Estudo Técnico Preliminar para a Solução de Certificação Digital

Instituto Brasileiro de Meio Ambiente e dos Recursos Naturais Renováveis – Ibama

Janeiro de 2013

Sumário

1 – Introdução

Este documento apresenta o estudo técnico preliminar, que constitui primeira etapa do planejamento de uma contratação (planejamento preliminar) e serve essencialmente para assegurar a viabilidade técnica da contratação e embasar o termo de referência ou o projeto básico, conforme previsto na Lei 8.666/1993, art. 6º, inciso IX.

A estrutura deste documento baseia-se nas orientações constantes do Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação V1.0 (GCSTI), publicado pelo Tribunal de Contas da União, e por conseguinte encontra-se respaldo no arcabouço técnico legal acerca das contrações de bens e serviços de Tecnologia da Informação.

2 – Necessidade da contratação[1]

Os sistemas de informação do IBAMA são providos aos cidadãos por meio da internet. A utilização deste meio de comunicação requer um mecanismo de segurança, denominado certificação digital, que assegure a autenticidade, confiabilidade, integridade e validade jurídica de documentos e informações em forma eletrônica.

Segundo o Instituto Nacional de Tecnologia da Informação – ITI[2], a Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. Esta tecnologia baseia-se na existência de Certificados Digitais, que são "documentos de identificação" eletrônicos. Eles são emitidos por uma Autoridade Certificadora, que é uma entidade considerada confiável pelas partes envolvidas numa comunicação e/ou negociação.

Em face de vulnerabilidades detectadas pelo Comitê de Segurança da Informação e Informática do IBAMA – CSII, instituído por meio da Portaria IBAMA nº 1.098, de 5 de agosto de 2011, a Gestora do CSII solicitou via memorando[3] a implantação urgente da certificação digital para todos os serviços on-line do IBAMA.

Tal medida visa atender as recomendações de aprimoramento da segurança da informação exaradas pelo: Acórdão TCU n° 309/2009 – Plenário, fruto da realização de auditoria operacional a fim de avaliar a nova a sistemática de controle no trânsito de produtos florestais introduzida pelo sistema DOF quanto à sua efetividade, segurança, fidedignidade dos dados e prevenção de fraudes; e Acórdão TCU n° 605/2011 – Plenário, cujo objetivo foi avaliar os riscos no exercício da atividade institucional do Ibama para o alcance de seus resultados.

A implementação da certificação digital nos sistemas de informação e nos portais do IBAMA é uma das ações de segurança necessária para a implantação da Política de Segurança da Informação, Informática e Comunicações do IBAMA – POSIC[4].

---

1 Segundo o GCSTI/TCU, a necessidade da contratação é a justificativa da contratação da solução de TI, decorrente da necessidade de atender a uma demanda do negócio.

2 Fonte: Cartilha – Certificação Digital: entenda e utilize, disponível em: http://www.iti.gov.br/index.php/publicacoes/cartilhas/3893-certificacao-digital-entenda-e-utilize, acessado em 17/10/2012.

3 Memorando n° 81/2012 COINF/CGFIS/DIPRO, apenso à folha n° 2 do processo n° 02001.001830/2012-11.

4 Publicada no DOU de 06/06/2012 (nº 109, Seção 1, pág. 151).

3 – Alinhamento entre a contratação e os planos do órgão governante superior, do órgão e de TI do órgão[5]

A necessidade da presente contratação encontra-se registrada no Plano Diretor de Tecnologia da Informação (PDTI) 2010-2011, 2ª Edição, por meio da Ficha CNT n° 03, Grupo b2, GUT 250, aprovada pelo Comitê de Tecnologia da Informação do IBAMA em 26 de outubro de 2010, e oficializada por intermédio do Documento de Oficialização de Demanda - DOD CNT n° 01/2012, apenso à folha n° 4 do processo n° 02001.001830/2012-11.

A necessidade de implementação de uma solução de certificação digital encontra amparo no Plano Estratégico Institucional, no âmbito do Objetivo Estratégico n° 5 – Implementar práticas de gestão do conhecimento e da informação como forma de melhoria dos processos de trabalho e da interação com os cidadãos, e da Meta n° 43 – Implementar política de segurança corporativa.

