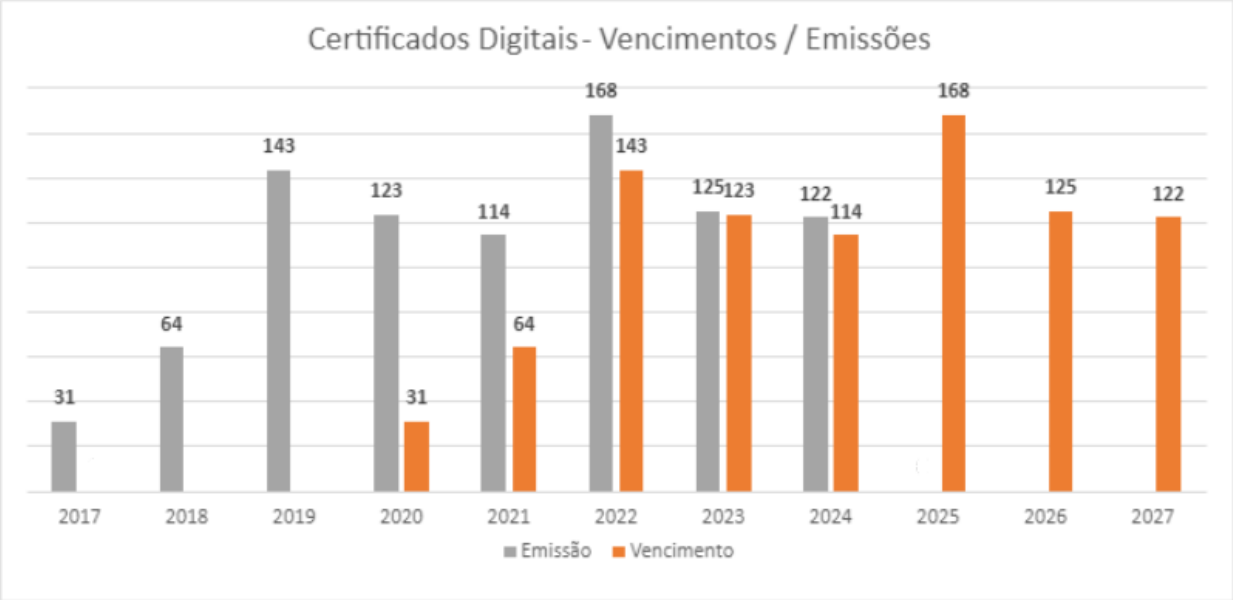
Além disso, no período de vigência previsto para o novo contrato ocorrerão eleições para a Reitoria da UFMG. Historicamente, há um aumento no consumo de certificados digitais nos meses que sucedem a posse da nova equipe de gestão, conforme ilustrado no gráfico abaixo:



Fonte: Relatórios técnicos fornecidos pelas contratadas

A nomeação ocorreu no final de março de 2018 e o gráfico evidencia um aumento considerável no consumo de certificados digitais nos meses subsequentes à nomeação.

Considerando que os certificados digitais emitidos possuem uma validade de 3 (três) anos, no gráfico a seguir, mostra-se a correlação entre os certificados vencidos e o número de emissões anuais.

