Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 6 - Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação 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.06	**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).

Listas de Ilustrações

Lista de Tabelas

1 Introdução

Este manual descreve os requisitos técnicos a serem observados no processo de homologação de software de sigilo no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

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 Objetivo da homologação

O objetivo do processo de homologação de software de sigilo é propiciar a interoperabilidade e operação segura por meio da avaliação técnica de aderência aos requisitos técnicos definidos neste manual.

1.2 Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos definidos neste manual que devem ser atendidos por um software de sigilo para prover interoperabilidade e operação segura.

Estes requisitos técnicos são avaliados pela execução de ensaios de aderência aos requisitos técnicos. Para a realização destes ensaios, a parte interessada deve submeter ao processo de homologação um conjunto de materiais requisitados, efetuando o depósito destes materiais no LEA.

1.3 Escopo deste manual

O escopo dos requisitos técnicos e da avaliação de software de sigilo se aplicam aos seguintes componentes de software que realizam:

- Manipulação de certificados digitais;
- verificação de revogação de certificados digitais;
- manipulação de senhas e dados sensíveis;
- geração e verificação de assinatura digital de documentos eletrônicos; e
- cifração e decifração de documentos eletrônicos.

O resultado do processo de homologação de software de sigilo informa a aderência aos requisitos técnicos definidos neste manual.

1.4 Estruturação do MCT 6 – Volume I

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

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de software de sigilo;
- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de software de sigilo;
- Referência Bibliográfica: Descreve as referências bibliográficas que foram utilizadas na elaboração deste manual.

2 Parte 1

Requisitos técnicos 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 sigilo.

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

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.

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*).

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**).

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.

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.

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.

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.

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.

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.

REQUISITO I.10: [requisito baseado na RESOLUÇÃO Nº 41, de 18 de Abril de 2006 - Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil] 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.

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.

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**.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.*

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.

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

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*.

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.

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

REQUISITO I.30: Software ICP-Brasil deve possuir 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.

REQUISITO I.32: Software ICP-Brasil deve permitir a entidade usuária externa 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.

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*".

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.

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*".

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*".

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.

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*".

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**.

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.

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.

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.

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.

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.

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.

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*".

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**.

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.

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.

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.

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.

3 Parte 2

Material e documentação técnica a serem depositados para a execução do processo de homologação de software de sigilo no âmbito da ICP-Brasil

3.1 Introdução

Esta parte detalha os materiais e a documentação técnica a serem depositados pela parte interessada junto ao LEA para a execução dos processos de homologação de software de sigilo no âmbito da ICP-Brasil.

Os materiais e a documentação técnica referidos são classificadas em três categorias:

1. Documentação técnica: corresponde aos documentos de natureza técnica referentes aos dispositivos a serem submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formato eletrônico, devem estar armazenados, preferencialmente, em mídia tipo “leitura-somente” (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;
2. componentes em softwares executáveis: corresponde a todo software executável, solicitado por este documento, referente ao funcionamento do objeto de homologação. Devem ser depositados, obrigatoriamente, em formato eletrônico e armazenados, preferencialmente, em mídia tipo “leitura-somente” (*read-only*).

Para os NSHs 2 e 3, a parte interessada pode depositar o código fonte de duas maneiras diferentes:

1. Linguagem de alto nível: Código fonte deve ser depositado, por exemplo, em linguagem C, C++ ou Java. Se o código fonte estiver escrito em linguagem proprietária, o respectivo manual desta linguagem deve estar contido na documentação;
2. linguagem de baixo nível: Código fonte deve ser depositado em linguagem *assembler*, porém acompanhado do respectivo manual das instruções desta linguagem.

OBSERVAÇÃO: Para software de assinatura digital, a parte interessada deve indicar no formulário de depósito a plataforma de sistema operacional e sua versão a ser utilizada na análise de conformidade.

3.2 Materiais e documentação técnica a serem depositados

3.2.1 Documentação técnica

3.2.1.1 Nível de Segurança de Homologação 1

Os seguintes documentos técnicos devem ser depositados junto ao LEA pela parte interessada:

- Projeto de software: Projeto de software, como por exemplo, casos de uso *(use cases),* diagramas de sequência e diagramas de estado e outros documentos envolvidos na construção do software;
- Manual de usuário e instalação: Manual de usuário e instalação idêntico ao fornecido ao usuário;
- Manual de instalação e configuração de softwares adicionais para interação com hardware criptográfico (quando aplicável): Manual de instalação e configuração de softwares adicionais, tais como, Provedores de Serviço para interação com hardwares criptográficos que contém, por exemplo, certificados ICP-Brasil tipo A2, A3, A4 e/ou S2, S3, S4;
- Documentação técnica de homologações obtidas: Documentação técnica de homologações obtidas para o software e emitidas por entidades independentes, como por exemplo, *Common Criteria*;
- Outros documentos: Projetos técnicos e suas especificações que a Parte Interessada julgar necessários para completar toda documentação técnica exigida.

3.2.1.2 Níveis de Segurança de Homologação 2 e 3

Adicionalmente à documentação técnica solicitada no NSH 1, os seguintes itens devem ser depositados junto ao LEA pela parte interessada:

- Código fonte do software ICP-Brasil.

3.2.2 Componentes em software executável

Independentemente do NSH escolhido pela parte interessada, os seguintes componentes em softwares executáveis devem ser depositados junto ao LEA:

- Software ICP-Brasil: Software a ser homologado;
- Softwares de interação com hardware criptográfico (quando aplicável): Quando aplicável, a Parte Interessada deve fornecer todo software necessário para interação com hardwares criptográficos, como por exemplo, CSP para interação com cartões inteligentes ou *tokens* criptográficos.

3.2.3 Quantidade de materiais e documentação técnica a serem depositados para o software de sigilo

A Tabela 1 apresenta a quantidade de materiais e documentação técnica a serem depositados pela parte interessada referente ao processo de homologação de software de sigilo que se resumem em:

- Documentação técnica:
  - documentos impressos: devem ser entregues cópias de igual teor (por exemplo, duas cópias impressas do manual do usuário do software ICP-Brasil);
  - documentos eletrônicos: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o manual de usuário, manual de instalação/configuração e código fonte do software ICP-Brasil);
- componentes em softwares executáveis: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como componentes em softwares executáveis o software ICP-Brasil e software de interação com hardware criptográfico).

Tabela 1. Quantidade de material e documentação técnica a serem depositados pela parte interessada junto ao LEA referente ao processo de homologação de software de sigilo

Requisito de depósito	**Material e documentos técnicos a serem depositados pela parte interessada – NSH 1**	**Quantidade**
1	Projeto de software	2 cópias
2	Manual de usuário/instalação	2 cópias
3	Manual de instalação/configuração de softwares adicionais para interação com hardware criptográfico (quando aplicável)	
4	Documentação técnica de homologações obtidas	2 cópias
5	Outros documentos	2 cópias
Requisito de depósito	**Material e documentos técnicos a serem depositados pela parte interessada – NSH 2 e 3**	**Quantidade**
6	Código fonte do software de sigilo	2 cópias
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NSH 1, 2 e 3**	**Quantidade**
7	Software ICP-Brasil	2 cópias
8	Softwares de interação com hardware criptográfico (quando aplicável)	2 cópias

4 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.