MUNICÍPIO DE CAXIAS DO SUL

ESTUDO TÉCNICO PRELIMINAR

1 - INFORMAÇÕES BÁSICAS:

Número do processo no PROA: processo ainda não protocolado.

2 - DESIGNAÇÃO DA EQUIPE DE PLANEJAMENTO:

Não há Portaria ou Ordem de Serviço designada para este fim. O presente estudo será assinado pela Superintendência de Tecnologia da Informação e Comunicação.

3 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO:

O Certificado digital é um documento/arquivo eletrônico que identifica pessoas, microcomputadores e empresas no mundo digital, comprovando sua identidade e permitindo o acesso a serviços on-line, bem como a realização de transações eletrônicas com garantia de autenticidade, integridade e não repúdio. A autenticidade garante a autoria de um documento, o acesso legítimo a um sistema, dentre outros. A integridade garante que as informações não foram alteradas sem a devida autorização. O não repúdio fornece mecanismos que contribuem para comprovar a autoria de uma operação ou documento eletrônico, dificultando sua contestação posterior sob alegação de desconhecimento ou ausência de autoria.

O Município de Caxias do Sul faz uso de diversos tipos de certificado digital para atender às necessidades operacionais do Município, que demandam por segurança nas transações eletrônicas, na autenticação de usuários e na comprovação de identidade. Em outras palavras, faz-se uso de certificados digitais para lidar com documentos e acesso a sistemas, cuja autenticidade precisa ser comprovada, tornando-os elementos fundamentais para garantir a segurança, a autenticidade e a validade jurídica das operações digitais. Além disso, os certificados digitais são utilizados, de modo geral, para o cumprimento de obrigações fiscais, acesso a sistemas e sites governamentais, assinatura de documentos eletrônicos e realização de transações eletrônicas seguras.

Os Certificados A1 e A3 (emitidos na forma de e-CPF e e-CNPJ) são utilizados pelo Município para esse fim, observando-se as particularidades de cada um deles, conforme a aplicação específica. O certificado A1 é armazenado em arquivo digital, normalmente protegido no computador ou dispositivo do usuário, podendo também ser utilizado em servidores ou outros ambientes computacionais autorizados, conforme a aplicação, e utiliza criptografia de chave pública para garantir que as transações e comunicações sejam seguras. Já o certificado A3 é armazenado em um dispositivo físico, como um token USB ou um cartão inteligente, com a chave privada protegida no próprio dispositivo, requerendo sua disponibilidade e, conforme o dispositivo e a aplicação, a utilização de mecanismo de autenticação, como senha ou PIN, para a realização de operações criptográficas e assinaturas digitais.

De acordo com regramentos do ICP-BRASIL, a validade dos certificados A3 terão o prazo de validade reduzido até completarem o período de 1 ano para troca das cadeias superiores de assinatura. Conforme previsto na resolução CG ICP-BRASIL nº 211, não é mais possível a emissão de certificados digitais com validade superior à 02/03/2029 em função de um processo de transição da cadeia de certificados. Desta forma, o período que inicialmente se adquiria de 3 anos para os certificados do tipo A3 será gradativamente reduzido, sendo considerado o prazo de vigência o máximo permitido no momento da emissão, sendo contratado para 2 anos ou o prazo máximo disponível conforme cadeia de certificados vigente.

Conforme demonstrado acima, os certificados pretendidos são essenciais ao desempenho das atribuições de membros e servidores, uma vez que é imprescindível que estes assinem e tramitem documentos e processos com a devida validade jurídica, bem como acessem sistemas e serviços que exigem autenticação por certificado digital, provendo segurança e confiabilidade para os acessos aos sistemas e serviços mantidos no ambiente de TI do Município de Caxias do Sul. Ante o exposto, faz-se necessária a aquisição dos certificados digitais descritos neste documento, bem como dos dispositivos criptográficos (hardware), tais como tokens USB, quando houver necessidade de utilização de certificados A3, para que se atinjam os resultados pretendidos.