4 – Requisitos da contratação[6]

Visando garantir a segurança, confiabilidade e integridade nas transações executadas pela rede corporativa do IBAMA, a solução de certificação digital deverá ser composta de: Certificados digitais do tipo SSL (Secure Socket Layer) nos equipamentos servidores de aplicação (Aplications Servers); Certificados digitais do tipo e-CPF; e Mídias criptográficas (Tokens criptográficos) para armazenamento dos certificados digitais.

4.1 Requisitos Internos Funcionais

Os certificados digitais do tipo SSL para autenticação de Servidores Web do IBAMA, deverão possuir as seguintes características e funcionalidades mínimas:

ID	CARACTERÍSTICA/FUNCIONALIDADE
01	Ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil;
02	Ser aderente às normas do Comitê Gestor da ICP-Brasil;
03	Ter certificado com codificação (criptografia) mínima de 128 bits;
04	Possuir compatibilidade com os navegadores web: Microsoft Internet Explorer a partir da versão 7 e Mozila Firefox a partir da versão 16;
05	Ser compatível com os sistemas operacionais Windows 2003, 2008 Server e Linux;
06	Ser compatível com servidores web que suportem os protocolos SSL, TLS e HTTPS;
07	Vir acompanhado de documentação técnica.

5 Segundo o GCSTI/TCU, o Alinhamento entre a contratação e os planos do órgão governante superior, do órgão e de TI do órgão é a indicação exata do alinhamento da contratação com elementos dos planos estratégicos e de TI do órgão governante superior ao qual o órgão está vinculado (e.g. CNJ ou SLTI), dos planos do órgão (e.g. planos estratégicos e diretores) e de TI do órgão (e.g. PDTI), bem como com as metas do Plano Plurianual (PPA).

6 Segundo o GCSTI/TCU, os Requisitos da contratação são os requisitos que a solução contratada deverá atender, incluindo os requisitos mínimos de qualidade, de modo a possibilitar a seleção da proposta mais vantajosa mediante competição.

08	Incluir prestação de suporte remoto, via telefone, e-mail ou website, por equipe de técnicos especializados, para esclarecimento de dúvidas técnicas e cadastrais, tais como: geração do CSR, validação da solicitação de compra, instalação do certificado e selo do site seguro.
09	Garantia de reposição do Certificado ou a correção da solicitação pendente, em caso de constatação de erro técnico no CSR, no prazo máximo de 30 (trinta) dias após a emissão do mesmo.
10	Validade mínima de 01 (um) ano, contado a partir da data de sua emissão.

Tabela 1: Requisitos Funcionais dos Certificados do tipo SSL.

Os certificados digitais e-CPF deverão possuir as seguintes características mínimas:

ID	CARACTERÍSTICA/FUNCIONALIDADE
01	Ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil;
02	Permitir o armazenamento em dispositivo portátil do tipo Token.
03	Ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Fazenda, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros.
04	Conter nível: A3;
05	Ser compatível com os sistemas operacionais Windows XP, Windows Vista, Windows 7 e Linux;
06	Possuir compatibilidade com os navegadores web: Microsoft Internet Explorer a partir da versão 7 e Mozila Firefox a partir da versão 16;
07	Ser protegido por senha.
08	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 pelo CONTRATANTE. A CONTRATADA deverá manter central de atendimento para abertura de chamados pelo menos no horário das oito às dezoito horas, de segunda a sexta-feira, exceto feriados. A central deverá ser acionada por telefone ou pela internet.
09	Validade mínima de 3 (três) anos, contados a partir da data de sua emissão.
10	Ser emitido em Todas as capitais Brasileiras.

Tabela 2: Requisitos Funcionais do Certificado e-CPF.

