Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 6 - Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de Sigilo no Âmbito da ICP-Brasil

versão 2.0

São Paulo, 22 de novembro de 2007

Sumário

Controle de Versão

Versão atual	Data de emissão	Alterações realizadas
1.1.r.47	**13/09/2006**	Inclusão no glossário dos termos PIN e senha de acesso. Atualização dos **REQUISITOS I.3** e **I.12** quanto à revogação do certificado digital. Inclusão de observação aos **REQUISITOS I.23** e **II.2**. Inclusão dos **REQUISITO I.24** e **I.32**.
2.0.r.07	**22/11/2007**	Separação do Manual de Condutas Técnicas – Volume 4 em MCT 4 (software de assinatura digital), MCT 5 (software de autenticação) e MCT 6 (software de sigilo).

1 Introdução

Este documento descreve os procedimentos de ensaio a serem aplicados no processo de homologação de softwares de sigilo no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de ensaio referem-se ao conjunto de métodos que serão usados para avaliar se softwares de sigilo estão ou não em conformidade com os requisitos técnicos definidos pelo Manual de Condutas Técnicas 6 - Volume I.

Para uma melhor compreensão do disposto neste documento, entenda-se por:

- **Sigilo de Conteúdo**: Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê confidencialidade como serviço de segurança. Para o caso de pacotes CMS "*envelopedData*", tal processo está associado aos certificados digitais ICP-Brasil de tipos S1, S2, S3 e S4;
- **Decifração de Conteúdo**: Processo inverso ao sigilo de dados. Neste caso, dados mantidos de forma confidencial (ilegível) são retornados para um estado legível;

Neste manual, a não ser que seja explicitamente mencionado o contrário, o termo "Software ICP-Brasil" será usado como referência ao software de sigilo no âmbito da ICP-Brasil.

1.1 Organização deste documento

Cada seção deste manual contém um conjunto de requisitos que representam citações diretas do próprio texto do Manual de Condutas Técnicas 6 – Volume I. Os requisitos estão organizados da seguinte forma:

- *REQUISITO <número_do_requisito>.<número_de_seqüência_do_requisito>*
  - "número_do_requisito": corresponde ao número de área definido no Manual de Condutas Técnicas 6 – Volume I;
  - "número_de_seqüência_do_requisito": corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA estão organizados da seguinte forma:

- *EN.<número_do_requisito>.<número_de_seqüência_do_requisito>.<número_de_seqüência_do_ensaio>*
    - "número_do_requisito";
    - "número_de_seqüência_do_requisito";
    - "número_de_seqüência_do_ensaio": corresponde a um identificador seqüencial dos procedimentos que devem ser realizados.

Nota: Para os Níveis de Segurança de Homologação 2 e 3, a menos que sejam explicitamente mencionados, os ensaios de análise de código fonte do software ICP-Brasil devem ser realizados especificamente de acordo com a finalidade que cada requisito apresenta em seu conteúdo.

Este documento (MCT 6 – Volume II) está estruturado da seguinte forma:

- Parte 1: Descreve os procedimentos de ensaio que devem ser verificados no processo de homologação de software de sigilo.

2 Parte 1

Procedimentos de ensaio para homologação de software de sigilo no âmbito da ICP-Brasil

2.1 Requisitos gerais de certificação digital

Esta seção descreve os requisitos mínimos de certificação digital que devem ser atendidos por softwares ICP-Brasil para o processo de assinatura digital.

REQUISITO I: Software ICP-Brasil deve atender aos requisitos de certificação digital estabelecidos a seguir.

Nota: Este requisito não é testado separadamente e faz parte da Seção 2.1.

2.1.1 Requisitos de certificação digital

REQUISITO I.1: Software ICP-Brasil deve ser capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

As extensões definidas para certificados digitais X.509v3 correspondem aos atributos adicionais que estão associados às chaves públicas ou às entidades usuárias externas. No caso da ICP-Brasil, conforme RESOLUÇÃO Nº 41, de 18 de Abril de 2006, na seção 7.1.2, certificados digitais devem obrigatoriamente conter as seguintes extensões:

- "*Authority Key Identifier*": campo que deve conter o *hash* SHA-1 da chave pública da AC;
- "*Key Usage*": define o propósito da chave criptográfica contida no certificado digital. Em certificados de assinatura digital, somente os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment* podem estar ativos. Por outro lado, em certificados de sigilo, somente os bits *keyEncipherment* e *dataEncipherment* podem estar ativos;
- "*Certificate Policies*": deve conter o OID da PC correspondente e a URL da DPC da AC que emitiu o certificado digital;
- "*CRL Distribution Points*": deve conter a URL onde está publicada a LCR correspondente;
- "*Subject Alternative Name*": permite que identidades ou características adicionais sejam associadas ao proprietário de um certificado digital.

Procedimentos de Ensaio para NSH 1:

EN.I.1.1: Verificar se a documentação do Software ICP-Brasil descreve a manipulação de certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3).

EN.I.1.2: Verificar se o Software ICP-Brasil é capaz de manipular certificados digitais que implementam a versão 3 do padrão ITU-T X.509 (X.509v3), no mínimo, por meio de um dos seguintes procedimentos:

- Consulta da LCR obtida a partir da URL do campo "*CRL Distribution Points*" presente no certificado digital;
- Consulta da DPC da AC que emitiu o certificado digital;
- Visualização por meio de alguma interface das extensões X.509v3 do certificado digital;
- Validação dos propósitos ("*Key Usage*") de um certificado digital. Por exemplo, validar os propósitos *digitalSignature* e *nonRepudiation* para assinatura digital de um documento eletrônico;
- Validação das restrições básicas ("*Basic Constraints*") de um certificado digital. Por exemplo, validação do tipo de certificado como entidade final ou autoridade certificadora.

REQUISITO I.2: Software ICP-Brasil deve ser capaz de manipular certificados digitais nos seguintes formatos:

- DER (*Distinguished Encoding Rules*); ou
- DER codificado em base64 ou PEM (*Privacy Enhanced Mail*).

Procedimentos de Ensaio para NSH 1:

EN.I.2.1: Verificar se a documentação do Software ICP-Brasil descreve a manipulação de certificados digitais nos formatos DER ou DER codificado em base64 ou PEM.

EN.I.2.2: Verificar se o Software ICP-Brasil é capaz de utilizar certificados digitais nos formatos DER ou DER codificado em base64 ou PEM, no mínimo, em um dos seguintes processos:

- Assinatura digital;
- Verificação de assinatura digital;
- Sigilo;
- Decifração; e
- Autenticação.

REQUISITO I.3: Todo certificado digital ICP-Brasil, antes de ser utilizado por um Software ICP-Brasil, deve ser verificado. A verificação de um certificado digital ICP-Brasil envolve:

1. Realizar a validação criptográfica (verificação com a chave criptográfica assimétrica pública do assinante) da assinatura digital do certificado;
2. Verificar se o instante de seu uso está dentro do prazo de validade definido para o certificado digital;
3. Verificar se o instante de uso do certificado digital não é posterior a um instante de revogação. Caso a revogação do certificado digital não seja verificada, o Software ICP-Brasil deve estar em conformidade ao **REQUISITO I.18**;
4. Verificar se o certificado digital é utilizado de acordo com seu propósito de uso definido nas extensões "*keyUsage*" e "*extendedKeyUsage*";
5. Verificar se o certificado digital é usado de acordo com a combinação entre seu propósito de uso e suas restrições básicas definidas na extensão "*Basic Constraints"*. No caso de certificado digital de autoridade certificadora, quando o propósito "*keyCertSign*" estiver declarado na extensão "*keyUsage*" do certificado digital, então a restrição "cA" também deve estar declarada na extensão "*Basic Constraints"* (baseado na RFC 3280, seção 4.2.1.3). No caso de certificado digital de entidade final (certificados de assinatura A1, A2, A3 e A4 e certificados de sigilo S1, S2, S3 e S4) a restrição "*cA*" não deve estar declarada na extensão "*Basic Constraints"* (baseado na RFC 3280 , seção 4.2.1.10);
6. Validar o caminho de certificação (vide **REQUISITO I.4**).

<u>Procedimentos de Ensaio para NSH 1:</u>

EN.I.3.1: Verificar se a documentação do Software ICP-Brasil descreve os procedimentos utilizados na verificação de um certificado digital ICP-Brasil antes de ser utilizado.

EN.I.3.2 (referente ao parágrafo 1 do REQUISITO I.3): Verificar se o software ICP-Brasil realiza a validação criptográfica da assinatura digital do certificado em duas situações distintas:

- Certificado digital íntegro; e
- Certificado digital não-íntegro, apresentando modificações em seu conteúdo original.

EN.I.3.3 (referente ao parágrafo 2 do REQUISITO I.3): Verificar se o software ICP-Brasil realiza a verificação do instante de uso do certificado digital em relação ao seu prazo de validade em duas situações distintas:

- Certificado digital não-revogado e dentro de seu prazo de validade; e
- Certificado digital expirado (fora de seu prazo de validade).