4 - DESCRIÇÃO DOS REQUISITOS PARA A CONTRATAÇÃO:

1. CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A1

a) Certificado digital do tipo A1 para pessoa física (e-CPF).

b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros.

d) Deve ser gerado e armazenado em arquivo digital, permitindo sua instalação e utilização em ambiente computacional compatível, bem como a exportação do certificado e de sua chave privada, quando permitido pelas políticas e procedimentos aplicáveis.

e) Deve ter validade de 1 (um) ano, contada a partir da emissão do certificado.

f) O presente item engloba o serviço de autoridade de certificação e registro.

g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada.

g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais.

g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.

2. CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A1

a) Certificado digital do tipo A1 para pessoa jurídica (e-CNPJ).

b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros.

d) Deve ser gerado e armazenado em arquivo digital, permitindo sua instalação e utilização em ambiente computacional compatível, bem como a exportação do certificado e de sua chave privada, quando permitido pelas políticas e procedimentos aplicáveis.

e) Deve ter validade de 1 (um) ano, contada a partir da emissão do certificado.

f) O presente item engloba o serviço de autoridade de certificação e registro.

g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada.

g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais.

g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.

3. CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A3

a) Certificado digital do tipo A3 para pessoa física (e-CPF).

b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros.

d) Deve ser compatível com a emissão e utilização em dispositivo criptográfico compatível com os requisitos e certificações aplicáveis da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI), quando utilizado em token criptográfico.

e) Deve ter validade de 2 (dois) anos ou o prazo máximo disponível conforme cadeia de certificados vigente, contada a partir da emissão do certificado.

f) O presente item engloba o serviço de autoridade de certificação e registro.

g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada.

g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais.

g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.

4. CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A3

a) Certificado digital do tipo A3 para pessoa jurídica (e-CNPJ).

b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros.

d) Deve ser compatível com a emissão e utilização em dispositivo criptográfico compatível com os requisitos e certificações aplicáveis da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI), quando utilizado em token criptográfico.

e) Deve ter validade de 2 (dois) anos ou o prazo máximo disponível conforme cadeia de certificados vigente, contada a partir da emissão do certificado.

f) O presente item engloba o serviço de autoridade de certificação e registro.

g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada.

g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais.

g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.

5. TOKEN USB PARA CERTIFICADO DIGITAL

a) Dispositivo criptográfico com interface USB, compatível com portas USB-A existentes nos equipamentos utilizados pelo Município.

b) Deve ser capaz de gerar e utilizar, de forma segura, chaves criptográficas, bem como armazenar e utilizar certificados digitais A3 (e-CPF, e-CNPJ e/ou e-PJ), emitidos por autoridade certificadora credenciada pela ICP-Brasil.

c) Dispor de drivers e software utilitário de gerenciamento do dispositivo compatíveis com os sistemas operacionais Windows 11 64 bits, macOS e Linux Ubuntu 64 bits, nas versões oficialmente suportadas pelo fabricante durante a vigência contratual, em idioma português brasileiro.

d) O software utilitário de gerenciamento deve dispor de funcionalidades que permitam consultar informações gerais do token e, conforme suportado pelo dispositivo, realizar operações de inicialização, gerenciamento dos certificados, alteração do PIN e do PUK, desbloqueio do PIN mediante PUK e demais operações de gerenciamento previstas pelo fabricante.

e) Deve ser compatível com os navegadores Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera e Safari, em suas versões estáveis, permitindo acesso a sistemas que requeiram autenticação por meio de certificado digital.

f) Deve ser compatível com aplicações de assinatura digital de documentos PDF que utilizem certificados digitais e padrões criptográficos compatíveis com ICP-Brasil, incluindo o Adobe Acrobat Reader quando disponível para o sistema operacional utilizado.