As mídias criptográficas deverão possuir as seguintes características mínimas:

ID	CARACTERÍSTICA/FUNCIONALIDADE
01	Possuir numeração única para cada dispositivo;
02	Suportar os algoritmos RSA, MD5, SHA2, DES, 3DES e AES;
03	Deverá gerar chaves RSA de até 2048 bits (padrão ICP Brasil A3 e A4);
04	Deverá suportar a geração On-board de par de chaves RSA;
05	Deverá ser compatível com aplicações PKI;

06	Deverá suportar assinatura digital em Hardware;
07	Deverá suportar a geração de números aleatórios em hardware;
08	Deverá suportar gerenciamento através de PIN e PUK;
09	Seguir o padrão ISO 7816 partes 1, 2, 3, 4 e 8;
10	Atender aos requisitos da seção 4.7.2, do padrão FIPS 140-2, para a geração de chaves criptográficas;
11	As mídias destinadas ao armazenamento de certificados de nível de segurança 3 devem implementar a geração de chaves RSA com até 2048 bits;
12	Deverá possuir no mínimo Hardware com processador de 8 bits e memória de 32 Kb;
13	Deverá permitir o armazenamento de no mínimo 5 certificados com chaves RSA de tamanho 2048 bits;
14	Deverá ter conectividade compatível com USB 1.1/2.0;
15	Deverá possuir chassi em plástico rígido e resistente a água;
16	Deverá possuir software de gerenciamento ;
17	A solução deve ser compatível com as camadas de software definidas, para ambiente Microsoft por: Ambientes Windows 98, 98SE, 2000, XP, Vista, Windows 7 e versões superiores; suporte nativo para arquiteturas 32 bits e 64 bits para Windows Vista, Windows 7 e versões superiores; possuir biblioteca implementando a CryptoSPI do Microsoft Cryptographic Service Provider assinada pela Microsoft; possuir biblioteca implementando o padrão PKCS#11 e deve ser compatível com as bibliotecas NSS;
18	A solução deve ser compatível com as camadas de software definidas para ambiente Linux por: ambiente Linux kernel 2.4 e Linux kernel 2.6 versões estáveis; suporte nativo para arquiteturas 32 bits e 64 bits; possuir biblioteca implementando o padrão PKCS#11 e deve ser compatível com as bibliotecas OpenSSL e NSS.
19	Deverá possuir, no mínimo, as seguintes certificações: X.509 versão 3; ISO 7816 Compliant; PKCS#11 versão 2.20; Microsoft CryptoAPI (CAPI) 2.0; PC/SC versão 1.0 e SSL versão 3.
20	Plataformas suportadas (Sistemas Operacionais) : possuir driver disponíveis para o sistema operacional Linux kernel 2.4 e Linux kernel 2.6 versões estáveis; possuir driver disponíveis para o sistema operacional Microsoft Windows 98, 2000, XP, Vista 32 e 64 bits, Windows 7 32 e 64 bits e versões superiores.
21	Devem ser fornecidas mídias (CD-ROM) com todos os drives do dispositivo para as plataformas suportadas e/ou programas necessários à utilização e gerenciamento do token, guias de instalação e configuração, em Português (Brasil):
22	Permitir reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso;
23	Garantia de no mínimo 12 meses.

Tabela 3: Requisitos Funcionais da mídia criptográfica.

4.2 Requisitos Internos Não Funcionais

As soluções de certificação digital (tipo SSL ou tipo e-CPF) deverão ser aderentes ao padrão ICP-BRASIL.

O processo de emissão do certificado nas autoridades de registros deverá estar em conformidade com as orientações do Instituto Nacional de Tecnologia da Informação quanto aos procedimentos e documentação exigida.

4.3 Requisitos Externos

A presente contratação deve observar as seguintes leis e normas:

a) Lei n° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública.

b) Lei n° 10.520, de 17 de julho de 2002, que institui modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

c) Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação.

d) Decreto n° 3.555, de 08 de agosto de 2000, que aprova o regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

e) Decreto n° 5.450, de 31 de maio de 2005, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns.

f) Decreto n° 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal.

g) Instrução Normativa nº 04/2010 SLTI/MP nº, de 12 de novembro de 2010, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP).

h) Instrução Normativa nº 01/2010 SLTI/MP, 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.

i) Orientação Técnica n° 01 TiControle, de 12 de março de 2008, que dispõe sobre boas práticas para a estimativa de preços na contratação de bens e serviços de TI.

j) Política de Segurança do IBAMA – POSIC, publicada no Diário Oficial da União, em 06/06/2012, por meio da Portaria IBAMA nº 9/2012.