Nota: O instante de uso e prazo de validade do certificado digital será validado perante uma fonte de tempo adotada.

EN.I.3.4 (referente ao parágrafo 3 do REQUISITO I.3): Verificar se o software ICP-Brasil possibilita validar o instante de uso do certificado digital em relação ao seu instante de revogação em duas situações distintas:

- Certificado digital não-revogado e dentro de seu prazo de validade; e
- Certificado digital revogado anteriormente ao seu instante de uso e dentro do seu prazo de validade.

EN.I.3.5 (referente ao parágrafo 4 do REQUISITO I.3): Verificar se o software ICP-Brasil controla a utilização do certificado digital em relação ao seu propósito de uso ("*keyUsage*") nas seguintes condições:

- Certificado digital com propósitos de uso válidos para uma dada operação. Por exemplo, os propósitos "*digitalSignature*" e "*nonRepudiation*" para assinatura digital de um documento eletrônico; e

- Certificado digital com propósitos de uso inválidos para uma dada operação. Por exemplo, os propósitos "*keyEncipherment*" e "*dataEncipherment*" para assinatura digital de um documento eletrônico.

EN.I.3.6 (referente ao parágrafo 5 do REQUISITO I.3): Verificar se o software ICP-Brasil possibilita validar o propósito de uso do certificado digital em combinação com suas restrições básicas definidas na extensão "*Basic Constraints"* para duas situações distintas:

- Certificado digital com propósito de uso "*keyCertSign*" declarado na extensão "*keyUsage*" e restrição "*cA*" declarada na extensão "*Basic Constraints";*
- Certificado digital com propósito de uso "*keyCertSign*" declarado na extensão "*keyUsage*" e restrição "*cA*" não declarada na extensão "*Basic Constraints".*

EN.I.3.7 (referente ao parágrafo 6 do REQUISITO I.3): Este ensaio será realizado com base nos ensaios definidos para o **REQUISITO I.4**.

REQUISITO I.4: [requisito baseado na RFC 3280, seção 6] Um caminho de certificação consiste de uma seqüência de "n" certificados digitais {1, ..., n}, sendo que o primeiro certificado corresponde ao da entidade considerada como "âncora de confiança", ou seja, a AC Raiz. O n-ésimo certificado corresponde ao certificado que deve ser validado, neste caso, o de entidade final.

O processo de validação do caminho de certificação de um certificado digital deve satisfazer às seguintes condições:

- Para todo certificado digital "x" no intervalo {1, ..., n-1}, o proprietário do certificado digital "x" deve ser o emissor do certificado digital "x+1";
- Os requisitos 1, 2, 3, 4 e 5 do **REQUISITO I.3** devem ser aplicados para cada certificado digital que forma o caminho de certificação avaliado, compreendendo desde o certificado digital da AC raiz até os certificados digitais das ACs intermediárias.

<u>Procedimentos de Ensaio para NSH 1:</u>

EN.I.4.1: Verificar se a documentação do Software ICP-Brasil descreve a verificação do caminho de certificação de um certificado digital.

EN.I.4.2: Para os processos de assinatura digital, verificação de assinatura digital, sigilo, decifração e autenticação, verificar se o software ICP-Brasil realiza a verificação da relação entre o proprietário do certificado atual e o emissor do certificado subseqüente em duas situações distintas:

- Certificado digital com caminho de certificação completo; e
- Certificado digital com caminho de certificação incompleto.

EN.I.4.3: Para cada certificado digital que forma um caminho de certificação avaliado, verificar se o software ICP-Brasil aplica os ensaios correspondentes aos parágrafos 1, 2, 3, 4 e 5 do **REQUISITO I.3**.

REQUISITO I.5: [requisito baseado na RFC 3280, seção 4.2.1.10] Quando presente em um certificado digital, o Software ICP-Brasil deve ser capaz de verificar as restrições definidas sobre o comprimento do caminho de certificação válido. Na extensão "*Basic Constraints*" de um certificado digital, o campo "*pathLenConstraint*" representa o número máximo de certificados intermediários não auto-assinados que poderiam formar um caminho de certificação válido. O último certificado digital no caminho de certificação não é um certificado intermediário e, portanto, não está incluído neste limite. Além disso, quando apresentar um valor igual a zero, o campo "*pathLenConstraint*" indica que somente um certificado digital a mais poderia ser incluído em um caminho de certificação válido.

Procedimentos de Ensaio para NSH 1:

EN.I.5.1: Verificar se a documentação do Software ICP-Brasil descreve a verificação das restrições definidas sobre o comprimento do caminho de certificação válido.

EN.I.5.2: Verificar se o software ICP-Brasil valida as restrições definidas sobre o comprimento do caminho de certificação baseando-se na extensão "*Basic Constraints*" e no campo "*pathLenConstraint*", em duas situações distintas:

- Caminho de certificação com comprimento que atende às restrições do campo "*pathLenConstraint*"; e
- Caminho de certificação com comprimento que não atende às restrições do campo "*pathLenConstraint*" (por exemplo, caminho de certificação maior que o permitido).

REQUISITO I.6: [requisito baseado na RFC 3280, seção 4.2.1.13] Software ICP-Brasil deve processar as extensões "*keyUsage*" e "*extendedKeyUsage*" de forma independente e o certificado deve somente ser usado para um propósito consistente com ambas as extensões. Se não houver um propósito consistente com ambas as extensões, então o certificado digital não deve ser usado.
Por propósitos consistentes entende-se aqueles definidos na seção 4.2.1.13 do documento RFC 3280.

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO I.3**.

REQUISITO I.7: Ao final do processo de verificação de um certificado digital, com relação aos requisitos constantes no **REQUISITO I.3**, o Software ICP-Brasil deve ser capaz de informar à entidade usuária externa os problemas de não-conformidade encontrados, assim como também delegar à própria entidade usuária externa a escolha sobre continuar utilizando o certificado digital mesmo com os problemas de não-conformidade encontrados.

Procedimentos de Ensaio para NSH 1:

EN.I.7.1: Verificar se a documentação do Software ICP-Brasil descreve uma interface que permita informar à entidade usuária externa a respeito de problemas de não-conformidade encontrados ao final do processo de verificação de um certificado digital.

EN.I.7.2: Utilizando um certificado digital inválido em relação aos parágrafos constantes no **REQUISITO I.3**, como por exemplo, certificado não-íntegro ou expirado. Verificar se o software ICP-Brasil torna disponível à entidade usuária

externa informações sobre os problemas de não-conformidade encontrados. Na seqüência, deve-se verificar também se o software ICP-Brasil permite que a entidade usuária externa escolha sobre continuar ou não utilizando o certificado digital mesmo com os problemas de não-conformidade encontrados.

REQUISITO I.8: Software ICP-Brasil deve ser capaz de identificar e realizar uma indicação diferenciada à entidade usuária externa dos certificados digitais emitidos no âmbito da infra-estrutura de chaves públicas brasileira daqueles emitidos por outras ICPs.

Procedimentos de Ensaio para NSH 1:

EN.I.8.1: Verificar se a documentação do Software ICP-Brasil descreve uma indicação diferenciada para a entidade usuária externa dos certificados digitais emitidos no âmbito da infra-estrutura de chaves públicas brasileira.

EN.I.8.2: Manipular, por meio do Software ICP-Brasil, um certificado digital emitido no âmbito da infra-estrutura de chaves públicas brasileira, e verificar se o Software ICP-Brasil, por meio de alguma funcionalidade disponível, é capaz de identificar e realizar algum tipo de indicação à entidade usuária externa que permita diferenciar um certificado digital ICP-Brasil.

REQUISITO I.9: Baseando-se no tipo de certificado ICP-Brasil (A1, A2, A3, A4, S1, S2, S3 S4 ou de autoridade certificadora), assim como nas extensões "*keyUsage*", "*extendedKeyUsage*" e "*Basic Constraints*", o Software ICP-Brasil deve ser capaz de informar e esclarecer à entidade usuária externa sobre as possibilidades de uso de um certificado digital escolhido.

Procedimentos de Ensaio para NSH 1:

EN.I.9.1: Verificar se a documentação do Software ICP-Brasil descreve como uma entidade usuária toma conhecimento sobre as possibilidades de uso de um determinado certificado digital.

EN.I.9.2: Manipular um certificado digital emitido no âmbito da infra-estrutura de chaves públicas brasileira e por meio do Software ICP-Brasil, verificar se está disponível algum tipo de informação ou esclarecimento à entidade usuária externa sobre as possibilidades do uso do certificado digital escolhido.

REQUISITO I.10: Software ICP-Brasil deve ser capaz de identificar e mostrar à entidade usuária externa todos os campos específicos ICP-Brasil disponíveis em um certificado digital. Por campos específicos ICP-Brasil, ou simplesmente "campos ICP-Brasil" entende-se os parâmetros configurados no campo "*Subject Alternative Name*" do certificado digital conforme a RESOLUÇÃO Nº 41, de 18 de Abril de 2006, seção 7.1.2.

