



GOVERNO DO ESTADO DE MINAS GERAIS

Departamento de Estradas de Rodagem do Estado de Minas Gerais

Gerência de Tecnologia da Informação e Comunicação - Núcleo de Gestão de Contratos

Estudo Técnico Preliminar (ETP) 86152850 - DER/DPGF/GTIC-CONT

Belo Horizonte, 12 de abril de 2024.

ESTUDO TÉCNICO PRELIMINAR

I – INFORMAÇÕES GERAIS

1. Identificação do processo e solicitante

Número do processo SEI!: 2300.01.0050736/2024-83

Número da Solicitação no Portal de Compras MG: 2301403 000046/2024

Área solicitante: Gerência de Tecnologia da Informação

2. Equipe de Planejamento da Contratação:

Documento(s) de designação (número SEI!):

Samuel Rocha Franca

II – DIAGNÓSTICO DA SITUAÇÃO ATUAL

1. Descrição do problema a ser resolvido ou da necessidade apresentada (PREENCHIMENTO OBRIGATÓRIO) (art. 6º, I e IV)

Considerando a proximidade do fim de vigência do contrato N° DF-016/2023 em 09/08/2024, cujo objeto é a prestação de serviços de emissão de certificados digitais digitais SSL/TLS, solicitamos a realização de nova contratação a fim de possibilitar a continuação do serviço de certificado digital para autenticação de servidores de aplicação dos principais sistemas de informação do DER-MG apresentando maior grau de segurança aos serviços digitais.

Com o aumento do uso da Internet para diversos fins, tornou-se imprescindível a criação de meios que possibilitem a comunicação entre dois pontos, por meio da rede, com utilização de recursos de segurança que incrementem a confiabilidade e autenticidade.

O DER-MG optou-se pela inclusão dos certificados de servidores, pois esta Autarquia possui sistemas de informação essenciais para suportar seus processos e alguns desses sistemas são integrados a fontes de dados de Sistemas de Informações de entidades de governo estaduais por meio de componentes de software: API, Web Services, etc. Para aumentar a segurança dessas integrações, os sistemas que provêm as fontes de dados determinam como premissa a obrigatoriedade, por parte do sistema usuário para o consumo de seus Serviços, do uso de Certificado Digital para equipamento/aplicação emitido por uma Autoridade Certificadora pertencente à hierarquia da ICP-Brasil.

Além disso, o DER-MG possui alguns sistemas de informação em uso, a exemplo do Sistema Integrado de Gestão de Infraestrutura Viária (SGIV) e Observatório de Dados de Infraestrutura, que exigem que esta Autarquia, como pessoa jurídica, bem como os documentos e informações gerados por estes, tenha a sua autenticidade comprovada.

O Sistema Integrado de Gestão de Infraestrutura Viária (SGIV) é um abrangente e integrado conjunto de ferramentas de trabalho dos usuários no apoio às suas atividades finalísticas operacionais e gerenciais, além de disponibilizar um Portal de Serviços que permite ao cidadão realizar solicitações de serviços diversos, tais como abertura de defesa de autuação, abertura de recurso JARI, abertura de Recurso CETRAN, emissão de boletos para recolhimento de taxas, obtenção de informações sobre o andamento de seus processos, dentre outros.

O Observatório de Dados de Infraestrutura – DER-MG será um repositório de dados baseado na plataforma ArcGIS (ArcGIS Sites) que permitirá ao cidadão ter acesso à informação das obras, status, evolução física-financeira e fotografias de acompanhamento, mapa rodoviário do Estado de Minas Gerais, Obras de Artes, investimentos em infraestrutura e outras informações necessárias para dar transparência à sociedade.

Essa comprovação de autenticidade é garantida mediante o uso de certificados digitais SSL. O certificado SSL ou TLS, chamados respectivamente de Secure Socket Layer e Transport Layer Security, são protocolos de criptografia que proporcionam segurança na troca de dados via WEB entre aplicativos e servidores.

O Certificado Digital para Autenticação de Servidor com o uso do protocolo SSL/TLS confere a encriptação de páginas e sites característica que autentifica e protege as informações das duas partes envolvidas, o usuário e o site.

Do ponto de vista da segurança, existem algumas distinções importantes entre um Certificado SSL emitido por uma Autoridade Certificadora privada, mediante pagamento, e um SSL fornecido pela Let's Encrypt de forma gratuita. Um exemplo é o nível de validação e das garantias oferecidas em cada um dos padrões, em caso de rupturas na segurança.

Existem algumas considerações sobre a utilização de um certificado com SSL de cadeia de órgão credenciado, principalmente por se tratar de um provedor público. Por se tratar de um serviço mais recente, a Let's Encrypt, além de não transparecer muita confiança, não oferece garantias em relação à proteção dada por seu Certificado.