5) Relação entre a demanda prevista e a quantidade de cada item[7]

ID	ESPECIFICAÇÃO/ DESCRIÇÃO	QTDE	JUSTIFICATIVA DAS QUANTIDADES DOS ITENS DA SOLUÇÃO DE TI A CONTRATAR
1	Certificados Digitais SSL padrão ICP-Brasil	14	A estimativa do quantitativo das Certificações dos equipamentos servidores de rede via SSL baseou-se na quantidade de servidores de aplicação com capacidade de emitir o CSR[8] (*Certificate Signing Request*), quais sejam: 8 Servidores de Aplicação hospedados no Datacenter utilizado pelo IBAMA e 6 Servidores de Aplicação mantidos pelo Centro de Sensoriamento Remoto do IBAMA.
2	Certificados Digitais e-CPF A3	4300	O acesso seguro aos serviços eletrônicos da Rede Corporativa do IBAMA somente será garantido com a certificação digital de todos os usuários internos. Segundo a área de Recursos Humanos, esta estimativa de quantitativo, realizada em novembro de 2012, contempla os servidores ativos e os novos concursados para provimento dos cargos de técnicos e analista ambiental.

Tabela 4: Relação entre a demanda prevista e a quantidade da cada item.

6) Levantamento de mercado[9]

A solução de certificação digital consiste na emissão do certificado digital e no fornecimento das mídias criptográficas.

A emissão dos certificados digitais deverá ser providenciada por uma autoridade certificadora apta a emiti-la sob o padrão ICP-Brasil.

Segundo o Instituto Nacional de Tecnologia da Informação – ITI, uma autoridade certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Conforme lista das Autoridade Certificadoras divulgada pelo ITI, atualizado em 06 de dezembro de 2012, verifica-se que o mercado para emissão de certificados digitais com infraestrutura física e lógica e de recursos humanos para a prestação do serviço se restringe as seguintes empresas: SERASA S.A., CERTISIGN CERTIFICADORA DIGITAL S.A. e SERPRO.

---

7 Segundo o GSCTI/TCU, A relação entre a demanda prevista e a quantidade de cada item deve apresentar a justificativa das quantidades dos itens da solução de TI a contratar.

8 O CSR é um arquivo de texto criptografado, gerado pelo servidor web do seu site, contendo as informações para a solicitação do seu Certificado Digital. Este contém as informações da organização ou empresa, tais como: nome, departamento, cidade, estado, país; e a URL onde o certificado SSL será utilizado. *(Fonte: http://www.rapidssl.com.br/certificado-digital-ssl/gerar-csr.php)*

9 Segundo o GSCTI/TCU, O levantamento de Mercado consiste no levantamento para identificar quais soluções de TI existentes no mercado atendem aos requisitos estabelecidos.

Quanto à emissão de certificado digital do Tipo SSL, o serviço deve ser prestado na sede do Ibama em Brasília, deste modo as 3 (três empresas) estão aptas a prestá-lo. Entretanto quanto à emissão do certificado do tipo e-CPF, a dispersão geográfica das unidades do Ibama exige que a empresa emissora possua uma capilaridade em nível nacional.

Em consulta à rede de postos de atendimento da empresa SERASA S.A[10], observou-se que a rede de atendimento abrange apenas 24 estados brasileiros. A empresa CERTISIGN CERTIFICADORA DIGITAL S.A apresenta, conforme seu sítio[11] eletrônico, cobertura aos 27 estados brasileiros, por meio de pessoas jurídicas de direito privado distintas. O SERPRO apresenta, conforme seu sítio[12] eletrônico, cobertura em nível nacional por meio de regionais e escritórios e ainda por meio de autoridade de registro distinta.

O fornecimento de mídias criptográficas possui um mercado amplo de empresas aptas a distribuição deste tipo de hardware. Desse modo, em face desta característica e com o advento da iniciativa de Contratação Conjunta disponibilizada pelo Ministério do Planejamento Orçamento e Gestão, o Ibama oficializou junto a este ministério a participação no processo de contratação conjunta para a aquisição de Tokens Criptográfico, que foi realizado em 05/12/2012, por meio do Pregão Eletrônico por Registro de Preços nº 59/2012, promovido pelo Ministério do Planejamento, Orçamento e Gestão – MP.