Certificado digital de entidade final pessoa física deve possuir os seguintes campos "*otherName*":

- OID 2.16.76.1.3.1 = data de nascimento do titular no formato ddmmaa; Cadastro de Pessoa Física (CPF) do titular; Número de Identificação Social - NIS (PIS, PASEP ou CI); número do Registro Geral (RG) do titular; siglas do órgão expedidor do RG e respectiva UF;
- OID 2.16.76.1.3.6 = número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado;
- OID 2.16.76.1.3.5 = número de inscrição do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor; e
- OID 2.16.76.1.4.n = número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

Certificado digital de entidade final pessoa jurídica deve possuir os seguintes campos "*otherName*":

- OID 2.16.76.1.3.4 = data de nascimento do responsável pelo certificado no formato ddmmaa; Cadastro de Pessoa Física (CPF) do responsável; Número de Identificação Social – NIS (PIS, PASEP ou CI); número do RG do responsável; siglas do órgão expedidor do RG e respectiva UF;
- OID 2.16.76.1.3.2 = nome do responsável pelo certificado;
- OID 2.16.76.1.3.3 = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado; e

- OID 2.16.76.1.3.7 = número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

Certificado digital de equipamento ou aplicação deve possuir os seguintes campos "*otherName*":

- OID 2.16.76.1.3.8 = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações, se o certificado for de pessoa jurídica;
- OID 2.16.76.1.3.3 = Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;
- OID 2.16.76.1.3.2 = nome do responsável pelo certificado; e
- OID 2.16.76.1.3.4 = data de nascimento do responsável pelo certificado, no formato ddmmaa; Cadastro de Pessoa Física (CPF) do responsável; número de Identificação Social – NIS (PIS, PASEP ou CI); número do RG do responsável; siglas do órgão expedidor do RG e respectiva UF.

Procedimentos de Ensaio para NSH 1:

EN.I.10.1: Verificar se a documentação do Software ICP-Brasil descreve campos específicos ICP-Brasil, de tal forma que permita à entidade usuária externa visualizar todos os respectivos campos especificados, por meio de parâmetros configurados no campo "*Subject Alternative Name*" do certificado digital.

EN.I.10.2: Utilizando o Software ICP-Brasil, ao selecionar um certificado digital ICP-Brasil válido, verificar se existe alguma funcionalidade que possibilite apresentar à entidade usuária externa informações sobre todos os campos específicos ICP-Brasil, disponíveis neste certificado de acordo com o **REQUISITO I.10**.

REQUISITO I.11: Software ICP-Brasil deve ser capaz de identificar e utilizar os nomes atribuídos tanto ao titular quanto ao emissor de um certificado digital (campos "*Subject*" e "*Issuer*", respectivamente) de acordo com o padrão ITU-T X.500/ISO 9594. Nomes do titular e do emissor de um certificado digital são formados por atributos, tais como:

- C (*Country*);

- O (*Organization*);
- CN (*Common Name*);
- OU (*Organization Unit*);
- etc.

Procedimentos de Ensaio para NSH 1:

EN.I.11.1: Verificar se a documentação do Software ICP-Brasil descreve a identificação e utilização dos nomes atribuídos ao titular e emissor de um certificado digital, especificados nos campos "*Subject*" e "*Issuer*", respectivamente.

EN.I.11.2: Verificar se existe alguma funcionalidade no Software ICP-Brasil que permita à entidade usuária externa apresentar ou manipular os nomes atribuídos ao titular e emissor do certificado digital selecionado.

REQUISITO I.12: Software ICP-Brasil deve ser capaz de apresentar, no mínimo, as seguintes informações sobre um certificado digital de entidade final:

- Tipo de certificado digital ICP-Brasil (A1, A2, A3, A4, S1, S2, S3 ou S4);
- Caminho de certificação;
- Todos os campos ICP-Brasil presentes no certificado digital (como descrito no **REQUISITO I.10**);
- Identificação do proprietário do certificado ("*Subject*");
- Identificação do emissor do certificado ("*Issuer*");
- Propósitos de uso do certificado baseando-se nas extensões "*keyUsage*", "*extendedKeyUsage*" e "*Basic Constraints*";
- Número serial ("*serialNumber*");
- Datas de início e término de validade ("*validity*");
- Política de certificação ("*Certificate Policies*"); e
- Resultado do processo de verificação de revogação do certificado digital. Caso a revogação do certificado digital não seja verificada, o Software ICP-Brasil deve estar em conformidade ao **REQUISITO I.18**.

Procedimentos de Ensaio para NSH 1:

EN.I.12.1: Verificar se a documentação do Software ICP-Brasil descreve a apresentação das informações especificadas no **REQUISITO I.12** sobre um certificado digital de entidade final.

EN.I.12.2: Utilizando o Software ICP-Brasil, ao selecionar um certificado digital ICP-Brasil válido, verificar se existe alguma funcionalidade no Software que possibilite apresentar à entidade usuária externa, as informações especificadas no **REQUISITO I.12** sobre o certificado digital de entidade final escolhido.

REQUISITO I.13: Software ICP-Brasil deve ser capaz de apresentar, no mínimo, as seguintes informações sobre um certificado digital de autoridade certificadora:

- Caminho de certificação;
- Identificação do proprietário do certificado ("*Subject*");
- Identificação do emissor do certificado ("*Issuer*");
- Propósitos de uso do certificado baseando-se nas extensões "*keyUsage*", "*extendedKeyUsage*" e "*Basic Constraints*";
- Número serial ("*serialNumber*");
- Datas de início e término de validade ("*validity*");
- Política de certificação ("*Certificate Policies*"); e
- Resultado do processo de verificação de revogação do certificado digital.

Procedimentos de Ensaio para NSH 1:

EN.I.13.1: Verificar se a documentação do Software ICP-Brasil descreve as informações especificadas no **REQUISITO I.13** sobre um certificado digital de autoridade certificadora.

EN.I.13.2: Utilizando o Software ICP-Brasil, ao selecionar um certificado digital ICP-Brasil de autoridade certificadora válido, verificar se existe alguma funcionalidade no Software que possibilite apresentar à entidade usuária externa, as informações especificadas no **REQUISITO I.13** sobre o certificado digital de autoridade certificadora escolhido.

2.1.2 Requisitos Específicos sobre a Revogação de Certificados Digitais

Quando um certificado digital é emitido, um período de validade de uso é definido. Entretanto, sob diversas circunstâncias, um certificado digital pode tornar-se inválido antes de sua data de expiração e ser revogado pelo seu proprietário.

Um dos métodos de revogação comumente utilizados pelas ACs consiste na emissão periódica de listas de certificados revogados, ou simplesmente LCRs. Uma LCR é uma lista cronologicamente selada (*timestamped list*) que identifica certificados digitais revogados e, além disso, deve ser assinada pela AC e tornada disponível em um repositório público.

Um outro método de se obter informações sobre a revogação de um certificado digital é por meio do protocolo OCSP (*Online Certificate Status Protocol*) que, de forma imediata (*on-line)*, permite com que o estado de revogação de um certificado digital seja determinado.

Os requisitos descritos nesta seção correspondem a requisitos específicos ICP-Brasil que são aplicáveis ao processo de consulta sobre a revogação de certificados digitais.

REQUISITO I.14: Software ICP-Brasil deve atender aos requisitos específicos ora estabelecidos sobre a revogação de certificados digitais, conforme descrito a seguir.

Nota: Este requisito não é testado separadamente e faz parte da Seção 2.1.2.

REQUISITO I.15: Software ICP-Brasil deve ser capaz de manipular Listas de Certificados Revogados (LCRs) que implementam a versão 2 do padrão ITU-T X.509.

Procedimentos de Ensaio para NSH 1:

EN.I.15.01: Verificar se a documentação do Software ICP-Brasil descreve a manipulação de Listas de Certificados Revogados (LCRs), que implementam a versão 2 do padrão ITU-T X.509.

EN.I.15.2: Verificar se o Software ICP-Brasil é capaz de manipular as LCRs que implementam a versão 2 do padrão ITU-T X.509, no mínimo por meio de um dos seguintes procedimentos:

- Visualização por meio de alguma interface dos campos de uma LCR recebida ou armazenada; e
- Uso de uma LCR obtida a partir da URL do campo "*CRL Distribution Points*" presente no certificado digital. Por exemplo, durante um processo de assinatura digital, uma LCR obtida poderia ser utilizada para determinar a validade do certificado digital de assinatura.

REQUISITO I.16: Software ICP-Brasil deve ser capaz de oferecer à entidade usuária externa a opção de configurar se deseja ou não buscar a LCR e verificar, via consulta, a revogação de certificados digitais.

