

Número do Documento de Formalização da Demanda: 92/2024

1. Informações Básicas

Área requisitante	Data da conclusão da contratação	UASG	Editado por
CGTEC	01/07/2024 00:00	370003	JOSE EWERTON LEOCADIO DE SANTANA

Descrição sucinta do objeto
Certificados digitais SSL A1 e Tokens FIDO2
Justificativa da prioridade

1) A não contratação dos certificados na data prevista irá impactar diretamente o acesso do cidadão e dos servidores a alguns sistemas internos e processos de cargas de dados da CGU como Super, e-Aud, bCadastro, etc. 2) 10 unidades de tokens FIDO2 são necessárias para incremento do acesso de contas de alto privilégio no ambiente de nuvem da AWS da CGU.

2. Justificativa de necessidade

1. Contratação - Certificados Digitais SSL A1 (2024)

A CGU disponibiliza informações e serviços internos e externos para outros órgãos de estado e servidores por meio de um conjunto de sítios eletrônicos sob sua gestão, como E-aud, Super, etc.

Para isso, faz-se necessário que os servidores que hospedam estes sítios utilizem certificados digitais válidos para que qualquer ente que irá acessá-los possa confirmar sua autenticidade. Esse ente pode ser um computador pessoal ou uma aplicação, por exemplo. Sem a confirmação por meio de um certificado digital, não há segurança para o usuário sobre a autenticidade do sítio.

Essa autenticidade é garantida por meio de técnicas de criptografia assimétrica que permitem assegurar a integridade das informações constantes no certificado de posse de cada servidor, além de uma cadeia de outros agentes na Internet, considerados confiáveis, que atestam a veracidade das informações.

Dentre os formatos de certificados digitais, o A1 é o mais adequado para este uso, pois permite sua instalação diretamente nos servidores que irão prover estes serviços.

Atualmente 3 (três) servidores/domínios já utilizam os referidos certificados para hospedagem dos sítios da CGU e 1 (um) e-CNPJ da CGU é utilizado para acesso de dados, porém estes certificados terão sua validade finalizando no segundo semestre deste ano, o que implica na necessidade de renovação ou emissão de novos certificados para substituí-los, conforme tabela abaixo.

Domínio	Tipo	Validade dos certificados atuais
*.cgu.gov.br	Wildcard	07/08/2024
Controladoria-Geral da União (26.664.015/0001-48)	e-CNPJ	26/08/2024
bcadastro.cgu.gov.br	Single Domain padrão ICP – Brasil	22/08/2024

2. Aquisição de 10 unidades de tokens FIDO2

A CGU possui diversos sistemas e cargas de trabalho já em produção na nuvem da AWS, como portal da transparência, Fala.BR, etc. Faz-se cada vez mais necessário fortalecer os métodos de autenticação de acesso as contas administrativas com alto privilégio a esse ambiente de nuvem e demais cenários de proteções de acessos e dados sensíveis. Hoje, existem 10 contas administrativas com este nível de privilégio.

FIDO2 é um padrão de autenticação aberto, hospedado pela FIDO Alliance, que consiste na especificação W3C *Web Authentication (WebAuthn API)* e no *Client to Authentication Protocol (CTAP)*. CTAP é um protocolo de camada de aplicativo usado para comunicação entre um cliente (navegador) ou uma plataforma (sistema operacional) com um autenticador externo.

FIDO2 é a evolução do FIDO U2F e oferece o mesmo nível aprimorado de segurança baseado em criptografia de chave pública. FIDO2 oferece opções de autenticação expandidas, incluindo autenticação forte de fator único (sem senha), de dois fatores e multifator. Com esses novos recursos, permite-se a substituição de credenciais fracas de nome de usuário/senha por fortes credenciais de pares de chaves criptográficas apoiadas por hardware. Essas credenciais não são compartilhadas entre serviços, são resistentes a ataques de *phishing* e de repetição e, com a arquitetura correta, resistentes a ataques MiTM.

Opções de autenticação FIDO2:

- autenticação sem senha (*passwordless*): autenticação forte de fator único usando um autenticador de hardware elimina a necessidade de autenticação fraca baseada em senha;
- autenticação de dois fatores: autenticação forte de dois fatores usando um autenticador de hardware como uma camada extra de proteção além de uma senha; e
- autenticação multifator: autenticação multifatorial forte usando um autenticador de hardware e um PIN ou biométrico, para atender a requisitos de alta garantia, como os necessários para transações financeiras e pedidos de receitas.

3. Materiais/Serviços

3.1 Materiais

Nenhum material incluído.

3.2 Serviços

Nº do item	Grupo	Descrição	Qtd	Val. unit. (R\$)	Val. total (R\$)
1	SERVIÇOS DE EMISSÃO DE CERTIFICADOS DIGITAIS	EMISSÃO DE OUTROS TIPOS DE CERTIFICADOS COM TOKEN	10,00	951,01	9.510,10
2	SERVIÇOS DE EMISSÃO DE CERTIFICADOS DIGITAIS	EMISSÃO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR	4,00	656,75	2.627,00

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](#).

JEFTE MEDEIROS DE SOUZA

Coordenador-Geral de Infraestrutura de Tecnologia

5. Acompanhamento

Nenhum acompanhamento incluído.

6. Relacionamentos

Nenhum relacionamento encontrado.