Por outro lado, Autoridades Certificadoras diversas oferecem uma espécie de “seguro”, caso falhas sejam detectadas no Certificado. Com isso, o SSL acaba sendo uma opção mais confiável.

Além desses pontos, também podemos citar mais alguns que diferenciam essas tecnologias:

SSL Pago

- para ser instalado, depende de um IP dedicado;
- necessita ser gerado por uma Autoridade Certificadora devidamente homologada;
- oferece garantias contra falhas e rupturas na segurança, ressarcindo financeiramente o utilizador por eventuais danos;
- tem um prazo de validade médio de 1 ano;
- possui uma melhor retrocompatibilidade com softwares e navegadores mais antigos, visto que se trata de um padrão mais consolidado no mercado.

SSL gratuito Let's Encrypt

- não depende de IP dedicado para ser instalado na página;
- não tem nenhum custo de utilização, muito embora também não ofereça nenhuma garantia de proteção avançada;
- não possui seguro contra fragilidades na segurança;
- tem duração de 90 dias, o que significa que precisa ser constantemente renovado pelo utilizador e requer um acompanhamento;
- por se tratar de um Certificado mais recente, tem um menor retro compatibilidade com sistemas, softwares e navegadores mais antigos, o que pode gerar falhas.

No mais, existem algumas desvantagens que são exclusivas do Certificado fornecido pela Let's Encrypt. São elas:

- impossibilidade de proteger múltiplos subdomínios dentro da página;
- não é capaz de verificar a identidade do indivíduo da empresa — o que torna mais sensível a troca de informações entre o visitante e o servidor, pois não se sabe se a página é realmente de quem se diz ser;
- não trabalha com a validação estendida de domínio — isso significa que não há a presença da barra verde ao lado da URL da página;
- não opera com Certificados de validação da organização (OV);
- não possui Certificados com validação estendida (EV).

Na prática, o SSL padrão, por um custo totalmente acessível, oferece uma maior confiabilidade, robustez e segurança tanto para a página quanto para o visitante. Além disso, esse é um protocolo já bastante validado no mercado, sendo utilizado por empresas de diferentes segmentos e que necessitam de alto rigor na gestão de suas informações.

Busca-se nesta ação, portanto, atender as necessidades de Segurança da Informação nos processos de Tecnologia da Informação, adquirindo certificados digitais do tipo SSL, conforme quantitativo detalhado neste documento.

A presente contratação encontra-se alinhada com o seguinte objetivo estratégico: “Promover a adesão efetiva à Política de TIC do Governo”.

Além disso, o [Decreto Estadual nº 47.974/2020](#), que institui a Política de Tecnologia da Informação e Comunicação, define diretrizes estratégicas para a área de tecnologia no âmbito da administração pública estadual. Dentre estas diretrizes estratégicas, destacamos:

III – segurança da informação:

a) aprimorar as políticas de segurança de informação existentes, agregando regulações e diretrizes sobre novas tecnologias;

Dessa forma, a contratação também atenderá ao definido na diretriz estratégica III, aplicando mais segurança aos seus sistemas de informação por meio de novas tecnologias.

A não contratação do fornecimento do item trará prejuízos à administração desta Autarquia, uma vez que a comunicação entre o usuário e os serviços web do DER-MG não serão criptografados, com isso os dados trafegados estarão inseguros.

2. Alinhamento entre a contratação e o planejamento da Administração (art. 6º, II)

A necessidade da presente contratação encontra-se registrada no Planejamento Anual de Compras, nos termos da Resolução SEPLAG nº. 14/2014.

3. Descrição dos requisitos da potencial contratação (art. 6º, III)

De acordo com as regras vigentes para certificação digital, para que certificados digitais possam ser usados nos sistemas do DER-MG, estes deverão ser emitidos em conformidade com os padrões estabelecidos por instituições cadastradas como Autoridade Certificadora (AC).

III – PROSPECÇÃO DE SOLUÇÕES (PREENCHIMENTO OBRIGATÓRIO)

1. Levantamento de Mercado (art. 6º, V)

O protocolo SSL age como se fosse uma camada de proteção que decodifica informações, protegendo-as de ataques. Trata-se de uma coleção de arquivos de dados emitidos por uma organização chamada Autoridade de Certificação (CA). Sua finalidade é adicionar uma camada de segurança por cima do protocolo HTTP, usado

para transferir o tráfego do site na Internet.

Quando um site tem um certificado SSL, seu URL começa com https:// em vez de http://. Ele também tem um ícone de cadeado na barra de endereço.

O certificado digital SSL possui diversos níveis de validação, que podem ser escolhidos de acordo com a demanda e a área de atuação, tais como:

- Validação de Domínio (SSL DV).
- Validação de Organização (SSL OV) ,
- Validação Estendida (SSL EV).

