

Estudo Técnico Preliminar 74/2022

1. Informações Básicas

Número do processo: 00094.001012/2022-73

2. Introdução

Este Estudo Técnico Preliminar tem por objetivo identificar e analisar soluções possíveis para o atendimento da demanda que consta no DOD - Documento de Oficialização da Demanda, qual seja a contratação de prestação de serviço, **sob demanda**, de emissão de Certificados Digitais Internacionais do Tipo SSL para os sistemas que estão na DMZ da rede PR, para que sejam reconhecidos internacionalmente e validados por padrão nos navegadores Web Internet Explorer, Google Chrome, Mozilla Firefox e Safari, e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais nas últimas versões dos respectivos navegadores.

3. Descrição da necessidade

Contratação de prestação de serviço, **sob demanda**, de emissão de Certificados Digitais Internacionais do Tipo SSL para os sistemas que estão na DMZ da rede PR, de acordo com as especificações técnicas descritas no Termo de Referência, visando o atendimento das necessidades da Autoridade Certificadora da Presidência da República (AC PR) vinculada à Diretoria de Tecnologia da Secretaria Especial de Administração da Secretaria-Geral da Presidência da República (DITEC/SA/SG/PR).

4. Área requisitante

Área Requisitante	Responsável
DITEC/SA	Carlos Augusto Pissutti
ACPR/DITEC/SA	Gustavo Adriane de Carvalho Freire

5. Necessidades de Negócio

A DITEC, no cumprimento de sua missão institucional, dentre outras competências, provê o fornecimento de Certificados Digitais do Tipo A1, com validade de 01 (um) ano, para Equipamento/Aplicação para os servidores de domínio da Presidência da República, visando comprovar a autenticidade e confidencialidade das informações trafegadas.

Atualmente, o fornecimento supracitado é feito através de certificados digitais da cadeia de certificação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), emitidos pela Autoridade de Registro (AR) vinculada à Autoridade Certificadora da Presidência da República (AC PR) por meio da contratação do Serviço Federal de Processamento de Dados (SERPRO), Contrato 70/2019.

Entretanto, apesar da cadeia v10 ICP-Brasil (Raiz e AC-Final) possuírem o selo Webtrust, *não é possível o reconhecimento internacional e automático por parte dos navegadores*, fazendo com que o usuário receba as mensagens de **“esta conexão não é confiável”** ou **“o certificado de segurança do site não é confiável”**.

Esta situação prejudica a experiência dos usuários que acessam domínios da rede da Presidência da República, exigindo procedimentos adicionais e específicos para proceder à navegação, ou até, impedindo sua navegação, além de causar danos à imagem institucional deste órgão, por estar constantemente diante de um potencial incidente de segurança.

Apesar da tratativa de inclusão da cadeia v10 ICP-Brasil nos repositórios de confiança dos navegadores Web estar em curso, com um esforço participativo do SERPRO e do Instituto Nacional de Tecnologia da Informação (ITI), a contratação de prestação de serviço de emissão de Certificados Digitais Internacionais do Tipo SSL, sob demanda, é indispensável para o reconhecimento internacional e nativo pelos principais navegadores e dispositivos móveis, celulares e tablets compatíveis com IOS e Android.

6. Necessidades Tecnológicas

Os Certificados Digitais Internacionais SSL, a serem emitidos sob demanda para os sistemas que estão na DMZ da rede PR, deverão:

1. Ser emitidos por uma Autoridade Certificadora (AC) que possua o selo Webtrust válido, que esteja associada ao CA Browser Forum - Certification Authority Browser Forum e que seja reconhecida internacionalmente e automaticamente pelos navegadores Web Internet Explorer, Google Chrome, Mozilla Firefox e Safari, e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais nos repositórios de confiança das últimas versões dos respectivos navegadores e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android;
2. Ser aderentes aos requisitos de Certificate Transparency (CT), exigidos por navegadores do mercado; e
3. Permitir ao usuário final conferir a autenticidade do site/domínio em que navega e comunicar-se por meio de um canal seguro e protegido (baseado em SSL) utilizando tecnologia de criptografia.