Procedimentos de Ensaio para NSH 1:

EN.I.16.1: Verificar se a documentação do Software ICP-Brasil descreve a configuração de busca de LCRs e verificação, via consulta, da revogação de certificados digitais, por opção da entidade usuária externa.

EN.I.16.2: Verificar se o Software ICP-Brasil, permite que a entidade usuária externa configure a busca de LCRs e a verificação, via consulta, de certificados digitais revogados.

REQUISITO I.17: Software ICP-Brasil deve ser capaz de oferecer à entidade usuária externa a opção de configurar se deseja verificar a revogação de certificados digitais.

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO I.16.**

REQUISITO I.18: Caso a verificação de revogação de certificados digitais não esteja habilitada, em qualquer processo de validação de certificado digital, o Software ICP-

Brasil deve emitir um alerta à entidade usuária externa indicando que a verificação de revogação não foi realizada.

Procedimentos de Ensaio para NSH 1:

EN.I.18.1: Verificar se a documentação do Software ICP-Brasil descreve a emissão de um alerta, o qual indica à entidade usuária externa, durante o processo de validação de um certificado digital, que a verificação de revogação do certificado não foi realizada.

EN.I.18.2: Para os processos de validação de certificado digital, onde a verificação de revogação de certificados digitais não esteja habilitada, verificar se o Software ICP-Brasil emite um alerta à entidade usuária externa indicando que a verificação de revogação não foi realizada.

REQUISITO I.19: Caso a opção de verificar a revogação de um dado certificado digital esteja habilitada, o Software ICP-Brasil deve permitir tal verificação por meio dos seguintes métodos:

- Obtenção de LCR de um pacote CMS "*SignedData*"; ou
- Busca de LCR utilizando os protocolos:
  - HTTP; ou
  - LDAP.

Procedimentos de Ensaio para NSH 1:

EN.I.19.1: Verificar se a documentação do Software ICP-Brasil descreve os métodos que permitem verificar a revogação de um dado certificado digital.

EN.I.19.2: Utilizando um pacote CMS "SIGNED DATA", verificar se o Software ICP-Brasil é capaz de verificar a revogação do certificado digital utilizando as seguintes situações:

- Pacote CMS "SIGNED DATA" com assinatura digital realizada utilizando certificado digital não-revogado;

- Pacote CMS “SIGNED DATA” com assinatura digital realizada utilizando certificado digital revogado.

EN.I.19.3: Utilizando o protocolo HTTP ou LDAP, por meio da análise de pacotes na interface de acesso à rede, verificar se o Software ICP-Brasil é capaz de buscar a LCR e depois verificar a revogação de um dado certificado digital utilizando as seguintes situações:

- Certificado digital não-revogado;
- Certificado digital revogado.

EN.I.19.4: Para cada um dos métodos descritos no **REQUISITO I.19**, verificar se o Software ICP-Brasil informa à entidade usuária externa quando a LCR utilizada encontra-se nos seguintes estados:

- LCR mais atual;
- LCR correntemente publicada; e
- LCR desatualizada.

EN.I.19.5: Verificar se o Software ICP-Brasil alerta à entidade usuária externa que uma LCR desatualizada ou correntemente publicada não é adequada para verificar a revogação de um dado certificado digital.

REQUISITO I.20: Para o caso de verificação de revogação por meio de LCR, o Software ICP-Brasil deve ser capaz de verificar se a LCR é válida utilizando os seguintes procedimentos:

1. Verificação criptográfica da assinatura digital (verificação com a chave criptográfica assimétrica pública do assinante);
2. Verificação se o assinante da LCR é a AC que assina o certificado digital;
3. Verificação do certificado digital do assinante da LCR perante os requisitos constantes no **REQUISITO I.3.** Neste caso, especificamente para a extensão “*Key Usage*”, deve-se verificar que no certificado digital de assinatura da LCR o propósito “*cRLSign*” esteja declarado;
4. Verificação se o instante corrente de uso da LCR é, no mínimo, anterior ao valor de tempo registrado no campo “*nextUpdate*” da LCR.

Procedimentos de Ensaio para NSH 1:

EN.I.20.1: Verificar se a documentação do Software ICP-Brasil descreve os procedimentos para verificar se uma dada LCR é válida.

EN.I.20.2: Verificar se o Software ICP-Brasil realiza a verificação criptográfica da assinatura digital da LCR nas seguintes situações:

- LCR assinada e íntegra; e
- LCR assinada, porém com modificações em seu conteúdo original para caracterizar um problema de integridade.

EN.I.20.3: Verificar se o Software ICP-Brasil realiza a verificação entre o assinante da LCR e a AC de um certificado digital, para os seguintes casos:

- LCR assinada pela mesma AC do certificado digital; e
- LCR assinada por AC diferente do certificado digital.

EN.I.20.4: Considerando o certificado digital do assinante da LCR, aplicar os ensaios especificados no **REQUISITO I.3** considerando para a extensão "*Key Usage*" que o propósito "*cRLSign*" esteja declarado.

EN.I.20.5: Verificar se o Software ICP-Brasil realiza a verificação do instante corrente de uso da LCR com o valor de tempo registrado no campo "*nextUpdate*" da LCR, para as seguintes situações:

- LCR com campo "*nextUpdate*" contendo valor de tempo anterior ao instante de uso; e
- LCR com campo "*nextUpdate*" contendo valor de tempo posterior ao instante de uso.

RECOMENDAÇÃO I.1: Para o caso da consulta "*on-line*" sobre o estado de um certificado digital via protocolo OCSP, recomenda-se que o Software ICP-Brasil seja capaz de verificar se a resposta OCSP é válida e confiável por meio dos seguintes procedimentos:

- Verificação criptográfica da assinatura digital (verificação com a chave criptográfica assimétrica pública do assinante);
- Verificação se o assinante da resposta OCSP é a mesma AC que assina o certificado digital;
- Verificação do certificado digital do assinante da resposta OCSP perante os requisitos constantes no **REQUISITO I.3**. Neste caso, os propósitos "*digitalSignature*" e/ou "*nonRepudiation*" devem estar declarados na extensão "*Key Usage*" e o propósito "*OCSPSigning*" deve estar presente na extensão "*Extended Key Usage*"; e
- Quando aplicável, o intervalo de validade da resposta OCSP.

Procedimentos de Ensaio para NSH 1:

EN.REC.I.1.1: Verificar se a documentação do Software ICP-Brasil descreve os procedimentos de verificação de validade da resposta OCSP, de acordo com a **RECOMENDAÇÃO I.1**.

EN.REC.I.1.2: Verificar se o Software ICP-Brasil realiza a verificação criptográfica da assinatura digital da resposta OCSP nas seguintes situações:

- Resposta OCSP assinada e íntegra; e
- Resposta OCSP assinada, porém com modificações em seu conteúdo original para caracterizar um problema de integridade.

EN.REC.I.1.3: Verificar se o Software ICP-Brasil realiza a verificação entre o assinante da resposta OCSP e a AC de um certificado digital, para os seguintes casos:

- Resposta OCSP assinada pela mesma AC do certificado digital; e
- Resposta OCSP assinada por AC diferente do certificado digital.

EN.REC.I.1.4: Considerando o certificado digital do assinante da resposta OCSP, aplicar os ensaios especificados no **REQUISITO I.3** considerando para a extensão "*Key Usage*" que os propósitos "*digitalSignature*" e/ou "*nonRepudiation*" estejam

declarados e para a extensão "*Extended Key Usage*" o propósito "*OCSPSigning*" esteja declarado.

EN.REC.I.1.5: Quando aplicável, verificar se o Software ICP-Brasil realiza a verificação do instante corrente de uso da resposta OCSP com seu intervalo de validade.

REQUISITO I.21: Software ICP-Brasil deve ser capaz de obter o endereço de busca da LCR diretamente no campo "*CRL Distribution Points*" presente no certificado digital.

Procedimentos de Ensaio para NSH 1:

EN.I.21.1: Verificar se a documentação do Software ICP-Brasil descreve a obtenção do endereço de busca da LCR a partir do campo "*CRL Distribution Points*" presente no certificado digital.

EN.I.21.2: Executar o processo de verificação de revogação de um certificado digital, por meio do Software ICP-Brasil, utilizando a opção de busca de LCR. Neste caso, verificar na interface de acesso a rede, por meio de observação de pacotes, se o Software ICP-Brasil requisita a busca da LCR na URL presente no campo "*CRL Distribution Points*" do certificado digital usado.

RECOMENDAÇÃO I.2: Recomenda-se que o Software ICP-Brasil seja capaz de oferecer à entidade usuária externa a opção de configurar se deseja consultar a LCR mais atual (*CRL Grace Time*). Por "LCR mais atual" entende-se a LCR que estará disponível no próximo período de publicação (subseqüente ao instante atual) e não a LCR correntemente publicada.

Procedimentos de Ensaio para NSH 1:

EN.REC.I.2.1: Verificar se a documentação do Software ICP-Brasil descreve a configuração da consulta da LCR mais atual (*CRL Grace Time*) pela entidade usuária externa.

