Infraestrutura de Chaves Públicas Brasileira

PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE EQUIPAMENTOS CRIPTOGRÁFICOS NÃO CONTEMPLADOS EM MANUAL DE CONDUTA TÉCNICA ESPECÍFICOS

DOC-ICP-10.08

Versão 1.0

29 de abril de 2014

SUMÁRIO

1. CONTROLE DE ALTERAÇÕES....2
1. LISTA DE SIGLAS e ACRÔNIMOS....3
1. DISPOSIÇÕES GERAIS....4
2. REQUISITOS TÉCNICOS....4
3. MATERIAL E DOCUMENTAÇÃO TÉCNICOS A SEREM DEPOSITADOS....5
4. ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE....6
5. NÍVEL DE SEGURANÇA DE HOMOLOGAÇÃO....6
6. DOCUMENTOS REFERENCIADOS....7

1. CONTROLE DE ALTERAÇÕES

Ato que Aprovou A Alteração	*Item Alterado*	*Descrição da Alteração*
IN Nº 02/2014, de 29.04.2014		Procedimentos Para Homologação de Equipamentos não Contemplados nos Manuais de Conduta Técnica, no Âmbito Da ICP-Brasil (DOC-ICP-10.08).

1. LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
CG-ICP-BRASIL	Comitê Gestor da ICP-Brasil
FIPS	*Federal Information Processing Standards*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electrotechnical Commissiona*
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
LEA	Laboratório de Ensaios e Auditoria
MSC	Módulo de Segurança Criptográfica
MCT	Manual de Conduta Técnica
NSH	Nível de Segurança de Homologação

1. DISPOSIÇÕES GERAIS

1.1 Este documento se aplica aos processos de homologação de todo e qualquer equipamento ou dispositivo criptográfico ***não categorizados em Manual de Conduta Técnica (MCT) específico***.

1.1.1 Os equipamentos ou dispositivos criptográficos tratados neste regulamento devem ser submetidos previamente ao LEA para enquadramento e avaliação preliminar quanto à viabilidade de homologação.

1.2 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 de equipamentos ou dispositivos criptográficos são:

a) aderência aos requisitos de segurança estabelecidos pelo padrão FIPS 140-2, de acordo com o escopo e os requisitos complementares, quanto às áreas de atuação do padrão referido, definidos no documento citado no parágrafo 3.2;

b) aderência aos requisitos de interoperabilidade estabelecidos, derivados e complementares aos padrões ISO/IEC 7816, ISO/IEC 14443 e PC/SC versão 1.0, de acordo com o estabelecido pelo documento citado no parágrafo 3.2;

c) aderência aos requisitos de gerenciamento estabelecidos e detalhados pelo documento citado no parágrafo 3.2;

d) aderência aos requisitos funcionais estabelecidos e detalhados pelo documento citado no parágrafo 3.2;

e) aderência aos requisitos de documentação estabelecidos e detalhados pelo documento citado no parágrafo 3.2.

2.2 Os requisitos técnicos estabelecidos por este documento têm caráter macroestrutural. 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 documento **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 equipamentos ou dispositivos 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 [3]**, devidamente preenchido e assinado, em quatro vias;

b) amostras de cada modelo e/ou versão do dispositivo a ser submetido ao processo de homologação, segundo o disposto nos documentos citados no parágrafo 3.2;

c) documentação técnica, segundo o disposto nos documentos citados no parágrafo 3.2; e

d) componentes em softwares executáveis, segundo o disposto nos documentos citados no parágrafo 3.2.

3.2 Para conhecer o completo detalhamento de materiais de hardwares, softwares e documentos técnicos consultar os seguintes manuais:

a) MANUAL DE CONDUTAS TÉCNICAS 1 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE CARTÕES CRIPTOGRÁFICOS (*SMART CARDS*) NO ÂMBITO DA ICP-BRASIL [4].

b) MANUAL DE CONDUTAS TÉCNICAS 2 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE LEITORAS DE CARTÕES INTELIGENTES NO ÂMBITO DA ICP-BRASIL [5].

c) MANUAL DE CONDUTAS TÉCNICAS 3 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE *TOKENS* CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL [6].

d) MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE MSC NO ÂMBITO DA ICP-BRASIL [12].