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

Além dos requisitos tecnológicos, os certificados a serem emitidos, deverão ainda atender aos seguintes requisitos:

1. Fazer a validação do domínio e verificação das informações da organização;
2. Apresentar os dados sobre a empresa portadora do domínio, ou seja, prover a validação do domínio;
3. Possuir criptografia SHA de 256 bits e chave RSA de 2048 bits;
4. Ser compatível com todos os servidores Web que suportem os protocolos SSL e TLS, como, por exemplo, o Windows Server e Linux Red Hat;
5. Constar na lista de certificados confiáveis da versão mais recente do sistema operacional IOS, conforme lista disponível na URL <https://support.apple.com/pt-br/HT212140>;

8. Estimativa da demanda - quantidade de bens e serviços

Na DMZ da rede PR, constam 54 sistemas que necessitam de Certificados Digitais Internacionais do Tipo SSL para estes sejam reconhecidos internacionalmente e validados por padrão nos navegadores Web Internet Explorer, Google Chrome, Mozilla Firefox e Safari, e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais nas últimas versões dos respectivos navegadores.

Abaixo, os certificados digitais internacionais do tipo SSL a serem emitidos:

Item	Descrição	Descrição detalhada	Quantidade
		Emissão de Certificado digital internacional SSL do tipo OV com validade de 1 (um) ano, para um	

1	Certificado SSL OV de domínio único	domínio, com criptografia SHA de 256 bits e chave RSA de 2048 bits e com selo Webtrust válido.	20
2	Certificado SSL OV Multidomínios	Emissão de Certificado digital internacional SSL do tipo OV com validade de 1 (um) ano, para vários domínios, com criptografia SHA de 256 bits e chave RSA de 2048 bits e com selo Webtrust válido.	5
3	Certificado SSL OV WildCard	Emissão de Certificado digital internacional SSL do tipo OV com validade de 1 (um) ano, para um domínio e utilizado para uma quantidade ilimitada de subdomínios vinculados ao domínio principal, com criptografia SHA de 256 bits e chave RSA de 2048 bits e com selo Webtrust válido.	10

Os certificados supracitados serão emitidos pelos Agentes de Registro (AGR) da Autoridade de Registro (AR) vinculada à Autoridade Certificadora da Presidência da República (AC PR) e utilizados sob demanda, **não havendo obrigatoriedade de realização total ou de parte do estimado.**

9. Levantamento de soluções

Solução 1: Certificado ICP-Brasil

A Presidência da República possui um contrato com a empresa SERPRO para a prestação de serviços de emissão de Certificados Digitais de Equipamento A1 do Tipo SSL sob a cadeia de certificação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Solução 2: Certificado Internacional SSL

Contratação de prestação de serviços de emissão de Certificados Digitais Internacionais do Tipo SSL, sob demanda, atendida por uma Autoridade Certificadora (AC) com selo Webtrust válido, associada ao CA Browser Forum - Certification Authority Browser Forum, reconhecida internacionalmente e por padrão pelos principais navegadores Web e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android.

10. Análise comparativa de soluções

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
A Solução possui criptografia SHA de 256 bits e chave RSA de 2048 bits?	Solução 1	X		
	Solução 2	X		
A Solução possui selo Webtrust válido?	Solução 1	X		
	Solução 2	X		
A Solução consta na lista de certificados confiáveis da versão mais recente do sistema operacional IOS, conforme lista disponível na URL https://support.apple.com/pt-br/HT212140 ?	Solução 1		X	
	Solução 2	X		
A Solução é reconhecida internacionalmente e automaticamente pelos principais navegadores Web e dispositivos móveis, celulares e tablets compatíveis com IOS e Android?	Solução 1		X	
	Solução 2	X		
A Solução disponibiliza plataforma à Autoridade Certificadora da Presidência da República (AC PR) para emissão e gerenciamento dos certificados pelos Agentes de Registro da Autoridade de Registro (AR) vinculada à AC PR?	Solução 1	X		
	Solução 2	X		

11. Registro de soluções consideradas inviáveis

A Presidência da República possui um contrato (nº 70/2019) com a empresa SERPRO para a prestação de serviços de emissão de Certificados Digitais, porém, os certificados digitais de Equipamento A1 do Tipo SSL são emitidos sob a cadeia de certificação v10 da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil (Raiz e AC-Final), que apesar de possuir o selo Webtrust válido, não é possível o reconhecimento internacional e automático desta cadeia de certificação pelos principais navegadores e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android.

12. Análise comparativa de custos (TCO)

Não se aplica, uma vez que só existe uma solução viável tecnicamente: **Solução 2: Certificado Internacional SSL**

13. Descrição da solução de TIC a ser contratada

Contratação de prestação de serviços, sob demanda, de emissão de Certificados Digitais Internacionais do Tipo SSL para os sistemas que estão na DMZ da rede PR, para que sejam reconhecidos internacionalmente e validados por padrão nos navegadores Web Internet Explorer, Google Chrome, Mozilla Firefox e Safari, e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais nas últimas versões dos respectivos navegadores.

