**Infra-Estrutura de Chaves Públicas Brasileira**

# PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL (DOC-ICP-10.05)

**Versão 1.0**

**11 de dezembro de 2007**

# Índice

# 1. Disposições Gerais

1.1 Este documento se aplica aos processos de homologação de Módulos de Segurança Criptográfica (MSC) no âmbito da ICP-Brasil, compreendendo-se por MSC um servidor ou placa auxiliar de segurança fisicamente seguro, resistente à violação que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltados para utilização em uma Infra-estrutura de Chaves Públicas (ICP).

1.2 Este documento define o conjunto de requisitos técnicos, material e documentação técnicos para depósito e ensaios de conformidade, bem como os volumes do Manual de Condutas Técnicas do ITI aplicáveis aos processos de homologação dos objetos citados no parágrafo 1.1.

1.3 Suplementa, no que se refere aos objetos de homologação citados no parágrafo 1.1, o documento REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [1].

# 2. Requisitos Técnicos

2.1 Os requisitos técnicos a serem observados nos processos de homologação dos objetos citados no parágrafo 1.1 são:

a) aderência aos requisitos de segurança, gerenciamento, restrição de substâncias nocivas e documentação conforme definido no documento citado no parágrafo 3.2; e

b) aderência a interfaces de interoperabilidade específicas, das quais ao menos uma deve ser suportada:

Aderência aos requisitos de interoperabilidade ao nível de PKCS#11, informando o ambiente operacional no qual foi analisada a interoperabilidade;
Aderência aos requisitos de interoperabilidade ao nível de CryptoAPI, informando o ambiente operacional no qual foi analisada a interoperabilidade;
Aderência aos requisitos de interoperabilidade ao nível de JCE, informando o ambiente operacional no qual foi analisada a interoperabilidade;
Aderência aos requisitos de interoperabilidade ao nível de OpenSSL, informando o ambiente operacional no qual foi analisada a interoperabilidade;
Aderência aos requisitos de interoperabilidade ao nível de uma API proprietária, caso utilizada, informando o ambiente operacional no qual foi analisada a interoperabilidade;

2.2 Os requisitos técnicos estabelecidos por este documento têm caráter macroestrutural, ou seja, representam, na verdade, um conjunto de requisitos técnicos específicos e pormenorizados. Para conhecer o completo detalhamento destes, consultar os documentos citados no item 3.2.

# 3. Material e documentação técnicos a serem depositados

3.1 Para efeitos do disposto no parágrafo 8.6 dos PROCEDIMENTOS ADMINISTRATIVOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [2] quanto aos processos de homologação dos sistemas de que trata este documento, o responsável técnico da parte interessada deverá apresentar ao

LEA para depósito, o material e documentação técnicos, conforme descritos a seguir:

a) FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [6], devidamente preenchido e assinado, em quatro vias;

b) amostras de MSCs a serem submetidas ao processo de homologação, bem como leitoras de cartões inteligentes, cartões e *tokens* criptográficos para apoio no processo de controle de acesso ao módulo criptográfico, segundo o disposto no documento citado no parágrafo 3.2 ;

c) documentação técnica, segundo o disposto no documento citado no parágrafo 3.2; e

d) componentes em softwares executáveis, segundo o disposto no documento citado no parágrafo 3.2.

3.2 O material e documentação técnicos estabelecidos por este documento têm caráter macroestrutural, ou seja, representam, na verdade, um conjunto de materiais de hardware, software e documentos técnicos específicos e pormenorizados. Para conhecer o completo detalhamento destes, consultar o documento MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICOS (MSC) NO ÂMBITO DA ICP-BRASIL [4].

3.3 O documento referido no parágrafo anterior poderá ser atualizado, a qualquer tempo, pelo ITI, de forma a melhor explicitar e explicar os requisitos técnicos e recomendações a serem observados nas avaliações de conformidade do dispositivo de que trata este documento, bem como o material e documentação técnicos a serem depositados.

3.4 Para alterar, incluir ou excluir qualquer requisito técnico, material ou documentação de caráter macroestrutural, o ITI deverá editar nova instrução normativa.

## 4. Ensaios para avaliação de conformidade

4.1 A avaliação de conformidade dos dispositivos de que trata este documento será realizada pelos LEA, tendo por referência os ensaios descritos no documentos MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II: PROCEDIMENTOS DE ENSAIO PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICOS (MSC) NO ÂMBITO DA ICP-BRASIL [5].

4.2 O documento referido no parágrafo anterior poderá ser atualizados pelo ITI, a qualquer tempo, de forma a melhor explicitar e explicar os ensaios técnicos a serem empregados nas avaliações de conformidade aos requisitos técnicos e recomendações estabelecidos para o dispositivo de que trata este documento.

## 5. Nível de Segurança de Homologação

5.1 No FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [3] a Parte Interessada deverá definir qual o Nível de Segurança de Homologação (NSH) pretendido para o objeto a ser homologado, conforme documento 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 [6] .

5.2 A escolha do NSH influenciará no tipo e quantidade de materiais a serem depositados para avaliação da conformidade.

## 6. Nível de Segurança Física

6.1 No FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL [3] a Parte Interessada deverá definir qual o Nível de Segurança Física (NSF) pretendido para o objeto a ser homologado.

6.2 A escolha do NSF influenciará no tipo e quantidade de materiais a serem depositados para avaliação da conformidade.

6.3 A escolha do NSF influenciará no nível de análise de conformidade a ser realizada sobre os mecanismos de segurança física dos MSC.

## 7. Documentos referenciados

7.1 O documento abaixo é aprovado por Resolução do Comitê-Gestor da ICP-Brasil, podendo ser alterado, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desse documento e a Resolução que a aprovou.

| Ref. | Nome do documento | Código |
|---|---|---|
| [1] | REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL | DOC-ICP-10 |

7.2 Os documentos abaixo são aprovados por Instrução Normativa do ITI, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e a Instrução Normativa que a aprovou.

| Ref. | Nome do documento | Código |
|---|---|---|
| [2] | 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 |
| [6] | 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 |

6.3 Os documentos abaixo são disponibilizados pelo ITI, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

| Ref. | Nome do documento | Código |
|---|---|---|
| [3] | FORMULÁRIO DE DEPÓSITO DE SISTEMA OU EQUIPAMENTO DE CERTIFICAÇÃO DIGITAL | ADE-ICP-10.03.A |
| [4] | MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICOS (MSC) NO ÂMBITO DA ICP-BRASIL | MCT 7 – Vol. I |
| [5] | MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II: PROCEDIMENTOS DE ENSAIO PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICOS (MSC) NO ÂMBITO DA ICP-BRASIL | MCT 7 - Vol.II |