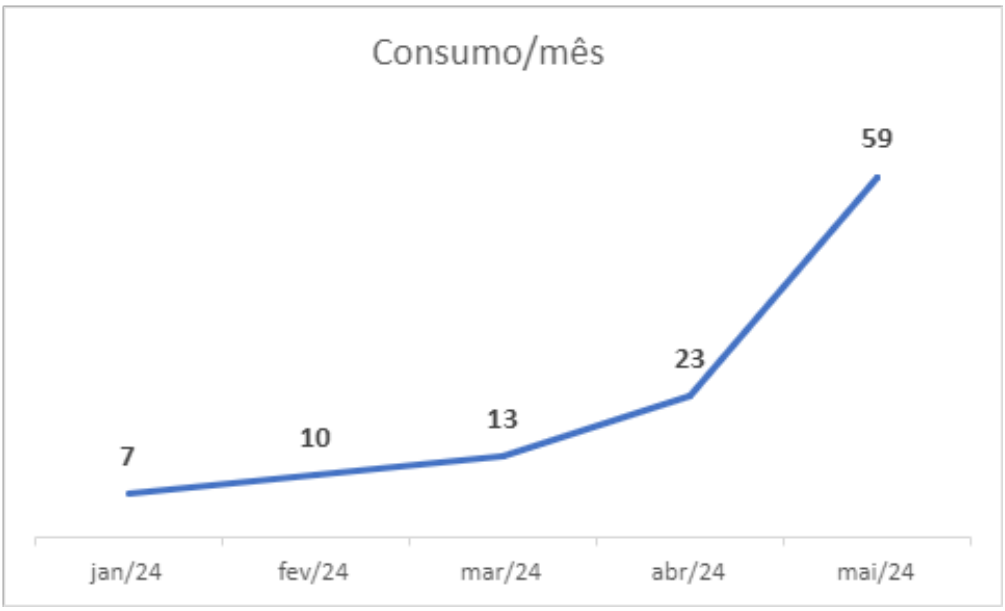


Fonte: Relatórios técnicos fornecidos pelas contratadas

No período de 2020-2023, a emissão de novos certificados sofreu um aumento médio de 42 unidades por ano.

Ainda de acordo com o gráfico acima, o vencimento de certificados digitais nos próximos 2 anos (2025-2026) totalizará 293 certificados. Seguindo a tendência da média de aumento auferida nos anos anteriores, teria-se um gasto de aproximadamente 378 certificados, considerando o consumo normal no período.

No entanto, no ano de 2024, modificações nos requisitos de segurança da informação do Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) acarretaram em consumo incomum de certificados digitais, conforme ilustrado no gráfico seguinte.



Fonte: Relatórios técnicos fornecidos pela contratada

O consumo total do mês de maio/2024 corresponde a um aumento de 156% com relação ao mês anterior, contribuindo para um aumento significativo na média total do ano calculada até o momento. A projeção é que em 2024 ocorra um consumo de 268 certificados até o fim do ano.

Considerando à troca de gestão da Reitoria da UFMG que ocorrerá dentro da vigência prevista para o contrato;

Considerando a tendência crescente de exigência de uso de certificados digitais nos sistemas estruturantes da APF e um consumo que praticamente duplicou em abr/24 quando comparado a mar/2024, e que quase triplicou em mai/2024 com relação a abr/2024;

Considerando que os níveis de segurança exigidos pelo governo federal para acesso aos sistemas estruturantes aumentaram significativamente e cada vez mais sistemas exigem o uso de certificado digital;

Considerando que o risco de interrupção do serviço de emissão de novos certificados e renovação dos existentes, comprometeria o funcionamento da universidade, e adotando uma margem de segurança estima-se a necessidade de contratação de 800 (oitocentos) certificados digitais para o presente contrato.

8. Levantamento de soluções

Certificado digital A3 com armazenamento em mídias criptografadas

O Certificado digital A3 é emitido e armazenado em um objeto físico. São fabricados em diversos formatos de mídia, que determinam sua forma de utilização. São eles:

- Token: artefato USB, semelhante a um pendrive;
- Smartcard: cartão plástico com chip, lido através de hardware específico.

O prazo de validade do certificado digital A3 varia entre 1 ano e 3 anos a partir da data de emissão.

Vantagens

- Segurança, pois não pode ser transferido ou copiado para outros equipamentos além da mídia original;
- Geralmente, um único certificado A3 com duração de 3 anos fica mais barato do que 3 certificados A1 com duração de 1 ano.

Desvantagens

- Pode ser perdido, roubado ou danificado fisicamente, acarretando em perda do certificado;
- Só pode ser utilizado em um computador ou dispositivo móvel por vez;
- Requer periférico de leitura no caso de smartcards.
- Obsolescência tecnológica - O token USB adquirido pode não ser reutilizável no momento do vencimento e renovação do certificado por não ser mais compatível com o novo certificado a ser instalado.
- Maior dificuldade de assistência técnica por haver diversos modelos de token USB em uso na universidade, cada modelo com suas especificidades e manuais de operação distintos.
- O bloqueio do dispositivo em caso de excesso de tentativa de senhas (principal e de administração) inutiliza o certificado digital.