14. Estimativa de custo total da contratação

Valor (R\$): 27.047,60

Valor estimado em conformidade com a tabela abaixo:

Item	Descrição	Quantidade	Unidade	Preço Unitário Referência (R\$)	Valor Total (R\$)
1	Certificado SSL OV de domínio único	20	Certificado	R\$ 617,58	R\$ 12.351,60
2	Certificado SSL OV Multidomínios	5	Certificado	R\$ 602,00	R\$ 3.010,00
3	Certificado SSL OV WildCard	10	Certificado	R\$ 1.168,60	R\$ 11.686,00

Os certificados supracitados serão emitidos pelos Agentes de Registro (AGR) da Autoridade de Registro (AR) vinculada à Autoridade Certificadora da Presidência da República (AC PR) e utilizados sob demanda, **não havendo obrigatoriedade de realização total ou de parte do estimado.**

O detalhamento das pesquisas de preços se encontra na Planilha de Comparação de Preços.

15. Justificativa técnica da escolha da solução

A demanda para a contratação de prestação de serviços de emissão de Certificados Digitais Internacionais do Tipo SSL, com validade de 01 (um) ano, sob demanda, **só pode ser atendida** por uma Autoridade Certificadora (AC) com Raiz Internacional, que possua o selo WebTrust válido e que tenha o reconhecimento internacional e automático da sua cadeia de certificação pelos principais navegadores e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android.

16. Justificativa econômica da escolha da solução

Não se aplica, tendo em vista que é a única solução que atende a todos os requisitos.

17. Benefícios a serem alcançados com a contratação

Manter o serviço de emissão de Certificado Digital Internacional do Tipo SSL, com validade de 01 (um) ano, para os sistemas que estão na DMZ da rede PR, permitindo:

1. O reconhecimento internacional e validação por padrão nos navegadores Web Internet Explorer, Google Chrome, Mozilla Firefox e Safari, e em dispositivos móveis, celulares e tablets compatíveis com IOS e Android, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais nas últimas versões dos respectivos navegadores.
2. Que aplicativos cliente/servidor possam trocar informações com segurança, garantindo a confidencialidade e integridade do conteúdo que trafega na Internet.
3. Ao usuário conferir a autenticidade do site em que navega e comunicar-se por meio de um canal seguro e protegido (baseado em SSL) utilizando tecnologia de criptografia.
4. Aumentar a relação de confiança.
5. Obter mais segurança de dados.
6. Garantir ao usuário que o site é seguro e que o certificado é confiável, sem a necessidade de qualquer configuração manual por parte do usuário, uma vez que o certificado SSL Internacional é compatível com todos os principais navegadores e dispositivos móveis.

18. Providências a serem Adotadas

Não há providências a serem adotadas, uma vez que os Agentes de Registro (AGR) da Autoridade de Registro (AR) vinculada à Autoridade Certificadora da Presidência da República (AC PR), detém capacitação de cursos e experiências na atividade de emissão e gerenciamento dos respectivos certificados a serem adquiridos.

19. Assinaturas

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 122, de 13 de maio de 2022.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
<hr/>	<hr/>
STHEFANO GIOVANNY LOBATO BENATHAR	GUSTAVO ADRIANE DE CARVALHO FREIRE
Matrícula/SIAPE: 3278960	Matrícula/SIAPE: 3516914
Brasília, 17 de janeiro de 2023	Brasília, 17 de janeiro de 2023

20. Aprovação e Declaração de Conformidade

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC

CARLOS AUGUSTO PISSUTTI

Matrícula/SIAPE: 2321304

Brasília, 17 de janeiro de 2023

21. Declaração de Viabilidade

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

21.1. Justificativa da Viabilidade

Esta equipe de planejamento declara viável esta contratação, considerando os aspectos de relevância da demanda para atendimento das demandas de emissão de certificados digitais internacionais SSL para os sistemas que estão na DMZ da Rede PR.

22. Responsáveis

STHEFANO GIOVANNY LOBATO BENTHAR

Assistente Militar / Integrante Técnico

GUSTAVO ADRIANE DE CARVALHO FREIRE

Assessor Técnico / Integrante Requisitante

CARLOS AUGUSTO PISSUTTI

Diretor de Tecnologia