O levantamento de mercado permitiu as seguintes conclusões acerca do objeto a ser contratado: A solução é passível de parcelamento, incluindo a vantagem do ganho de escala por meio da participação da contratação conjunta em um dos itens. Quanto à emissão dos certificados, o mercado mostra-se reduzido por natureza do tipo de serviço prestado. Esta característica se assevera quando se confronta à exigência da emissão do certificado do tipo e-cpf em âmbito nacional. Entretanto, quanto à certificação dos servidores de aplicação a ser realizada na sede do IBAMA, todas as autoridades certificadoras são capazes de prestar o serviço.

7) Justificativas da escolha do tipo de solução a contratar[13]

As justificativas da escolha do tipo de solução a contratar consistem na demonstração de que o tipo de solução escolhido pela equipe de planejamento da contratação, com base no levantamento de mercado, é o que mais se aproxima dos requisitos definidos e que mais promove a competição, levando-se em conta os aspectos de economicidade, eficácia, eficiência e padronização, bem como práticas de mercado.

A presente aquisição visa atender a necessidade de utilização de certificados digitais SSL (Secure Socket Layer) para autenticação de equipamentos servidores da Rede Corporativa do IBAMA, de certificados digitais e-CPF para autenticação pessoal e de uso pelos titulares do corpo gerencial e gestores de contratos administrativos e servidores do IBAMA e de tokens para o armazenamento dos certificados tipo e-CPF.

A necessidade da certificação SSL é prover acesso seguro aos serviços eletrônicos da Rede Corporativa do IBAMA para os usuários internos (servidores e colaboradores) e externos

10 Consulta ao endereço: http://requisicao.certificadodigital.com.br/agendacliente/ControllerServlet?id_fluxo_tela=15, em 19/12/2012.

11 Consulta ao endereço: http://www.certisign.com.br/certisign/telefones-enderecos, em 19/12/2012.

12 Consulta ao endereço: http://www4.serpro.gov.br/imprensa/publicacoes/tema-1/antigas%20temas/tema-200/materias/escritorios-serpro, em 20/12/2012

13 Segundo o GSCTI/TCU, Justificativas da escolha do tipo de solução a contratar é a demonstração de que o tipo de solução escolhido é o que mais se aproxima dos requisitos definidos e que mais promove a competição, levando-se em conta os aspectos de economicidade, eficácia e eficiência.

(clientes e outros), garantindo dessa forma que os mesmos tenham acesso aos sítios originais do IBAMA, na Internet, e possam navegar com total tranquilidade, fazendo consulta à dados íntegros e confiáveis. Dentre os serviços disponibilizados que terão seus acessos protegidos, destacamos os serviços de acesso ao Sistema DOF, ao Licenciamento Ambiental e ao Cadastro Técnico Federal, e mais recentemente, o serviço de acesso ao Cadastro Ambiental Rural – CAR, em parceria com o MMA e ICMBio.

Verifica-se também, a necessidade de uso de certificados e-CPF para acesso aos Sistemas de Informação do IBAMA e da Administração Pública Federal. Esse tipo de certificado tem como objetivo confirmar se o usuário é exatamente aquele quem diz ser e se está autorizado a executar as transações eletrônicas. Na realidade, é a sua assinatura digital, sendo largamente utilizada para assegurar a integridade, confidencialidade e autenticidade da transação eletrônica. O tipo A3 de certificado, aquele armazenado em uma mídia móvel, mostrou-se mais adequado por permitir a mobilidade dos servidores, em especial do corpo gerencial, fiscais e servidores cujas atividades são realizadas em estações de trabalhos distintas.

Registra-se ainda, a necessidade de aquisição de tokens para o armazenamento dos certificados digitais e-CPF, como dito acima. O token é um hardware dotado de um chip criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas, estas chaves estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do token sem que o mesmo seja formatado, além de protegê-las de riscos, como roubo ou violação.

8) Estimativas preliminares dos preços

ID	ESPECIFICAÇÃO/ DESCRIÇÃO	UNID. MEDIDA	QTDE.	VALOR UNITÁRIO	PRAZO DE VALIDADE
1	**TRIBUNAL DE CONTAS DA UNIÃO – TCU (Pregão Eletrônico n.º 43/2011 – SRP)**	Unidade	2500	R$ 119,90	(3) três anos.
2	**Empresa CertSign (Proposta Comercial)**	Unidade	4300	R$ 148,50	(3) três anos.
3	**SERPRO (Proposta Comercial)**	Unidade	4300	R$ 111,39	(3) três anos.
Valor Médio				**R$ 126,60**	

Tabela 5: Estimativa de Preço - Emissão de Certificação Digital do tipo e-CPF (A3).