Certificado Digital A3 em nuvem

O certificado digital em nuvem é salvo diretamente em ambiente virtual, permitindo o acesso de qualquer dispositivo (celular, tablet, notebook, desktop) e em qualquer local, bastando que o usuário tenha os dados de acesso para usá-lo.

Vantagens do certificado em nuvem

- Este tipo de certificado é extremamente seguro por ser salvo em um servidor Hardware Security Module (HSM), o mesmo tipo de equipamento usado pelas Autoridades Certificadoras (AC).
- O modelo de certificado em nuvem elimina os custos com leitoras de cartão ou tokens e diminui a necessidade de suporte por parte das equipes de assistência técnica de T.I.

Desvantagens

- É necessário ter conexão à internet para realizar as operações.

9. Análise comparativa de soluções

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-94 de 23 de dezembro de 2022/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

Tradicionalmente um certificado digital pode ser instalado em um smartcard ou em um token criptográfico que estão sujeitos a danos físicos, perdas, roubos e bloqueios lógicos que podem inviabilizar sua utilização. Uma forma de evitar esses problemas é a utilização de certificados digitais na nuvem. Os certificados digitais em nuvem geralmente ficam armazenados nos servidores de alta segurança HSM (Hardware Security Module) dos prestadores de serviço e podem ser acessíveis de qualquer localidade, possibilitando a assinatura de documentos à distância por meio de celulares e tablets e aumentando a mobilidade dos usuários dos certificados digitais.

O cenário adotado pela UFMG no momento é um modelo híbrido com fornecimento de certificados digitais em nuvem e a utilização de Certificados digitais com fornecimento de token criptográfico para armazenamento do certificado, ambos com validade de 3 anos.

As desvantagens observadas na utilização do token criptográfico são desgaste natural pelo uso, extravio, perda, token danificado, esquecimento e incompatibilidade de hardware e software em caso de renovações. No momento da finalização do contrato e eventual mudança da empresa contratada, esta pode não dar suporte ao token já existente e ser necessário adquirir um novo token.

Há iniciativas do governo federal que visam estimular a utilização de soluções em nuvem. A estratégia brasileira para a Transformação Digital (E-Digital) 2022-2026 enumera como objetivo específico: "Adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal;" O certificado digital em nuvem proporciona ganho em eficiência por apresentar uma melhor praticidade e mobilidade em relação ao token. Pode ser instalado em notebooks, computadores e dispositivos móveis. Conta com a possibilidade de gerenciamento de dispositivos, podendo ser adicionados ou excluídos dispositivos de acordo com a necessidade. Há que se considerar também o crescente uso de smartphones para novas funções e serviços oferecidos pelo governo nas plataformas digitais. A utilização de certificação digital em nuvem, inclui benefícios que vão desde a praticidade e economia, passando por agilidade e segurança, já que o usuário tem controle sobre a utilização de sua chave, não precisa carregar o dispositivo token, e a assinatura poder ser realizada a partir do próprio celular. Uma das possíveis desvantagens do uso do certificado digital em nuvem é que ele utiliza proteção em dois fatores, ou seja, é necessário a utilização de um dispositivo móvel (smartphone ou tablet) com acesso a internet para utilização do certificado, no entanto, este tipo de autenticação garante um aumento significativo da segurança, o que descaracteriza a exigência como desvantagem.

Até o ano de 2023, a UFMG fornecia unicamente certificado digital com armazenado em token criptografado. A partir de abril de 2023 foi iniciado o fornecimento híbrido: armazenamento em token e nuvem, à escolha do usuário. Já havia sido identificada a solução em nuvem como a mais promissora para a universidade, porém, optou-se manter o fornecimento de token no momento de transição de modo a ter certeza que a solução em nuvem atenderia a totalidade dos sistemas utilizados pela UFMG. Os resultados foram positivos e a solução em nuvem foi bem aceita pelos servidores.