EN.REC.I.2.2: Executar o processo de verificação de revogação de um certificado digital, por meio do Software ICP-Brasil, utilizando a opção de busca da LCR mais atual. Verificar como o Software ICP-Brasil se comporta perante a entidade usuária externa quando a opção de consulta a LCR mais atual estiver habilitada.

EN.REC.I.2.3: Executar o processo de verificação de revogação de um certificado digital, por meio do Software ICP-Brasil, utilizando a opção de busca de LCR mais atual. Neste caso, verificar na interface de acesso a rede, por meio de observação de pacotes, se o Software ICP-Brasil realiza a busca da LCR mais atual.

RECOMENDAÇÃO I.3: Para verificar a revogação de um certificado digital por meio de LCR, recomenda-se que o Software ICP-Brasil possa oferecer à entidade usuária externa a opção de configurar um agente *proxy* para a obtenção local de LCRs.

Procedimentos de Ensaio para NSH 1:

EN.REC.I.3.1: Verificar se a documentação do Software ICP-Brasil, descreve a configuração de um agente *proxy* para obtenção local de LCRs pela entidade usuária externa.

EN.REC.I.3.2: Caso haja a opção de configurar um agente *proxy* para a obtenção local de de LCRs, executar o processo de verificação de revogação de um certificado digital, por meio do Software ICP-Brasil, utilizando a opção de busca de LCR. Neste caso, por meio da observação de pacotes, verificar se o Software ICP-Brasil permite à entidade usuária externa requisitar e obter localmente a LCR desejada do agente *proxy* configurado.

REQUISITO I.22: Ao verificar a LCR e a revogação de um certificado digital, o Software ICP-Brasil deve ser capaz de oferecer à entidade usuária externa as seguintes funcionalidades:

1. Mostrar a versão e o número da LCR;
2. Informar o estado em que se encontra o certificado digital da entidade usuária externa em termos de revogado ou não-revogado;
3. Para o certificado digital de assinatura da LCR:
   - Alertar à entidade usuária externa, quando for o caso, quais requisitos de verificação de certificado digital não estão em conformidade ao **REQUISITO I.3**, ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado;
   - Quando for do desejo da entidade usuária externa, mostrar as informações sobre o certificado digital conforme **REQUISITO I.13**;
4. Mostrar o estado da LCR verificada;
5. Caso o certificado digital da entidade usuária externa esteja revogado, mostrar, no mínimo, mas não limitado aos seguintes aspectos:
   - Número serial do certificado digital;
   - Data da revogação;
   - Motivo da revogação (*Reason Code*) do certificado. Caso não esteja presente, deve-se emitir um aviso à entidade usuária externa; e
   - Quando aplicável, a data que se conhece ou suspeita-se que o certificado digital tornou-se inválido (*Invalidity Date*). Esta data seria anterior à data de revogação presente na LCR e poderia preceder a data de emissão de LCRs anteriores.

Procedimentos de Ensaio para NSH 1:

EN.I.22.1: Verificar se a documentação do Software ICP-Brasil descreve as funcionalidades especificadas no **REQUISITO I.22**.

EN.I.22.2: Executar o processo de verificação de revogação de um certificado digital válido, por meio do Software ICP-Brasil, utilizando a opção de busca de LCR. Verificar se o Software ICP-Brasil informa à entidade usuária externa a versão,

número da LCR utilizada e o estado do seu certificado digital, para as seguintes situações:

- Certificado digital válido; e
- Certificado digital revogado.

EN.I.22.3: Em um processo de verificação de revogação de um certificado digital por meio de LCR e adotando um certificado digital de assinatura da LCR que apresenta alguma não- conformidade com os requisitos do **REQUISITO I.13**, verificar se o Software ICP-Brasil alerta à entidade usuária externa sobre a(s) não-conformidade(s) encontrada(s), ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado.

EN.I.22.4: Verificar se o Software ICP-Brasil mostra à entidade usuária externa o estado da LCR utilizada durante o processo de verificação de revogação de um certificado digital.

EN.I.22.5: Verificar se o Software ICP-Brasil mostra à entidade usuária externa informações relacionadas ao **REQUISITO I.13** sobre o certificado digital do assinante da LCR.

EN.I.22.6: Para situações onde o certificado digital do assinante da LCR está revogado, verificar se o Software ICP-Brasil torna disponível as seguintes informações:

- Número serial do certificado digital;
- Data da revogação;
- Motivo da revogação (*Reason Code*) do certificado. Caso não esteja presente, deve-se emitir um aviso à entidade usuária externa; e
- Quando aplicável, a data que se conhece ou suspeita-se que o certificado digital tornou-se inválido (*Invalidity Date*).

2.1.3 Requisitos de Segurança

REQUISITO I.23: Quando aplicável, caso o Software ICP-Brasil (aplicação) necessite lidar com o PIN (*Personal Identificantion Number*) ou senha de acesso (para chaves privadas armazenadas em arquivo) da entidade usuária externa, os seguintes requisitos de segurança devem ser atendidos:

- Em um processo de inserção, os caracteres devem sempre ser mascarados, ou seja, nunca devem ser visualizados em um campo na forma de texto legível;
- O valor do PIN nunca deve ser mantido em *cache*;
- Após seu uso, o valor do PIN deve ser eliminado. Quando em memória, a eliminação do valor do PIN deve ser realizada por meio da técnica de sobrescrita de valores.

OBSERVAÇÃO: Um software ICP-Brasil (aplicação) que necessite realizar diversas operações criptográficas em seqüência utilizando uma mesma chave privada que esteja armazenada em cartão inteligente, token criptográfico ou HSM (por exemplo, assinatura digital em lote), nunca deve manter o valor do PIN persistente em sua área de memória (cache). Neste caso, existem formas seguras para possibilitar a realização de operações criptográficas em seqüência utilizando uma mesma chave privada sem a necessidade de manter o valor do PIN persistente na área de memória do software ICP-Brasil (aplicação), como por exemplo, por meio da utilização da técnica de estabelecimento de canais seguros ou na interface PKCS#11 com o estabelecimento de uma sessão de software.

Procedimentos de Ensaio para NSH 1:

EN.I.23.1: Verificar se a documentação do Software ICP-Brasil descreve o manuseio do PIN (*Personal Identificantion Number*) da entidade usuária externa, por parte do próprio Software ICP-Brasil (aplicação) conforme os requisitos de segurança especificados no **REQUISITO I.23**.

EN.I.23.2: Executar o Software ICP-Brasil, e invocar uma operação que necessite manipular o PIN da entidade usuária externa (por exemplo, a realização de uma

assinatura digital). Durante o processo de inserção do PIN, verificar se os caracteres digitados são mascarados por meio de caracteres ilegíveis, por exemplo, asteriscos "*".

EN.I.23.3: Executar o Software ICP-Brasil, e solicitar ao mesmo a manipulação do PIN da entidade usuária externa. Após a inserção e validação bem sucedida do PIN da entidade usuária externa, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória), se o PIN esteve presente na memória do PC.

EN.I.23.4: Executar o Software ICP-Brasil, e solicitar ao mesmo a manipulação do PIN da entidade usuária externa. Após a inserção e validação bem sucedida do PIN da entidade usuária externa, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória), se o PIN foi apagado/removido da memória.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.23.5: Executar o Software ICP-Brasil, e solicitar ao mesmo a manipulação do PIN da entidade usuária externa. Após a inserção e validação bem sucedida do PIN da entidade usuária externa, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória) e com a análise do código fonte do Software ICP-Brasil, se o PIN foi apagado/removido da memória.

REQUISITO I.24: Caso o Software ICP-Brasil necessite lidar com chaves criptográficas armazenadas em arquivo, ou seja, chaves privadas associadas a certificados digitais ICP Brasil do tipo A1 ou S1, a chave privada deve ser mantida em sua área de memória apenas durante a realização da operação criptográfica, ou de operações criptográficas seqüenciais, devendo ser eliminada em seguida por meio da técnica de sobrescrita de valores. Assim, a chave privada nunca deve ser mantida em *cache.*

Procedimentos de Ensaio para NSH 1:

EN.I.24.1: Verificar se a documentação do Software ICP-Brasil, descreve a manipulação de chaves privadas associadas a certificados digitais ICP Brasil do tipo A1 ou S1.

EN.I.24.2: Executar o Software ICP-Brasil, e invocar uma operação criptográfica que necessite manipular uma determinada chave privada associada a um certificado digital ICP Brasil do tipo A1 ou S1, como por exemplo, assinatura digital de um documento eletrônico ou a decifração de um documento protegido. Após a conclusão bem sucedida da operação, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória), se a chave privada associada ao certificado permanece aberta em memória ou pode ter sido eliminada.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.24.3: Executar o Software ICP-Brasil, e invocar uma operação criptográfica que necessite manipular uma determinada chave privada associada a um certificado digital ICP Brasil do tipo A1 ou S1, como por exemplo, assinatura digital de um documento eletrônico ou a decifração de um documento protegido. Após a conclusão bem sucedida da operação, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória) e com a análise do código fonte do Software ICP-Brasil, se a chave privada associada ao certificado permanece em memória ou foi eliminada.

