ANEXO II – Arquitetura Tecnológica

ANEXO II - Requisitos Tecnológicos da Solução de TIC		
ID	**Descrição**	**Detalhamento dos Requisitos**
1	Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, **SEM fornecimento de dispositivo físico de armazenamento - RENOVAÇÃO**, com validade por 3 anos.	1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 1.2. Nível: A3. 1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 1.5. Tipo: e-CPF. 1.6. 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, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios, entre outros. 1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, SIAPENET, Compras, SIORG, SIGEPE, entre outros). **1.8. Os certificados digitais deverão ser compatíveis com os tokens modelo: Token Epass 2003, Token StarSign USB – G&D Burti, StarSign Crypto – USB-Token S, SafeNet iKey 2032 e SafeNet Token 5100/5110, já existentes no IFS**.
2	Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, **COM fornecimento de token criptográfico para armazenamento do certificado**, com validade por 3 anos.	**2.1. Certificado** 2.1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 2.1.2. Nível: A3. 2.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 2.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 2.1.5. Tipo: e-CPF. 2.1.6. 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, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros. 2.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal

		(SCDP, SIAFI, SIAPENET, Compras, SIORG, SIGEPE, entre outros). **2.2. Dispositivo Físico de armazenamento** 2.2.1. Dispositivo Físico de armazenamento (token criptográfico), em modelo homologado conforme padrão ICP-Brasil e constante na lista de homologação atual disponível no site do Instituto Nacional de Tecnologia da Informação (ITI); 2.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 2.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior. 2.2.4. Ser aderente às normas do Comitê Gestor da ICP-Brasil. 2.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2. 2.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes. 2.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas. 2.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3). 2.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas. 2.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório. 2.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits. 2.2.12. Possuir carcaça resistente à água e à violação. 2.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores). 2.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores). 2.2.15. Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da Microsoft (Windows 2000 e versões superiores). 2.2.16. Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente. 2.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio

		dos frameworks Java JCA e Java JCE. 2.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4. 2.2.18. Possuir indicador luminoso de estado do dispositivo. 2.2.19. Assinar dados digitalmente em até 10 (dez) segundos. 2.2.20. O token criptográfico deverá possuir certificação do INMETRO. 2.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura. **2.3. Funcionalidades** 2.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores. 2.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label). 2.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres. 2.3.4. Permitir criação de senhas com caracteres alfanuméricos. 2.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos. 2.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459. 2.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo. 2.3.8. Permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key). 2.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). 2.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. 2.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores). 2.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo. 2.3.13. Implementar mecanismo de autenticação tipo challenge-response. 2.3.14. Forçar a troca da senha padrão no primeiro acesso.

ANEXO II – Arquitetura Tecnológica

		2.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos. 2.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida. 2.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. **2.4. Software** 2.4.1. Características do software de gerenciamento do dispositivo, no idioma português do Brasil, que permita: 2.4.1.1. gerenciamento do dispositivo; 2.4.1.2. exportação de certificados armazenados no dispositivo; 2.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; 2.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; 2.4.1.5. visualização de certificados armazenados no dispositivo; 2.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; 2.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso. 2.4.2. Deverá ser disponibilizado portal para download de drivers/softwares de forma ilimitada e gratuita. 2.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.
3	Emissão de e-CPF A3 - Certificado Digital EM NUVEM ICP Brasil para Pessoas Físicas, com 3 anos de validade.	3.1 Ser aderente às normas do Comitê Gestor da ICP-Brasil; 3.2 Compatível com certificados digitais gerados pelas autoridades certificadoras ICP-Brasil; 3.3 A solução deve ser compatível com as camadas de software definidas, para ambiente Microsoft por: Ambientes Windows 98, 98SE, 2000, XP, Vista, Windows 7, Windows 8, Windows 10 e versões superiores; Suporte nativo para arquiteturas 32 bits e 64 bits para Windows Vista, Windows 7, Windows 8, Windows 10 e versões superiores; 3.4 Possuir biblioteca implementando a CryptoSPI do Microsoft Cryptographic Service Provider assinada pela Microsoft; 3.5 Possuir biblioteca implementando o padrão PKCS#11; 3.6 Deve ser compatível com as bibliotecas NSS; 3.7 Deve ser fornecida documentação específica para cada plataforma bem como suporte técnico;