Considerações

Considerando a estratégia brasileira para a transformação digital (E-Digital) 2022-2026, que estimula a adoção de soluções em nuvem nos processos e serviços governamentais;

Considerando a maior segurança, ganho em eficiência, acessibilidade, economicidade, diminuição de incompatibilidades proporcionada pela certificação em nuvem;

Considerando que os certificados digitais em nuvem foram testados na UFMG e apresentaram compatibilidade com os sistemas utilizados, maior facilidade logística para fornecimento e manutenção do serviço, boa aceitação dos usuários finais, nesta contratação opta-se pelo fornecimento de certificados digitais com armazenamento em nuvem de forma integral.

10. Registro de soluções consideradas inviáveis

Os certificados digitais A3 com armazenamento em mídias criptografadas apesar de atenderem a demanda apresentam algumas desvantagens que podem ser sanadas com o fornecimento de certificado digital em nuvem.

Smartcards

- Inviável devido à necessidade de aquisição de hardware específico para leitura.

Token

- danos físicos, perdas, roubos e bloqueios lógicos que podem inviabilizar sua utilização;
- obsolescência tecnológica da mídia pode tornar necessária a substituição e descarte de tokens;
- diversos modelos de token com manuais e manuseios distintos tornam mais complexa sua utilização por parte do usuário. Por ser pouco intuitivo necessitam de suporte constante para instalação e manutenção, o que pode sobrecarregar a equipe de T.I.

11. Análise comparativa de custos (TCO)

O levantamento de preços foi realizado utilizando o site "Painel de Preços do Governo Federal", localizado em: https://paineldeprecos.planejamento.gov.br/ Os relatórios gerados encontram-se anexados a este Estudo Técnico Preliminar. Segue tabela comparativa de preços:

Fornecedor: X.DIGITAL BRASIL SEGURANCA DA INFORMACAO LTDA Órgão: SUPREMO TRIBUNAL FEDERAL	R$ 92,90
Fornecedor: THOMAS GREG & SONS GRAFICA E SERVICOS, INDUSTRIA E COMERCIO, IMPORTACAO E EXPORT Órgão: CONSELHO FEDERAL DE ECONOMIA	R$ 105,72
Fornecedor: AR RP CERTIFICACAO DIGITAL LTDA Órgão: TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS	R$ 143,31
Fornecedor: SERVICO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO) Órgão: FUNDACAO UNIVERSIDADE FEDERAL DE MATO G. SUL	R$ 79,90

O principal diferencial entre as soluções disponíveis no mercado e que diminui consideravelmente os valores praticados é que o SERPRO fornece certificados integrados ao SIGEPE. É uma modalidade especial de emissão de certificados digitais para

servidores públicos federais . Trata-se de uma solução menos onerosa para o poder público, visto que, o serviço é prestado por meio da Autoridade de Registro-AR MPDG, vinculado ao Ministério da Economia e integrada ao SIAPE/SIGEPE e regulamentada pela INSTRUÇÃO NORMATIVA No 06, DE 11 DE AGOSTO DE 2017.

De acordo com o levantamento realizado no painel de preços, o menor preço é oferecido pelo **Serviço Federal de Processamento de Dados** (**Serpro**). Trata-se de empresa pública criada para modernizar e dar agilidade a setores estratégicos da administração pública. Está vinculada ao Ministério da fazenda e é regida pela **LEI Nº 5.615, DE 13 DE OUTUBRO DE 1970.**

Há que se considerar que o Serviço de emissão de Certificado Digital tem seus custos relacionados a AC (Autoridade Certificadora) e AR(Autoridade de Registro). As ARs têm a competência de identificar e cadastrar usuários, conferir e validar documentação na presença destes e encaminhar solicitações de certificados às AC. A AR corresponde a maior parte do custo dos certificados Digitais. Esta modalidade criada especialmente para servidores públicos o AR MPDG vinculado ao SIAPE/SIGEPE praticamente zera os custos relativos a AR no serviço de certificação digital. Se os órgãos públicos já possuem um sistema de gestão de pessoal que efetua o cadastro dos servidores e há servidores públicos nos diversos órgãos da administração pública que já são remunerados para executar este trabalho a contratação de uma AR particular para este fim, tendo em vista a possibilidade de vinculação a este sistema de gestão de pessoas, configuraria uma dupla oneração dos cofres públicos.