REQUISITO I.25: Software de carga dinâmica, como por exemplo, *applets*, deve possuir controles adicionais de segurança para:

- Garantia da integridade do software; e
- Garantia da origem do software.

Procedimentos de Ensaio para NSH 1:

EN.I.25.1: Verificar se a documentação do Software ICP-Brasil, descreve controles adicionais de segurança para softwares de carga dinâmica, em relação à integridade e origem do software.

EN.I.25.2: Para o controle de segurança que provê a integridade do software de carga dinâmica, verificar se tal controle é feito em uma situação provocada que contenha erro de integridade.

EN.I.25.3: Para o controle de segurança que provê a origem do software de carga dinâmica, verificar se tal controle é feito em situações provocadas que contenham erros na origem e autoria do software.

REQUISITO I.26: Controles adicionais de segurança para software de carga dinâmica devem estar documentados nos manuais.

Procedimentos de Ensaio para NSH 1:

EN.I.26.1: Verificar se algum manual do Software ICP-Brasil contém documentado os controles adicionais de segurança para a verificação da integridade e origem dos softwares de carga dinâmica.

REQUISITO I.27: Software ICP-Brasil deve manipular senhas e dados sensíveis assegurando:

- Sobreposição do seu valor após o uso;
- Utilização de ponteiros dinâmicos para seu armazenamento; e
- Não utilização de mecanismos de *cache*.

Procedimentos de Ensaio para NSH 1:

EN.I.27.1: Verificar se a documentação do Software ICP-Brasil, descreve a manipulação segura de senhas e dados sensíveis conforme especificado no **REQUISITO I.27**.

EN.I.27.2: Iniciar o Software ICP-Brasil, e executar operações que envolvam a manipulação de senhas e dados sensíveis, como por exemplo, a assinatura digital e sigilo de um documento eletrônico. Em seguida, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória), se, após o uso do Software ICP-Brasil, senhas e dados sensíveis ainda permanecem na memória alocada pelo Software ICP-Brasil e/ou pelo seu Middleware.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.27.3: Iniciar o Software ICP-Brasil, e executar repetitivamente operações que envolvam a manipulação de senhas e dados sensíveis, como por exemplo, a assinatura digital e sigilo de um documento eletrônico. Em seguida, verificar por meio de aplicação específica (por exemplo, aplicação que realiza *dump* de memória), e com o auxílio do código fonte do Software ICP-Brasil, se, após o uso do Software ICP-Brasil, senhas e dados sensíveis ainda permanecem na memória alocada pelo Software ICP-Brasil e/ou pelo seu Middleware.

2.1.4 Requisitos de Documentação

REQUISITO I.28: O responsável deve fornecer, com o software, a seguinte documentação em idioma português do Brasil:

- Manual de usuário;
- Manual de instalação;
- Especificação técnica.

Procedimentos de Ensaio para NSH 1:

EN.I.28.1: Verificar se a documentação que acompanha o Software ICP-Brasil, apresenta manuais de usuário e instalação, assim como uma parte de especificação técnica do software, em idioma português do Brasil.

REQUISITO I.29: Software ICP-Brasil deve possuir ou possibilitar a configuração da sua interface em idioma português do Brasil.

Procedimentos de Ensaio para NSH 1:

EN.I.29.1: Verificar se o Software ICP-Brasil possui sua interface em idioma português do Brasil, ou então, se é possível configurar tal interface.

REQUISITO I.30: Software ICP-Brasil deve possuir manual de usuário e tópicos de ajuda em idioma português do Brasil.

Procedimentos de Ensaio para NSH 1:

EN.I.30.1: Verificar se a documentação que acompanha o Software ICP-Brasil, apresenta manual de usuário e tópicos de ajuda em idioma português do Brasil.

REQUISITO I.31: O manual de usuário, manual de instalação e especificação técnica devem informar as plataformas suportadas pelo software e os requisitos de ambiente operacional necessários para sua operação.

Procedimentos de Ensaio para NSH 1:

EN.I.31.1: Verificar se a documentação que acompanha o Software ICP-Brasil, descreve as plataformas de sistemas operacionais que são suportadas pelo Software ICP-Brasil.

EN.I.31.2: Verificar se a documentação que acompanha o Software ICP-Brasil, descreve os requisitos do ambiente operacional que são necessários para operação do Software ICP-Brasil.

REQUISITO I.32: Software ICP-Brasil deve permitir a entidade usuária externa visualizar a versão do software e o nome de seu responsável.

Procedimentos de Ensaio para NSH 1:

EN.I.32.1: Verificar se o Software ICP-Brasil possui uma funcionalidade na qual é possível visualizar a versão do software e o nome de seu responsável.

2.2 Requisitos Específicos para Softwares de Sigilo

Os requisitos descritos nesta seção correspondem a requisitos técnicos específicos que são aplicáveis aos softwares que utilizam certificados digitais ICP-Brasil para a realização de sigilo (cifração) e decifração de dados sigilosos.

Nesta seção, a não ser que seja explicitamente mencionado o contrário, o termo "Software de Sigilo" será usado como referência aos softwares que realizam tanto cifração (sigilo) quanto a decifração de conteúdos presentes em documentos eletrônicos.

REQUISITO II: Software de Sigilo que faz uso de certificado digital deve atender aos requisitos técnicos específicos ora estabelecidos a seguir.

Nota: Este requisito não é testado separadamente e faz parte da Seção 2.2.

REQUISITO II.1: Software de Sigilo que utiliza certificado digital deve ser capaz de gerar e manipular documentos eletrônicos de acordo com os seguintes formatos:

- CMS "*EnvelopedData*"; ou
- CMS "*EncryptedData*".

Procedimentos de Ensaio para NSH 1:

EN.II.1.1: Verificar se a documentação do Software de Sigilo descreve a geração e manipulação de documentos eletrônicos de acordo com um dos formatos especificados no **REQUISITO II.1**.

EN.II.1.2: Verificar se o Software de Sigilo apresenta funcionalidades que permitem gerar e manipular documentos eletrônicos de acordo com um dos formatos especificados no **REQUISITO II.1**.

EN.II.1.3: Analisar os documentos gerados no ensaio **EN.II.01.02**, por meio de aplicação específica, e verificar se tais documentos estão de acordo com os padrões que definem os formatos especificados no **REQUISITO II.1**.

2.2.1 Formato CMS "EnvelopedData"

REQUISITO II.2: Software de Sigilo que realize envelope digital deve ser capaz de identificar e lidar com certificado digital ICP-Brasil de entidade final do tipo S1, S2, S3 ou S4.

Procedimentos de Ensaio para NSH 1:

EN.II.2.1: Verificar se a documentação do Software de Sigilo, descreve a identificação e manuseio de certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4.

EN.II.2.2: Realizar, por meio do Software de Sigilo, os processos de cifração e decifração de um documento eletrônico utilizando certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4. Em seguida, verificar se o Software de Sigilo é capaz de identificar o certificado digital utilizado, e também completar os processos de cifração e decifração de forma bem sucedida.

EN.II.2.3: Verificar no Software de Sigilo se existe alguma outra funcionalidade que evidencie a identifcação e manipulação de certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4.

REQUISITO II.3: O certificado digital utilizado em um processo de envelope digital deve estar em conformidade ao **REQUISITO I.3**. Além disso, o propósito "*keyEncipherment*" deve estar declarado na extensão "*Key Usage*".

Nota: Este requisito não é testado separadamente e faz parte da Seção 2.1.

REQUISITO II.4: Software de Sigilo que utilize certificado digital ICP-Brasil deve ser capaz de identificar e utilizar para os devidos controles, no mínimo, mas não limitado às seguintes extensões de certificados digitais previstas no padrão ITU-T X.509v3:

- "*Key Usage*";
- "*Certificate Policies*";
- "*Subject Alternative Name*";
- "*Basic Constraints*";
- "*CRL Distribution Points*";
- "*Authority Key Identifier*".

Procedimentos de Ensaio para NSH 1:

EN.II.4.1: Verificar se a documentação do Software de Sigilo descreve quais extensões de certificados digitais previstas no padrão ITU-T X.509v3, podem ser identificadas e utilizadas pelo Software de Sigilo.

EN.II.4.2: Verificar se o Software de Sigilo apresenta alguma funcionalidade que evidencie a identificação das extensões de certificados digitais ITU-T X.509v3 conforme o **REQUISITO II.4**.

EN.II.4.3: Verificar no Software de Sigilo as funcionalidades que permitem evidenciar a utilização das extensões de certificados digitais ITU-T X.509v3 conforme o **REQUISITO II.4**. Como exemplos destas funcionalidades pode-se citar: a verificação de certificados digitais, a cifração e decifração de um documento eletrônico ou visualização da política de uso do certificado digital. Além disso, tais funcionalidades podem ser analisadas com um certificado digital que apresenta condições de erro em seus campos.