ID	ESPECIFICAÇÃO/ DESCRIÇÃO	UNID. MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL	PRAZO DE VALIDADE
1	**TRIBUNAL DE CONTAS DA UNIÃO – TCU (Pregão Eletrônico n.º 43/2011 – SRP)**	Unidade	2500	R$ 32,00	R$ 80.000,00	(3) três anos.
2	**TRIBUNAL REGIONAL ELEITORAL DE RORAIMA (Pregão Eletrônico N.º 46/2012)**	Unidade	150	R$ 94,67	R$ 14.200,50	(3) três anos.
3	**MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO – MP (Pregão Eletrônico n.º 59/2012 – SRP)**	Unidade	94375	R$ 19,69	R$ 1.858.243,75	(3) três anos.
4	**Tribunal Regional Federal da Quarta Região (Pregão nº 12/2012)**	Unidade	348	R$ 29,00	R$ 10.092,00	(3) três anos.
5	**DIGITAL SAFE DO BRASIL (Proposta Comercial)**	Unidade	4300	R$ 84,00	R$ 361.200,00	(3) três anos.
TOTAL				**R$ 51,87**		

Tabela 6: Mídia Criptográfica.

ID	ESPECIFICAÇÃO/ DESCRIÇÃO	UNID. MEDIDA	QTDE.	VALOR UNITÁRIO	VALOR TOTAL	PRAZO DE VALIDADE
1	**SERASA S.A.**	Unidade	12	R$ 1.890,00	R$ 22.680,00	(1) um ano.
2	**STRONGSECURITY**	Unidade	12	R$ 1.500,00	R$ 18.000,00	(1) um ano.
3	**Agência Estadual de Tecnologia da Informação – ATI Pregão Eletrônico N.º 019/2010**[14]	Unidade	38	R$ 2.681,17	R$ 101.884,46	(1) um ano.
TOTAL				**R$ 2.023,72**		

Tabela 7: Emissão de Certificado do tipo SSL.

9) Descrição da Solução de TI como um todo

A solução de certificação Digital envolve a aquisição e instalação de certificados digitais SSL (Secure Socket Layer) para autenticação de equipamentos servidores da Rede Corporativa do IBAMA, a aquisição e mídias criptográficas, a contratação do serviço de emissão do certificado digital e-CPF A3 para autenticação pessoal e de uso pelos titulares do corpo gerencial e gestores de contratos administrativos e servidores do IBAMA.

10) Justificativas para o parcelamento ou não da solução

O IBAMA adotou o parcelamento do objeto, conforme preconiza o Art. 23, §1º da lei nº 8.666/1993, os Acórdãos do TCU nº 1.331/2003, nº 1.327/2006, nº 111/2011 (específico ao IBAMA), Súmula nº 247-TCU e inciso I do Art. 5º da IN nº 04/2010 SLTI/MPOG, que

14 Disponível em: http://www2.ati.pe.gov.br/c/document_library/get_file?p_l_id=46076&folderId=56454&name=DLFE-8515.pdf , acesso 20/12/2012.

assegura o alcance dos resultados de forma eficiente, uma vez que utiliza o pagamento por produto entregue, atendidos os critérios de qualidade.

Os serviços contratados devem ser divididos em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, tendo em vista o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade. Além disso, no âmbito da contratação de soluções de TI, é vedada a contratação de mais de uma solução de TI em um único contrato.