A Instrução Normativa que regulamenta a AR MPDG integrada ao SIGEPE veio para desburocratizar a emissão de certificados digitais para servidores públicos. Conforme exposto acima, é improvável que alguma empresa ofereça certificados digitais a preços menores que os praticados por esta modalidade especial oferecida aos servidores públicos. Ainda que alguma empresa ofereça o serviço a um custo menor, seria inviável sua contratação devido a logística que seria imposta ao servidor e a universidade para emissão do certificado digital. O tempo que o servidor dedicaria ao agendamento, comparecimento a AR e posterior retorno as atividades laborais acarretaria em diminuição das horas trabalhadas, configurando um custo que, por si só tem a capacidade de exceder o custo do próprio certificado.

Há que se ponderar que nem sempre o custo de um serviço está associado apenas ao preço pago por ele. Neste caso específico o tempo dedicado pelo servidor para comparecimento a AR em horário de trabalho onera o servidor e a universidade.

12. Descrição da solução de TIC a ser contratada

Para entendimento da solução a ser contratada consideramos válido definir: A.C. (Autoridade Certificadora) e A.R. (Autoridade de Registro)

Para garantir a emissão segura e livre de fraudes dos Certificados Digitais, existe uma hierarquia estabelecida na ICP-Brasil:

- **Autoridade Certificadora Raiz:** A AC Raiz é a autoridade máxima no país e é representada pelo Instituto Nacional de Tecnologia da Informação (ITI). Ela define as normas e regras da Certificação Digital e emite, distribui, revoga e gerencia os Certificados das Autoridades Certificadoras de nível subsequente.

- **Autoridade Certificadora de primeiro nível:** Esta entidade autentica, emite, revoga e gerencia os Certificados das Autoridades Certificadoras de segundo nível.

- **Autoridade Certificadora de segundo nível:** Responsável pela autenticação, emissão, revogação e gestão dos Certificados Digitais solicitados pela Autoridade de Registro.

- **Autoridade de Registro:** Atende o usuário final, coleta e valida a documentação e encaminha a solicitação à Autoridade Certificadora.

Os provedores de certificados em nuvem são:

SerproID; (SERPRO)

SafeID; (SafeWeb)

BirdID; (Soluti)

RemoteID; (CertiSign)

Vidaas; (Valid)

Serasa Experian; (Serasa Experian)

DS Cloud; (Digitalsign certificadora digital)

Os provedores listados acima são Autoridades Certificadoras de primeiro nível.(A.C. 1)

Foi credenciada junto A.C Raiz (ITI) no dia 31 de janeiro de 2019, a A.R. do Ministério do Planejamento. (A.R. MPDG). Conforme descrição abaixo fornecida pelo ITI.

> "A AR atenderá à Instrução Normativa nº 6, de agosto de 2017, que trata da validação das solicitações de certificados digitais ICP-Brasil para servidores públicos da ativa e militares da União.
>
> Na AR MPDG, a solicitação de certificado será realizada na presença de servidor ou militar autorizado. Serão utilizados para identificação dos requerentes do certificado digital o Sistema de Gestão de Pessoal – SIGEPE, administrado pelo Ministério do Planejamento, e os sistemas correlatos no âmbito dos Comandos Militares.
>
> Os servidores deverão ser biometricamente identificados e individualizados pela base biométrica oficial do Tribunal Superior Eleitoral – TSE ou pelos Prestadores de Serviço Biométrico – PSBios credenciados pela ICP-Brasil."

Fonte: https://mailman.iti.gov.br/noticias/indice-de-noticias/2467-credenciada-ar-do-ministerio-do-planejamento

Considerando:

- que a emissão do certificado digital envolve custos relacionados a A.C e A.R;
- que o SERPRO é a única Autoridade Certificadora com Autoridade de Registro vinculada ao SIGEPE;
- que além da economia financeira do A.R vinculada ao Sigepe, esta solução também proporciona ganhos logísticos e operacionais à universidade;
    - Logístico: o servidor não precisa se locomover até uma A.R para apresentação de documentos para validação de identidade e emissão de certificado. Apenas esse fato isoladamente já apresenta uma vantagem considerável para o servidor e a universidade.
    - Operacional: o certificado pode ser solicitado diretamente na plataforma do SouGov não sendo necessário criação de fluxo e recursos extras para este procedimento.