Os níveis de criptografia são os mesmos para cada certificado, o que os diferenciam são os processos de ativação e verificação necessários para obter o certificado.

O certificado SSL DV

A Autoridade Certificadora verifica o direito do requerente de usar um nome de domínio específico. O nível de segurança fornecido é básico e serve para validar o nível de confiança do domínio. Nenhuma informação de identidade da empresa é verificada e nenhuma informação é exibida além das informações de criptografia no Selo de Site Seguro. Apresenta a imagem do cadeado fechado nos navegadores.

O certificado SSL OV

A Autoridade Certificadora verifica o direito do requerente de usar um nome de domínio específico e realiza verificações da empresa. Informações adicionais verificadas da empresa são exibidas aos clientes ao clicar no Selo de Site Seguro, oferecendo maior visibilidade sobre quem está por trás do site e a confiança aprimorada associada.

O certificado SSL EV

A Autoridade Certificadora verifica o direito do requerente de usar um nome de domínio específico e realiza uma verificação completa da empresa. O processo de validação é ainda mais abrangente do que no OV.

Os certificados SSL são ofertados de acordo com o número de domínios protegidos:

Domínio único SSL	Permite que apenas um domínio utilize o certificado. Se for necessário instalar o certificado em outro endereço ou subdomínio será preciso adquirir uma nova licença.
Multidomínio SSL	Permite que vários domínios utilizem o mesmo certificado. A quantidade total de domínios no certificado é de 5 domínios, podendo ocorrer variação de endereços com diferentes domínios.
Wildcard SSL	Emitido para um domínio e utilizado para uma quantidade ilimitada de subdomínios vinculados ao domínio principal seguindo o exemplo “*.dominio.com.br”.

Ressalta-se ainda que, conforme verificado no mercado e contratações similares, este tipo de certificação somente é ofertada com validade de 1 (um) ano. Assim, a cada ano será necessário realizar nova contratação.

2. Estimativa do valor da contratação (art. 6º, VI)

Realizou-se pesquisa direta com vários fornecedores, mediante solicitação formal de cotação(doc. 87265358).

Ressalta-se que, apesar da ampla pesquisa, não foram encontradas Atas de Registro de Preço compatíveis com o objeto em questão.

A contratação, seguindo as normas de pesquisa de preços com orientações de boas práticas, foi estimada em R\$ 2.272,73 (dois mil, duzentos e setenta e dois reais e setenta e três centavos), conforme valores abaixo consolidados e de acordo com os tipos de certificado SSL definidos:

ITEM	CÓDIGO	DESCRIÇÃO	QUANT.	X. DIGITAL (doc. 87043636)		KEYSEC (doc. 87044379)		BMTECH (doc. 87330405)		PREÇO MÉDIO
				PREÇO UN	PREÇO TOTAL	PREÇO UN	PREÇO TOTAL	PREÇO UN	PREÇO TOTAL	
1	99520	CERTIFICADOS DE SERVIDOR WEB SSL A1 VALIDAÇÃO DO DOMÍNIO (SSL-DV) DE DOMÍNIO ÚNICO COM VALIDADE DE 01 ANO	1	R\$ 710,00	R\$ 710,00	R\$ 200,00	R\$ 200,00	R\$ 120,00	R\$ 120,00	R\$ 343,330
2	99511	CERTIFICADOS DE SERVIDOR WEB SSL A1 VALIDAÇÃO DE ORGANIZAÇÃO (SSL-OV) WILDCARD COM VALIDADE DE 01 ANO	1	R\$ 1.100,00	R\$ 1.100,00	R\$ 3.025,00	R\$ 3.025,00	R\$ 1.663,20	R\$ 1.663,20	R\$ 1.929,40
TOTAL								R\$ 2.272,73		

TABELA I:

Pesquisa de Mercado

Para o valor estimado para a contratação foram considerados os valores da pesquisa de mercado similares.

3. Escolha da solução (consequência dos incisos V e VI do art. 6º)

A emissão de certificados nos servidores do DER-MG é relacionada ao quantitativo de domínios/subdomínios, além de ser a mais praticada, proporciona menor custo, uma vez que a quantidade de ativos envolvidos é inferior, utilizando-se uma relação similar de custo unitário entre as soluções.