Diante do exposto, a solução admite o seguinte parcelamento:

ID	ITEM	JUSTIFICATIVA
1	Emissão de 14 Certificados Digitais SSL padrão ICP-Brasil	O levantamento de mercado evidenciou que a emissão deste tipo de certificado nas máquinas situadas na Sede do Ibama pode ser feita pelas Autoridades Certificadoras, bem como por Autoridades de Registro. Portanto, com vistas a garantir a ampliação competitividade, o pregão eletrônico para este item, classificado como de natureza comum, é o mais adequado. A separação deste serviço do restante da solução não compromete os resultados esperados pelo todo da solução.
2	Emissão de 4300 Certificados Digitais e-CPF A3	O levantamento de mercado e a estimativa preliminar de preços evidenciou que a solução proposta pelo SERPRO é a mais adequada, uma vez que tal empresa possui a capilaridade geográfica necessária para a emissão dos certificados em âmbito nacional, além de apresentar o menor valor, assegurando a economicidade da solução. A emissão dos certificados e-CPF é passível de separação desde que o Token possua as características mínimas descritas.
3	Aquisição de 4300 mídias criptográficas (Tokens)	A aquisição de tokens criptográficos por meio da participação na contratação conjunta promovida pelo Ministério do Planejamento apresentou-se como opção mais adequada em termos econômicos devido a escala da contratação, assegurando-se a qualidade das mídias adquiridas.

11) Resultados pretendidos[15]

Conforme informações do Centro Nacional de Telemática e do Comitê de segurança da informação e Informática do IBAMA, a solução deverá permitir o alcance dos seguintes resultados:

Id	Resultados pretendidos
1	Assegurar a autenticidade, confiabilidade e integridade das informações providas pelos sistemas corporativos via portais intranet e internet do IBAMA.
2	Garantir acesso seguro às informações armazenadas nas bases de dados do IBAMA.
3	Garantir a autenticidade e confiabilidade das transações executas pelo corpo gerencial e gestores do IBAMA.
4	Garantir a segurança das informações trafegadas entre o IBAMA e clientes externos.

Tabela 8: Tabela de Resultados a serem alcançados.

12) Providências para adequação do ambiente do órgão

O uso da certificação digital nos sistemas de informação requer, além da aquisição dos certificados digitais e respectiva mídia (token), a adaptação dos sistemas de informação que

15 Os resultados pretendidos são os benefícios diretos que o órgão almeja com a contratação da solução, em termos de economicidade, eficácia, eficiência, de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis.

utilizarão em seu processo de autenticação de usuário a opção de uso do certificado digital, seja para acessar o sistemas, seja para acionar determinada funcionalidade.

A adaptação dos sistemas não será objeto desta solução, uma vez que já está em curso por meio de ordens de serviço na fábrica de software (contrato n° 22/2011).

O processo de Certificação dos servidores deverá ser precedido de ampla divulgação dos procedimentos que deverá ser promovida pela DIPLAN, em especial junto aos servidores lotados nas Unidades Descentralizadas.

13) Análise de risco

13.1. Riscos do Processo de Contratação

Risco 1	Risco:	Não aprovação do Estudo Técnico ou do Termo de Referência.			
	Probabilidade:	média	Id	Dano potencial	
			1	Atraso no processo de contratação e, consequentemente, atraso no fornecimento da solução.	
	Id	Ação Preventiva			Responsável
	1	Instruir o Estudo Técnico e o Termo de Referência em estrita aderência à Instrução Normativa n° 04/2010 e ao Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação do TCU.			Equipe de Planejamento da Contratação
	Id	Ação de Contingência			Responsável
	1	Exposição do arcabouço legal em que a contratação de serviços de TI deva seguir.			Integrante Técnico

Tabela 9: Riscos do processo de contratação.