Além disso, o item 2.5 deste ETP esclarece que a solução deverá ser compatível com os diversos sistemas estruturantes da administração pública federal. Trata-se de uma necessidade de negócio conforme descrito no item 4.1 deste ETP: É necessário que a solução permita o acesso a todos os sistemas estruturantes da administração pública federal que exijam certificado digital para acesso. Foi comunicado recentemente pelo tesouro nacional a decisão de limitar o acesso ao Sistema Integrado de Administração Financeira do Governo Federal (Siafi) utilizando exclusivamente certificados digitais emitidos por Autoridades Certificadoras de Governo. Segundo o comunicado, os operadores que possuem perfil de acesso que não seja exclusivamente de consulta, só acessarão o SIAFI por meio de certificado digital emitido por autoridade certificadora de governo a partir de 31/10

/2024. Os comunicados emitidos pela Coordenação Geral de Sistemas e Tecnologia da Informação da STN, tesouro nacional e a listagem das autoridades certificadoras consideradas de governo e aceitas no acesso ao Siafi foram destacados e compõem o anexo III deste ETP.

Em consonância com as considerações elencadas acima, a solução proposta envolve a aquisição de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF com armazenamento em nuvem e A.R vinculada ao SIGEPE.

Com base no disposto no art. 74 da Lei nº 14.133/2021, o tipo de contratação que mais se adequa é a inexigibilidade de licitação, visto que entre as empresas que oferecem a solução apenas o SERPRO configura-se como autoridade certificadora do governo, fornece certificado em nuvem com vinculação ao SIGEPE e solicitação diretamente pelo SouGov.

Da Solução a ser contratada

800 certificados digitais com armazenamento em nuvem com A.R vinculada ao SIGEPE (SerproID)

13. Estimativa de custo total da contratação

Valor (R$): 63.920,00

800 x 79,90 = R$ 63.920,00 (sessenta e três mil, novecentos e vinte reais)

14. Justificativa técnica da escolha da solução

Certificado Digital em nuvem com A.R integrada ao SIGEPE

Justificativa técnica : Certificado digital em nuvem.

- Maior segurança e autenticação em dois níveis;
- O certificado digital em nuvem possui maior viabilidade técnica por poder ser instalado em diversos dispositivos enquanto o token uma vez perdido, danificado, formatado acidentalmente ou roubado acarreta em perda do certificado sendo necessário adquirir um novo certificado;
- Iniciativa do governo federal que visa estimular a utilização de soluções em nuvem. A estratégia brasileira para a Transformação Digital (E-Digital) 2022-2026 enumera como objetivo específico: "Adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal".

Justificativa técnica: A.R integrada ao SIGEPE

- A regulamentação para a implementação da política foi definida pela Instrução Normativa nº 6, em 2017, e funcionará a partir de solicitação pelo SouGov, certificação, verificação e aprovação do certificado digital utilizando os dados do SIGEPE;
- O processo de emissão do certificado para os servidores será mais ágil e econômico, pois utilizará os dados previamente apresentados ao Governo Federal no momento da posse e a biometria registrada pelos Prestadores de Serviço Biométrico – PSBios credenciados pela ICP-Brasil.
- O cadastro criado pelo governo na posse de seus servidores é seguro, o que garante a cadeia de confiabilidade e economicidade no processo, já que esta etapa é a mais cara, onerando a emissão do certificado.
- Interoperabilidade com demais sistemas da Administração Pública Federal;
- Vantagem logística e operacional quando comparado as demais soluções oferecidas no mercado.

Justificativa: SerproID

- AR integrada ao SIGEPE
- Necessidade de acesso a todos os sistemas estruturantes do Governo Federal.