REQUISITO II.5: A documentação que acompanha o produto (como por exemplo, manual de usuário, tópicos de ajuda etc) deve especificar se o Software de Sigilo suporta as seguintes funcionalidades:

1. Geração e verificação documentos eletrônicos sigilosos de acordo com o formato CMS "*EnvelopedData*";

2. Manipulação chaves criptográficas e certificados digitais armazenados em dispositivos criptográficos de hardware (por exemplo, cartões inteligentes ou *tokens*), assim como uma descrição de quais dispositivos podem ser utilizados pelo software;
3. Possibilidade de realização de envelope digital para múltiplos destinatários;
4. Verificação de revogação por meio da busca de LCR e/ou OCSP; e
5. Verificação de LCRs obtidas e respostas OCSP.

Procedimentos de Ensaio para NSH 1 e 2:

EN.II.5.1: Verificar se a documentação do Software de Sigilo descreve as funcionalidades especificadas no **REQUISITO II.5**.

2.2.1.1 Cifração

REQUISITO II.6: Software de Sigilo deve ser capaz de gerar conteúdo cifrado para vários destinatários no formato CMS "*EnvelopedData*".

Procedimentos de Ensaio para NSH 1:

EN.II.6.1: Verificar se a documentação do Software de Sigilo descreve a geração de conteúdo cifrado para vários destinatários no formato CMS "*EnvelopedData*".

EN.II.6.2: Verificar se o Software de Sigilo apresenta funcionalidades que permitem gerar conteúdo cifrado para vários destinatários no formato CMS "*EnvelopedData*".

EN.II.6.3: Analisar os conteúdos cifrados no ensaio **EN.II.06.02**, por meio de aplicação específica, e verificar se tais documentos estão de acordo com os padrões que definem os formatos especificados no **REQUISITO II.6**.

REQUISITO II.7: No momento que antecede a cifração de um conteúdo, o Software de Sigilo deve ser capaz de oferecer à entidade usuária externa as seguintes funcionalidades:

1. Permitir a visualização do conteúdo eletrônico a ser cifrado;
2. Possibilitar a escolha do certificado digital de sigilo que deve ser usado na cifração do conteúdo eletrônico;
3. Para cada certificado digital de sigilo escolhido pela entidade usuária externa:
   - Realizar a verificação do certificado conforme definido no **REQUISITO II.3;**
   - Alertar à entidade usuária externa, quando for o caso, quais requisitos de verificação de certificado digital não estão em conformidade ao **REQUISITO II.3**, ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado;
   - Quando for do desejo da entidade usuária externa, mostrar as informações sobre o certificado digital conforme **REQUISITO I.12**.

Procedimentos de Ensaio para NSH 1:

EN.II.7.1: Verificar se a documentação do Software de Sigilo descreve informações sobre as funcionalidades definidas pelo **REQUISITO II.7**.

EN.II.7.2: Verificar se o Software de Sigilo torna disponível à entidade usuária externa, uma interface que permita visualizar o conteúdo eletrônico a ser cifrado.

EN.II.7.3: Por meio do Software de Sigilo verificar se é solicitado à entidade usuária externa a escolha do certificado digital de sigilo antes da cifração do conteúdo eletrônico propriamente dita ser realizada.

EN.II.7.4: Verificar se o Software de Sigilo realiza a verificação de conformidade do certificado digital de sigilo escolhido conforme definido no **REQUISITO II.3**. Além disso, em caso de alguma não-conformidade em relação aos requisitos de verificação de certificado digital, por exemplo, assinatura do certificado não-válida, certificado expirado etc, deve-se também verificar se o Software de Sigilo alerta à

entidade usuária externa sobre tal situação, ressaltando que o certificado digital não está adequado e não deveria ser utilizado para o processo de cifração do conteúdo eletrônico.

EN.II.7.5: Verificar se o Software de Sigilo permite à entidade usuária externa, quando desejar, visualizar informações a respeito do certificado digital escolhido de acordo com o **REQUISITO I.12**.

RECOMENDAÇÃO II.1: Recomenda-se que o Software de Sigilo possa ser capaz de oferecer à entidade usuária externa opções de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*logs*) a respeito do processo de cifração.

Procedimentos de Ensaio para NSH 1:

EN.REC.II.1.1: Verificar se a documentação do Software de Sigilo, descreve a funcionalidade de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*log*), sobre um processo de cifração realizado.

EN.REC.II.1.2: Uma vez configurado no Software de Sigilo, verificar os aspectos da geração, visualização e/ou armazenamento de registros eletrônicos para diversos processos de cifração realizados.

2.2.1.2 Decifração

REQUISITO II.8: Antes da decifração de um pacote CMS "*EnvelopedData*", o Software de Sigilo deve ser capaz de:

1. Realizar a verificação do certificado digital conforme definido no **REQUISITO II.3**;
2. Alertar à entidade usuária externa, quando for o caso, quais requisitos de verificação de certificado digital não estão em conformidade ao **REQUISITO**

II.3, ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado.

Procedimentos de Ensaio para NSH 1:

EN.II.8.1: Verificar se a documentação do Software de Sigilo descreve informações sobre funcionalidades definidas pelo **REQUISITO II.8**.

EN.II.8.2: Verificar se o Software de Sigilo realiza a verificação de conformidade do certificado digital de sigilo escolhido conforme definido no **REQUISITO II.3**. Além disso, em caso de alguma não-conformidade em relação aos requisitos de verificação de certificado digital, por exemplo, assinatura do certificado não-válida, certificado expirado etc, deve-se também verificar se o Software de Sigilo alerta à entidade usuária externa sobre tal situação, ressaltando que o certificado digital não está adequado e não deveria ser utilizado para o processo de decifração do conteúdo eletrônico.

REQUISITO II.9: Ao decifrar pacotes CMS "*EnvelopedData*", o Software de Sigilo deve ser capaz de oferecer à entidade usuária externa as seguintes funcionalidades:

1. Permitir a visualização do conteúdo eletrônico decifrado;
2. Para o certificado digital de sigilo escolhido pela entidade usuária externa:
   - Quando for do desejo da entidade usuária externa, mostrar as informações sobre o certificado digital conforme **REQUISITO I.12**;
3. Mostrar o resultado do processo de decifração.

Procedimentos de Ensaio para NSH 1:

EN.II.9.1: Verificar se a documentação do Software de Sigilo descreve informações sobre as funcionalidades descritas no **REQUISITO II.9**.

EN.II.9.2: Verificar se o Software de Sigilo apresenta alguma funcionalidade que permite à entidade usuária externa visualizar o conteúdo eletrônico presente em um documento eletrônico decifrado.

EN.II.9.3: Verificar se o Software de Sigilo permite à entidade usuária externa, quando desejar, visualizar informações a respeito do certificado digital escolhido de acordo com o **REQUISITO I.12**.

EN.II.9.4: Verificar se o Software de Sigilo permite à entidade usuária externa visualizar o resultado do processo de decifração.

RECOMENDAÇÃO II.2: Recomenda-se que o Software de Sigilo possa ser capaz de oferecer à entidade usuária externa opções de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*logs*) a respeito do processo de decifração.

Procedimentos de Ensaio para NSH 1:

EN.REC.II.2.1: Verificar se a documentação do Software de Sigilo, descreve a funcionalidade de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*log*), sobre um processo de decifração realizado.

EN.REC.II.2.2: Uma vez configurado no Software de Sigilo, verificar os aspectos da geração, visualização e/ou armazenamento de registros eletrônicos para diversos processos de decifração realizados.

2.2.2 Formato CMS "EncryptedData"

REQUISITO II.10: Software de Sigilo que utilize chave assimétrica diretamente na codificação de conteúdo deve ser capaz de identificar e lidar com certificado digital ICP-Brasil de entidade final do tipo S1, S2, S3 ou S4.

Procedimentos de Ensaio para NSH 1:

EN.II.10.1: Verificar se a documentação do Software de Sigilo, descreve a identificação e manuseio de certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4.

EN.II.10.2: Realizar, por meio do Software de Sigilo, os processos de cifração e decifração de um documento eletrônico utilizando certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4. Em seguida, verificar se o Software de Sigilo é capaz de identificar o certificado digital utilizado, e também completar os processos de cifração e decifração de forma bem sucedida.

EN.II.10.3: Verificar no Software de Sigilo se existe alguma outra funcionalidade que evidencie a identificação e manipulação de certificados digitais ICP-Brasil do tipo S1, S2, S3 ou S4.

REQUISITO II.11: A documentação que acompanha o produto (como por exemplo, manual de usuário, tópicos de ajuda etc) deve especificar se o Software de Sigilo suporta as seguintes funcionalidades:

1. Geração e verificação de documentos eletrônicos sigilosos de acordo com o formato CMS "*EncryptedData*";
2. Manipulação de chaves criptográficas armazenadas em dispositivos criptográficos de hardware (por exemplo, cartões inteligentes ou *tokens*), assim como uma descrição de quais dispositivos podem ser utilizados pelo software.