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

3.4 Os equipamentos ou dispositivos criptográficos enquadrados neste regulamento devem atender ao conjunto de requisitos estabelecidos nos MCT-1 ou MCT-2 ou

MCT-3 ou MCT-7, conforme aderência em termos funcionais, de gerenciamento, de segurança e interoperabilidade (quando aplicável) sujeitos à ratificação ou não pelo ITI quando do processo de homologação.

3.4.1 Os requisitos de segurança criptográfica são obrigatórios.

3.4.2 O LEA deverá justificar o respectivo enquadramento do dispositivo criptográfico ao MCT referenciado.

3.5 Admite-se que alguns dos requisitos constantes no MCT utilizado como referência, eventualmente, não se apliquem aos dispositivos criptográficos sujeitos a este regulamento. Neste caso, caberá ao LEA registrar no Laudo de Conformidade que tal requisito não se aplica ao equipamento, com a respectiva ressalva e justificativa.

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 nos documentos:

a) MANUAL DE CONDUTAS TÉCNICAS 1 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE CARTÕES CRIPTOGRÁFICOS (*SMART CARDS*) NO ÂMBITO DA ICP-BRASIL [7].

b) MANUAL DE CONDUTAS TÉCNICAS 2 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE LEITORAS DE CARTÕES INTELIGENTES NO ÂMBITO DA ICP-BRASIL [8].

c) MANUAL DE CONDUTAS TÉCNICAS 3 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE *TOKENS* CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL [9].

d) MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE MSC NO ÂMBITO DA ICP-BRASIL [11].

4.2 Os documentos referidos no parágrafo anterior poderão ser atualizados pelo ITI, a qualquer tempo, de forma a melhor explicitar os ensaios técnicos a serem empregados nas avaliações de conformidade aos requisitos técnicos e recomendações estabelecidos para os dispositivos 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 TÉCNICAE NÍVEIS DE SEGURANÇA DE HOMOLOGAÇÃO A SEREM UTILIZADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [10].**

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

6. DOCUMENTOS REFERENCIADOS

6.1 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

6.2 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
[10]	**ESTRUTURA NORMATIVA TÉCNICA E NÍVEIS DE SEGURANÇA DE HOMOLOGAÇÃO A SEREM UTILIZADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE**	DOC-ICP-10.02

Ref.	Nome do documento	Código
	CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	

6.3 Os documentos abaixo são publicados 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 1 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE CARTÕES CRIPTOGRÁFICOS (*SMART CARDS*) NO ÂMBITO DA ICP-BRASIL**	MCT 1 – Vol. I
[5]	**MANUAL DE CONDUTAS TÉCNICAS 2 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE LEITORAS DE CARTÕES INTELIGENTES NO ÂMBITO DA ICP- BRASIL**	MCT 2 – Vol. I
[6]	**MANUAL DE CONDUTAS TÉCNICAS 3 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE *TOKENS* CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL**	MCT 3 – Vol.I
[7]	**MANUAL DE CONDUTAS TÉCNICAS 1 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE CARTÕES CRIPTOGRÁFICOS (*SMART CARDS*) NO ÂMBITO DA ICP-BRASIL**	MCT 1 – Vol.II
	MANUAL DE CONDUTAS TÉCNICAS 2 – VOLUME II: PROCEDIMENTOS DE	

Ref.	Nome do documento	Código
[8]	**ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE LEITORAS DE CARTÕES INTELIGENTES NO ÂMBITO DA ICP-BRASIL**	MCT 2 – Vol.II
[9]	**MANUAL DE CONDUTAS TÉCNICAS 3 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE *TOKENS* CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL**	MCT 3 – Vol.II
[11]	**MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME II: PROCEDIMENTOS DE ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE AOS REQUISITOS TÉCNICOS DE *MSC* NO ÂMBITO DA ICP-BRASIL**	MCT 7 – Vol.II
[12]	**MANUAL DE CONDUTAS TÉCNICAS 7 – VOLUME I: REQUISITOS, MATERIAIS E DOCUMENTOS TÉCNICOS PARA HOMOLOGAÇÃO DE *MSC* NO ÂMBITO DA ICP-BRASIL**	MCT 7 – Vol.I