ANEXO II – Arquitetura Tecnológica

		3.8 Deve ser fornecida correções de segurança e correção de bugs, pelo período mínimo de 3 anos, sem ônus adicional. 3.9 Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, SIAPENET, Compras, SIORG, SIGEPE, entre outros).
4	Emissão de e-CNPJ A3 – Certificado Digital **EM NUVEM** ICP Brasil, para Pessoas jurídicas, com 3 anos de validade	4.1 Ser aderente às normas do Comitê Gestor da ICP-Brasil; 4.2 Compatível com certificados digitais gerados pelas autoridades certificadoras ICP-Brasil; 4.3 A solução deve ser compatível com as camadas de software definidas, para ambiente Microsoft por: Ambientes Windows 98, 98SE, 2000, XP, Vista, Windows 7, Windows 8, Windows 10 e versões superiores; Suporte nativo para arquiteturas 32 bits e 64 bits para Windows Vista, Windows 7, Windows 8, Windows 10 e versões superiores; 4.4 Possuir biblioteca implementando a CryptoSPI do Microsoft Cryptographic Service Provider assinada pela Microsoft; 4.5 Possuir biblioteca implementando o padrão PKCS#11; 4.6 Deve ser compatível com as bibliotecas NSS; 4.7 Deve ser fornecida documentação específica para cada plataforma bem como suporte técnico; 4.8 Deve ser fornecida correções de segurança e correção de bugs, pelo período mínimo de 3 anos, sem ônus adicional. 4.9 Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, SIAPENET, Compras, SIORG, SIGEPE, entre outros)
5	Emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, **COM fornecimento de token criptográfico para armazenamento do certificado**, com validade por 3 anos.	**5.1. Certificado** 5.1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 5.1.2. Nível: A3. 5.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 5.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 5.1.5. Tipo: e-CNPJ. 5.1.6. 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, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco

		Central do Brasil, Justiça Federal, SERPRO, Correios entre outros. 5.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, SIAPENET, Compras, SIORG, SIGEPE, entre outros). **5.2. Dispositivo Físico de Armazenamento** 5.2.1. Dispositivo Físico de armazenamento (Token criptográfico), em modelo homologado conforme padrão ICPBrasil e constante na lista de homologação atual disponível no site do Instituto Nacional de Tecnologia da Informação (ITI). 5.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 5.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior. 5.2.4. Ser aderente às normas do Comitê Gestor da ICPBrasil. 5.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2. 5.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes. 5.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas. 5.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3). 5.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas. 5.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório. 5.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits. 5.2.12. Possuir carcaça resistente à água e à violação. 5.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores). 5.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores). 5.2.15. Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da Microsoft (Windows 2000 e versões superiores). 5.2.16. Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente. 5.2.16.1. Disponibilizar driver para que os frameworks Java JCA e

		Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE. 5.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4. 5.2.18. Possuir indicador luminoso de estado do dispositivo. 5.2.19. Assinar dados digitalmente em até 10 (dez) segundos. 5.2.20. O token criptográfico deverá possuir certificação do INMETRO. 5.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura. **5.3. Funcionalidades** 5.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores. 5.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label). 5.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres. 5.3.4. Permitir criação de senhas com caracteres alfanuméricos. 5.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos; 5.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459. 5.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo, sendo que no caso de certificados emitidos para pessoas jurídicas, o titular é a pessoa física responsável pela empresa. 5.3.8. Permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key). 5.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). 5.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. 5.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores) 5.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após

		autenticação da identidade do titular do dispositivo. 5.3.13. Implementar mecanismo de autenticação tipo challenge-response; 5.3.14. Forçar a troca da senha padrão no primeiro acesso; 5.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos; 5.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida; 5.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. **5.4. Software** 5.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita: 5.4.1.1. gerenciamento do dispositivo; 5.4.1.2. exportação de certificados armazenados no dispositivo; 5.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; 5.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; 5.4.1.5. visualização de certificados armazenados no dispositivo; 5.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; 5.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso. 5.4.2. Deverá ser disponibilizado portal para download de drivers/Softwares de forma ilimitada e gratuita. 5.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.

Aracaju/SE.

Elaborado por:

Integrante Requisitante	Integrante Técnico
gov.br Documento assinado digitalmente CRISTIANO ESTEVAN VASCONCELOS Data: 04/04/2024 10:20:17-0300 Verifique em https://validar.iti.gov.br	gov.br Documento assinado digitalmente JOAO SILVIO RIBEIRO DOS SANTOS Data: 04/04/2024 10:27:19-0300 Verifique em https://validar.iti.gov.br