Procedimentos de Ensaio para NSH 1 e 2:

EN.II.11.1: Verificar se a documentação do Software de Sigilo descreve as funcionalidades especificadas no **REQUISITO II.11**.

REQUISITO II.12: O certificado digital utilizado em um processo de cifração que está baseado no uso de chaves assimétricas deve estar em conformidade ao **REQUISITO I.3**. Além disso, o propósito "*dataEncipherment*" deve estar declarado na extensão "*Key Usage*".

Nota: Este requisito não é testado separadamente e faz parte da Seção 2.1.

2.2.2.1 Cifração

REQUISITO II.13: No momento que antecede a cifração de um conteúdo utilizando uma chave assimétrica, o Software de Sigilo deve ser capaz de oferecer à entidade usuária externa as seguintes funcionalidades:

1. Permitir a visualização do conteúdo eletrônico a ser cifrado;
2. Possibilitar a escolha do certificado digital de sigilo que deve ser usado na cifração do conteúdo eletrônico;
3. Para o certificado digital de sigilo escolhido pela entidade usuária externa:
   - Realizar a verificação do certificado conforme definido no **REQUISITO II.12;**
   - Alertar à entidade usuária externa, quando for o caso, quais requisitos de verificação de certificado digital não estão em conformidade ao **REQUISITO II.12**, ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado;
   - Quando for do desejo da entidade usuária externa, mostrar as informações sobre o certificado digital conforme **REQUISITO I.12**.

Procedimentos de Ensaio para NSH 1:

EN.II.13.1: Verificar se a documentação do Software de Sigilo descreve informações sobre funcionalidades definidas pelo **REQUISITO II.13**.

EN.II.13.2: Verificar se o Software de Sigilo torna disponível à entidade usuária externa, uma interface que permita visualizar o conteúdo eletrônico a ser cifrado.

EN.II.13.3: Por meio do Software de Sigilo verificar se é solicitado à entidade usuária externa a escolha do certificado digital de sigilo antes da cifração do conteúdo eletrônico propriamente dita ser realizada.

EN.II.13.4: Verificar se o Software de Sigilo realiza a verificação de conformidade do certificado digital de sigilo escolhido conforme definido no **REQUISITO II.12**. Além disso, em caso de alguma não-conformidade em relação aos requisitos de

verificação de certificado digital, por exemplo, assinatura do certificado não-válida, certificado expirado etc, deve-se também verificar se o Software de Sigilo alerta à entidade usuária externa sobre tal situação, ressaltando que o certificado digital não está adequado e não deveria ser utilizado para o processo de cifração do conteúdo eletrônico.

EN.II.13.5: Verificar se o Software de Sigilo permite à entidade usuária externa, quando desejar, visualizar informações a respeito do certificado digital escolhido de acordo com o **REQUISITO I.12**.

RECOMENDAÇÃO II.3: Recomenda-se que o Software de Sigilo possa ser capaz de oferecer à entidade usuária externa opções de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*logs*) a respeito do processo de cifração.

Procedimentos de Ensaio para NSH 1:

EN.REC.II.3.1: Verificar se a documentação do Software de Sigilo, descreve a funcionalidade de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*log*), sobre um processo de cifração realizado.

EN.REC.II.3.2: Uma vez configurado no Software de Sigilo, verificar os aspectos da geração, visualização e/ou armazenamento de registros eletrônicos para diversos processos de cifração realizados.

2.2.2.2 Decifração

REQUISITO II.14: Antes da decifração de um pacote CMS "*EncryptedData*", o Software de Sigilo deve ser capaz de:

1. Realizar a verificação do certificado digital conforme definido no **REQUISITO II.12**;

2. Alertar à entidade usuária externa, quando for o caso, quais requisitos de verificação de certificado digital não estão em conformidade ao **REQUISITO II.12**, ressaltando que o certificado digital não passou pelo processo de validação e não deveria ser utilizado.

Procedimentos de Ensaio para NSH 1:

EN.II.14.1: Verificar se a documentação do Software de Sigilo descreve informações sobre funcionalidades definidas pelo **REQUISITO II.14**.

EN.II.14.2: Verificar se o Software de Sigilo realiza a verificação de conformidade do certificado digital de sigilo escolhido conforme definido no **REQUISITO II.12**. Além disso, em caso de alguma não-conformidade em relação aos requisitos de verificação de certificado digital, por exemplo, assinatura do certificado não-válida, certificado expirado etc, deve-se também verificar se o Software de Sigilo alerta à entidade usuária externa sobre tal situação, ressaltando que o certificado digital não está adequado e não deveria ser utilizado para o processo de decifração do conteúdo eletrônico.

REQUISITO II.15: Ao decifrar pacotes CMS "*EncryptedData*", o Software de Sigilo deve ser capaz de oferecer à entidade usuária externa as seguintes funcionalidades:

1. Permitir a visualização do conteúdo eletrônico decifrado;
2. Para o certificado digital de sigilo escolhido pela entidade usuária externa:
   - Quando for do desejo da entidade usuária externa, mostrar as informações sobre o certificado digital conforme **REQUISITO I.12**;
3. Mostrar o resultado do processo de decifração.

Procedimentos de Ensaio para NSH 1:

EN.II.15.1: Verificar se a documentação do Software de Sigilo descreve informações sobre as funcionalidades descritas no **REQUISITO II.15**.

EN.II.15.2: Verificar se o Software de Sigilo apresenta alguma funcionalidade que permite à entidade usuária externa visualizar o conteúdo eletrônico presente em um documento eletrônico decifrado.

EN.II.15.3: Verificar se o Software de Sigilo permite à entidade usuária externa, quando desejar, visualizar informações a respeito do certificado digital escolhido de acordo com o **REQUISITO I.12**.

EN.II.15.4: Verificar se o Software de Sigilo permite à entidade usuária externa visualizar o resultado do processo de decifração.

RECOMENDAÇÃO II.4: Recomenda-se que o Software de Sigilo possa ser capaz de oferecer à entidade usuária externa opções de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*logs*) a respeito do processo de decifração.

Procedimentos de Ensaio para NSH 1 e 2:

EN.REC.II.4.1: Verificar se a documentação do Software de Sigilo, descreve a funcionalidade de configurar a geração, visualização e/ou armazenamento de registros eletrônicos (*log*), sobre um processo de decifração realizado.

EN.REC.II.4.2: Uma vez configurado no Software de Sigilo, verificar os aspectos da geração, visualização e/ou armazenamento de registros eletrônicos para diversos processos de decifração realizados.

3 Referências bibliográficas

[1] COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 38, de 18 de abril de 2006: Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.** Brasília: ICP-BRASIL, 2006. 21 p.

[2] COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília: ICP-BRASIL, 2006. 20 p.

[3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – ISO/IEC 8825-1.** Genève, Switzerland, Reference Number: ISO/IEC 8825-1:2002.

[4] THE INTERNET ENGINEERING TASK FORCE. Freed, N. e Borenstein, N. **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.** RFC 2045, Category: Standards Track, November 1996. Disponível em <http://www.ietf.org/rfc/rfc2045.txt>. Acesso em: 30.jan.2006.

[5] THE INTERNET ENGINEERING TASK FORCE. Linn, J. **Privacy Enhancement for Internet Electronic Mail:** Part I: Message Encryption and Authentication Procedures. RFC 1421, February 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.jan.2006.

[6] RSA LABORATORIES. PKCS #7: **Cryptographic Message Syntax Standard.** Version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.jan.2006.

[7] THE INTERNET ENGINEERING TASK FORCE. Housley, R.; Polk, W.; Ford, W. e Solo, D. **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.** RFC 3280, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 30.jan.2006.

[8] THE INTERNET ENGINEERING TASK FORCE. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. e Adams, C. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.** RFC 2560, Category: Standards Track, June 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 30.jan.2006.

[9] THE INTERNET ENGINEERING TASK FORCE. Housley, R. **Cryptographic Message Syntax (CMS).** RFC 3852, Category: Standards Track, July 2004. Disponível em <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 30.jan.2006.

[10] IN 01/2007 – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 01/2007: Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** DOC-ICP-10.01. Brasília. ICP-Brasil: 2007.

[11] IN 02/2007 – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 02/2007: Estrutura normativa técnica e níveis de segurança de homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** DOC ICP-10.02. ICP-Brasil: 2007.

[12] IN 04/2007 – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução Normativa 04/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de softwares de assinatura digital, sigilo e autenticação no âmbito da ICP-Brasil**. DOC-ICP-10.04. ICP-Brasil: 2007.

[13]GLOSSÁRIO ICP-BR – INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. **Glossário ICP-Brasil.** Versão 1.2. Brasília. ICP – BR: 2007.