Os sistemas e portais do DER-MG que necessitam de transmissão segura pela Internet são atendidos pelos domínios e subdomínios listados abaixo:

ID	DOMÍNIO/SUBDOMINIO
1	observatorio.infraestrutura.mg.gov.br
2	www.autoinfracao.der.mg.gov.br
3	www.consultaait.der.mg.gov.br
4	www.consultas.der.mg.gov.br

5	ead. der.mg.gov.br
6	www.grin. der.mg.gov.br
7	homolog.mapasmo. der.mg.gov.br
8	smo.sgiv. der.mg.gov.br
9	portal.sgiv. der.mg.gov.br
10	www.sgtf. der.mg.gov.br
11	www.sgtm. der.mg.gov.br
12	www.sicar. der.mg.gov.br
13	homolog.smo. der.mg.gov.br
14	mapa.smo. der.mg.gov.br
15	www.srh. der.mg.gov.br
16	portalhml. der.mg.gov.br
17	suporte. der.mg.gov.br

Conforme a necessidade de segurança de cada domínio listado acima e o custo, conclui-se que para o domínio "**observatorio.infraestrutura.mg.gov.br**" que possui somente um domínio e será utilizado inicialmente para publicação de conteúdos referente às informações das obras optou-se pelo **tipo de certificado SSL-DV**.

Já para o domínio "***.der.mg.gov.br**" que possui diversos subdomínios que disponibilizam informações e serviços aos usuários internos e externos optou-se pelo tipo de **certificado SSL-OV Wildcard**. Desta forma, o uso de um certificado do tipo Wildcard, que atende a todo o domínio e subdomínios de uma organização, encaixa-se perfeitamente como solução, já que pode ser utilizado para todos os serviços web provido pelo DER-MG. Em especial, esse tipo de certificado digital é utilizado para prover acesso seguro ao sítio desta Autarquia (www.der.mg.gov.br), ao Portal de Serviços que permite ao público acompanhar o andamento dos seus processos e realizar abertura de defesa de autuação, abertura de recurso JARI, abertura de Recurso CETRAN, emissão de boletos para recolhimento de taxas.

IV – DETALHAMENTO DA SOLUÇÃO ESCOLHIDA

1. Descrição da solução como um todo (PREENCHIMENTO OBRIGATÓRIO) (art. 6º, VII)

Solução de certificado digital do tipo SSL (Secure Socket Layer) do tipo SSL-DV e SSL-OV Wildcard, visando credenciar como confiável o Observatório de Dados de Infraestrutura, assim como os demais serviços web oferecidos pelo DER-MG por meio do domínio "***.der.mg.gov.br**", para os navegadores de internet.

2. Justificativas para o parcelamento ou não da contratação (PREENCHIMENTO OBRIGATÓRIO)

Como regra geral, exige-se o parcelamento do objeto sempre que isso se mostre técnica e economicamente viável. Ocorre que, apesar do objeto ser dividido em itens, sendo que tal divisão o não traz prejuízo para o objetivo final almejado, os itens devem compor um único lote. Esse entendimento se deve ao fato dos serviços agrupados estarem intrinsecamente relacionados.

Por praxe, o mercado atende a este requisito entregando tais bens e serviços como uma solução indissociável

de modo a ser fornecido por uma só empresa. Desta forma, assegura-se a eficiência no emprego dos recursos financeiros para a aquisição da solução pretendida.

Há também que se considerar o aspecto da economicidade pelo fator de escala no caso de um único fornecimento, em contraposição à aquisição ou contratação segmentada.

3. Contratações correlatas e/ou interdependentes (art. 6º, XI)

Não se faz necessária a realização de, quaisquer outras, contratações correlatas e ou interdependentes ao objeto pretendido.

4. Resultados pretendidos (art. 6º, IX)

Os certificados deverão assegurar a autenticidade, confiabilidade e integridade das informações providas pelos sistemas corporativos via portais do DER-MG.

5. Providências a serem adotadas (art. 6º, X)

Não há evidência de necessidades de adequações no ambiente do órgão advindas da contratação de certificados digitais.

6. Possíveis impactos ambientais (art. 6º, XII)

Não se fez observar a existência de possíveis impactos ambientais, razão pela qual este item não será considerado no planejamento.

V - POSICIONAMENTO CONCLUSIVO (PREENCHIMENTO OBRIGATÓRIO) (art. 6º, XIII)

Os estudos preliminares evidenciaram que a contratação de Serviço de fornecimento de certificado digital SSL mostra-se viável em termo de eficiência, de eficácia, de economicidade e de padronização, pois apresenta maior grau de segurança aos serviços digitais, bem como atende com melhor satisfação o requisito de segurança, forçando a atualização das informações de cada certificado em períodos de 12 meses e assim garantir que os Certificados sempre estejam utilizando os padrões de criptografia mais recentes.

ASSINATURAS:

- Equipe de Planejamento da Contratação e Autoridade Competente nos termos do art. 5º da Resolução SEPLAG nº 115/2021.



Documento assinado eletronicamente por **Samuel Rocha França, Servidor(a) Público (a)**, em 17/05/2024, às 13:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 47.222, de 26 de julho de 2017](#).



A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **86152850** e o código CRC **86CB9E0E**.