g) A instalação do driver e do software utilitário de gerenciamento do dispositivo não deve interferir com outros dispositivos que, porventura, já estejam instalados no sistema operacional, e não deverá exigir a desativação de mecanismos de segurança do sistema operacional, como antivírus, firewall ou mecanismos de proteção equivalentes, nem exigir privilégios administrativos permanentes para sua utilização normal.

h) Deve dispor de manuais de instalação do driver e de instalação e operação do software utilitário de gerenciamento do dispositivo, com documentação específica aplicável a cada um dos sistemas operacionais referidos na letra "c".

i) O dispositivo deve implementar mecanismo de bloqueio após quantidade configurada ou definida pelo fabricante de tentativas consecutivas de PIN inválido, de forma a impedir tentativas ilimitadas de autenticação.

j) O dispositivo deve implementar mecanismo de proteção contra tentativas consecutivas de PUK inválido, conforme os requisitos de segurança e homologação aplicáveis ao dispositivo.

k) Deve permitir a reinicialização segura do dispositivo para seu estado inicial, com remoção dos certificados e chaves privadas armazenados e possibilidade de configuração de novo PIN de acesso, conforme os procedimentos previstos pelo fabricante.

l) Deve permitir a importação de certificados e respectivas chaves privadas, quando tecnicamente aplicável, para a área de armazenamento do dispositivo, a partir de arquivos no formato PKCS#12 (PFX/P12), conforme os padrões aplicáveis.

m) Deve permitir a exportação dos certificados públicos armazenados no dispositivo, sem permitir a exportação das respectivas chaves privadas.

n) Deve possuir capacidade de armazenamento de certificados digitais e respectivas chaves privadas suficiente para permitir a instalação e utilização simultânea de, no mínimo, 10 (dez) certificados digitais A3 distintos, sem comprometer o funcionamento e a segurança do dispositivo.

o) Deve possuir garantia mínima de 1 (um) ano, contado a partir do recebimento pelo Município, contra defeitos de fabricação e funcionamento.

5 - LEVANTAMENTO DE MERCADO:

De acordo com experiências anteriores em adquirir estes objetos e objetos similares, não há restrições iniciais acerca de qual empresa poderá fornecê-lo. Qualquer empresa apta a fornecer o objeto pretendido e que satisfaça os requisitos do presente estudo e exigências previstas futuramente no termo de referência poderá fazê-lo.

6 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

Fornecimento de Certificados Digitais A1 e A3 nas formas de e-CPF e e-CNPJ e tokens para atender as necessidades da Administração Pública Municipal, conforme condições, quantidades e exigências estabelecidas neste instrumento.

7 - ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS:

A estimativa de consumo projetada para o período de 24 meses considera o histórico de emissões dos últimos 24 meses e dos tokens solicitados além de considerar as emissões anteriores que estariam por vencer, novas nomeações de pessoal e a movimentação de pessoal ao longo do tempo nos setores em que se faz uso dos objetos contidos neste Estudo Técnico Preliminar.

8 - ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

Foram realizadas buscas de contratações recentes por outros entes governamentais com certificados e tokens nas mesmas características conforme tabela a seguir:

Grupo	Item	Un.	Descrição	Unitário medio	Total estimado
1	1	50	Certificado A1 (e-CPF)	R$ 57,66	R$ 2.883,00
	2	20	Certificado A1 (e-CNPJ)	R$ 56,02	R$ 1.120,40
	3	200	Certificado A3 (e-CPF)	R$ 48,33	R$ 9.666,00
	4	10	Certificado A3 (e-CNPJ)	R$ 68,80	R$ 688,00
	5	50	Token USB para certificado digital	R$ 46,48	R$ 2.323,75

9 - JUSTIFICATIVA PARA PARCELAMENTO:

A justificativa pelo fornecimento dos objetos do presente Estudo Técnico Preliminar por adjudicação por grupo deverá ocorrer, uma vez que a aquisição de um item de cada fornecedor pode causar incompatibilidade entre o token e o certificado. Nos casos em que for necessário a aquisição de token USB a mesma será realizada juntamente com o certificado.