13.2. Riscos da Solução de Tecnologia da Informação

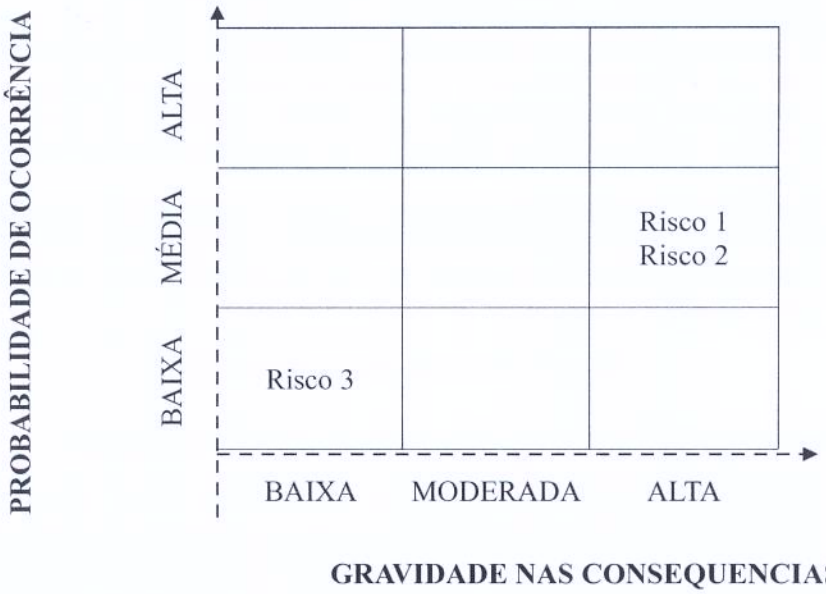
Risco 2	Risco:	Resistência a mudança por parte do corpo gerencial, gestores e servidores do IBAMA quanto da utilização da certificação digital.			
	Probabilidade:	média	Id	Dano potencial	
			1	Comprometimento da segurança das transações na Rede Corporativa do IBAMA	
	Id	Ação Preventiva			Responsável
	1	Conscientização dos titulares e substitutos do corpo gerencial, gestores e servidores do IBAMA na utilização da certificação digital.			Integrante Técnico
	Id	Ação de Contingência			Responsável
	1	Exposição aos titulares e substitutos do corpo gerencial, gestores e servidores do IBAMA do risco da não utilização da certificação digital.			Integrante Técnico
Risco 3	Risco:	Quantidade de certificados insuficientes			
	Probabilidade:	baixa	Id	Dano potencial	

			1	Impossibilidades do uso do serviço por alguns servidores, principalmente, das unidades descentralizadas.
	Id	Ação Preventiva		Responsável
	1	Confirmar com o Integrante Requisitante a quantidade demandada de certificações digitais, se esta será suficiente.		Equipe de Planejamento da Contratação
	Id	Ação de Contingência		Responsável
	1	Retornar ao Estudo Técnico e verificar a solução adequada.		Equipe de Planejamento da Contratação

Riscos da solução de Tecnologia da Informação.

13.3. Avaliação Qualitativa dos Riscos

A seguir encontra-se a matriz de avaliação qualitativa dos riscos identificados.



Através da matriz, percebe-se que o risco de maior probabilidade e gravidade é o Risco 1 (Não aprovação do Estudo Técnico ou do Termo de Referência) e o Risco 2 (Resistência a mudança por parte do corpo gerencial, gestores e servidores do IBAMA quanto da utilização da certificação digital) cujas ocorrências dos eventos associados a estes riscos poderão comprometer o resultado da contratação. Desse modo estes riscos deverão ser mitigados por meio das ações de prevenção registradas neste documento. O Risco 3 será assumido em virtude da baixa probabilidade e gravidade.

14) Declaração da viabilidade ou não da contratação

Os estudos preliminares evidenciaram que a forma de contratação que maximiza a probabilidade do alcance dos resultados pretendidos com a mitigação dos riscos e observância dos princípios da economicidade, eficácia e eficiência apresenta-se a seguir:

a) Realização de processo licitatório com vistas a adquirir 14 certificados digitais do Tipo SSL;

b) Aquisição via contratação conjunta de 4300 mídias criptográficas (Tokens);

c) Contratação da emissão de 4300 certificados digitais do tipo e-CPF junto ao Serviço Federal de Processamento de Dados (SERPRO);

d) Adequação dos sistemas de informação via emissão de ordem de serviço específica junto à fábrica de software (Contrato n° 22/2011).

Diante do exposto, a equipe de planejamento declara ser viável a contratação da solução pretendida.

Brasília - DF, 16 de Janeiro de 2013.

Márcio Pereira Lima
Matrícula SIAPE nº 1816137
ATI - MPOG

Cristiano Jorge Poubel de Castro
Matrícula SIAPE nº 1243346
ATI – MPOG

Cleia dos Santos de Oliveira
Matrícula SIAPE nº 686116
Técnico Administrativo

Nelson Gonçalves Rezende
Matrícula SIAPE nº 686325
Técnico Administrativo

De acordo,

Brasília - DF, 16 de janeiro de 2013.

Rosana de Souza Ribeiro
Chefe do Centro Nacional de Telemática