- Os operadores que possuem perfil de acesso que não seja exclusivamente de consulta, só acessarão o SIAFI por meio de certificado digital emitido por autoridade certificadora de governo a partir de 31/10/2024. Das soluções em nuvem o SerproID é o único que possui AR MPDG.(Autoridade de Registro do Ministério do Planejamento, Desenvolvimento e Gestão)

15. Justificativa econômica da escolha da solução

Por permitir que processos sejam realizados do início ao fim no meio eletrônico, o Certificado Digital diminui gastos relacionados à compra, impressão e armazenamento de papel, ao transporte e à mão de obra, porque melhora a eficiência operacional.

O certificado digital em nuvem do Serpro, possui A.R. (Autoridade de Registro) vinculada ao Sigepe. A A.R. integrada ao Sigepe zera custos com logística para a universidade e otimiza o tempo dos servidores com deslocamentos e apresentação de documentos até uma unidade física para emissão do certificado.

Além de reduzir custos operacionais, é a solução mais econômica quando comparada as demais soluções oferecidas no mercado.

16. Benefícios a serem alcançados com a contratação

12.1. A presente contratação importará no atingimento dos seguintes resultados:

12.1.1. Aumentar a eficiência operacional quanto à celeridade e produtividade na execução das atividades administrativas;
12.1.2. Maximizar os resultados da governança administrativa;

12.1.3. Maximizar os resultados da governança de TIC;

12.1.4. Aumentar e manter os serviços que fazem uso de certificado digital com elevado padrão de desempenho, qualidade e confiabilidade;

12.1.5. Garantir a autenticidade, integridade e o não repúdio das transações realizadas;

12.1.6. Garantir a segurança das informações trafegadas por meio dos acessos realizados às aplicações disponibilizadas pelos órgãos do Poder Executivo;

12.1.7 Fornecimento de alternativa de certificação que propicia maior mobilidade aos usuários de certificado digital (certificado armazenado em nuvem);

12.1.9 Garantia de autenticidade, confidencialidade, integridade e não-repúdio às informações eletrônicas. O resultado de sua adoção é segurança, redução de custos, sustentabilidade e celeridade processual.

12.1.10 Acesso aos sistemas estruturantes da Administração Pública Federal que exigem o certificado digital. O acesso a tais sistemas é essencial para possibilitar a continuidade de atividades fundamentais da Instituição.

17. Providências a serem Adotadas

17.1 Elaboração de documentos relacionados (Termo de Oficialização da Demanda, ETP e Termo de Referência)

17.2. Capacitar servidores para a correta fiscalização do contrato em tela, evitando-se vícios ou desvios, bem como garantir o cumprimento das metas de eficiência e eficácia necessárias para o atendimento do objeto dessa contratação.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Após os estudos realizados neste ETP, verificou-se que a solução do SERPRO é a mais indicada para esta universidade devido a integração ao SIGEPE e facilidade/flexibilidade de pedidos de emissão de certificado pelo SouGov.

Alem disso, a viabilidade de contratação se justifica pela economicidade tendo em vista os valores praticados pelo SERPRO ficarem abaixo daqueles praticados no mercado conforme apresentado no estudo.

O serviço de Emissão simplificada de certificados para servidor público é uma solução que permitirá ao órgão uma maior desburocratização do processo de aquisição e emissão de Certificados ICP-Brasil para seus Servidores trazendo agilidade e economicidade, culminando no atendimento de seus objetivos institucionais e princípios de segurança da assinatura digital, bem como o uso racional dos recursos públicos da Instituição.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

LUCILENE MIRANDA DA SILVA

Analista de tecnologia da informação

Assinou eletronicamente em 29/08/2024 às 17:21:30.

SADALLO ANDERE NETO

Diretor da Divisão de Processos e Segurança

Assinou eletronicamente em 29/08/2024 às 17:24:40.

Lista de Anexos

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

- Anexo I - INSTRUÇÃO NORMATIVA No 6.pdf (878.14 KB)
- Anexo II - Levantamento painel de preços do governo federal.pdf (574.94 KB)
- Anexo III - Considerações relacionadas ao acesso SIAFI.pdf (1.89 MB)