10 - CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES:

A aquisição do objeto ora estudado não demanda a realização de contratações correlatas ou interdependentes.

11 - DEMONSTRATIVO DA PREVISÃO DA CONTRATAÇÃO NO PLANO ANUAL DE CONTRATAÇÃO – PAC:

O Município possui Plano Anual de Contratações vigente para o exercício 2026, tendo o objeto deste estudo técnico preliminar cadastrado no id 953.

12 - DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS:

Contar com possibilidade de obter certificados em substituição aos certificados que irão expirar em todas as aplicações cabíveis, além da emissão de novos certificados que venham a se fazer necessários, garantindo a continuidade de atividades essenciais, como por exemplo a assinatura e tramitação de documentos e processos com a devida validade jurídica.



MUNICÍPIO DE CAXIAS DO SUL

13 - PROVIDÊNCIAS PRÉVIAS AO CONTRATO:

Entendemos não haver necessidade de providências prévias, uma vez que devemos aguardar o recebimento do objeto e após isso conferir se esta de acordo com o que foi solicitado e destiná-los conforme as necessidades já mencionadas no presente estudo.

14 - IMPACTOS AMBIENTAIS:

Não existe impacto ambiental para o fornecimento dos serviços objetos desta contratação.

15 - VIABILIDADE DA CONTRATAÇÃO:

Declaramos **VIÁVEL** esta contratação, tendo em vista tratar-se de subsídio para segurança nas transações eletrônicas, autenticação de usuários, comprovação de identidade e prestação continuada de serviços informáticos de suma importância para as atividades do Município.

Caxias do Sul, 29 de setembro de 2026.

Fernando Brombatti - matr. 8715
Responsável pela elaboração do Estudo Técnico Preliminar - ETP
(ou Equipe de Planejamento instituída por Portaria ou Ordem de Serviço)

JUSTIFICATIVA PARA A INADMISSÃO DE CONSÓRCIOS

A Lei nº 14.133/2021 tem como regra a permissão à participação de consórcios, inclusive quando o instrumento for omisso sobre o tema. A Administração Pública, quando não permitir a participação de licitantes em consórcios, deve motivar essa decisão, justificando as razões para tanto.

O ato convocatório poderá admitir ou não a participação de consórcio, sendo essa escolha um ato discricionário da Administração Pública, o que evidentemente não significa autorização para decisões arbitrárias ou imotivadas. Por este motivo, a Autoridade Licitante, dentro do poder discricionário de melhor conveniência e oportunidade decidirá pela vedação ou não à participação de empresas em regime de consórcio.

A admissão de participação de consórcio faz-se necessária quando em razão das circunstâncias do mercado e/ou a complexidade do objeto tornam problemática a competição, ou seja, quando parcela significativa de empresas, isoladamente, não dispuser de condições para participar da licitação. Dessa forma, a participação de empresas reunidas em consórcio ampliará o universo de licitantes, pois possibilitará a junção de 2 ou mais empresas para realização de determinado objeto. (Marçal Justen Filho, Comentários à Lei de Licitações e Contratações Administrativas, 2021).

A jurisprudência do TCU traz entendimento que a formação de consórcio tanto pode fomentar a concorrência, como cerceá-la. Ou seja, a vedação ou a admissão de consórcio em licitação dever ter em vista possibilitar maior concorrência, que conforme o caso concreto pode ocorrer em uma ou outra situação (...) (Acórdão TCU 2.813/2004 e 1.782/2009).

Com relação a presente contratação, a vedação à participação de interessadas, que se apresentem constituídas sob a forma de consórcio, se justifica na medida em que nas contratações de bens e serviços comuns, tendo em vista a proporção da demanda do Município, é perfeitamente pertinente e compatível com empresas que atuam em todo território nacional, empresas essas que possuem condições suficientes para a execução de objetos dessa natureza, o que não tornará restrito o certame a um pequeno número de empresas.

Assim sendo, avaliando a realidade do mercado para este objeto, **não será permitida a participação de empresas reunidas em consórcio.**