



**Infraestrutura de Chaves Públicas Brasileira**

**PADRÕES E PROCEDIMENTOS TÉCNICOS  
A SEREM OBSERVADOS  
NOS PROCESSOS DE HOMOLOGAÇÃO  
DE CARTÕES INTELIGENTES (*SMART CARDS*),  
LEITORAS DE CARTÕES INTELIGENTES  
E *TOKENS* CRIPTOGRÁFICOS  
NO ÂMBITO DA ICP-BRASIL**

**DOC-ICP-10.03**

**Versão 3.0**

**11 de dezembro de 2007**



# Infraestrutura de Chaves Públicas Brasileira

## SUMÁRIO

1. DISPOSIÇÕES GERAIS.....	4
2. REQUISITOS TÉCNICOS.....	4
3. MATERIAL E DOCUMENTAÇÃO TÉCNICOS A SEREM DEPOSITADOS.....	4
4. ENSAIOS PARA AVALIAÇÃO DE CONFORMIDADE.....	5
5. NÍVEL DE SEGURANÇA DE HOMOLOGAÇÃO.....	6
6. DOCUMENTOS REFERENCIADOS.....	6



## Infraestrutura de Chaves Públicas Brasileira

### CONTROLE DE ALTERAÇÕES

<i>Resolução ou IN que aprovou alteração</i>	<i>Item Alterado</i>	<i>Descrição da Alteração</i>
Instrução Normativa nº 03, de 11.12.2007 (Versão 3.0)		Aprova a versão 3.0 dos Requisitos Técnicos a serem observados nos processos de homologação de cartões inteligentes (smart cards)m leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil, na forma definida pelo anexo.
Instrução Normativa nº 03, de 14.02.2006 (Versão 2.0)	Item 8.3, “Meios de Acesso: Especificações Técnicas para Smart Cards, Tokens e Cartões e m Geral”, do Documento de Referência da ePING– Versão 1.5	Aprova a versão 2.0 dos Requisitos Técnicos a serem observados nos processos de homologação de cartões inteligentes (smart cards), leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil, na forma definida pelo anexo.
Instrução Normativa nº 05, de 22.04.2005 (Versão 1.0)		Estabelece os requisitos técnicos a serem observados nos processos de homologação de cartões inteligentes (smart cards)m leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil, na forma definida pelo anexo.



## Infraestrutura de Chaves Públicas Brasileira

### LISTA DE SIGLAS

SIGLA	DESCRIÇÃO
CG	Comitê-Gestor da ICP-Brasil
FIPS	<i>Federal Information Processing Standards</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	<i>International Electrotechnical Commission</i>
ITI	Instituto Nacional de Tecnologia da Informação
ISO	<i>International Organization for Standardization</i>
LEA	Laboratório de Ensaios e Auditoria
MCT	Manual de Conduta Técnica
NSH	Nível de Segurança de Homologação
PC	Política de Certificado
SC	<i>Smart Card</i>



# Infraestrutura de Chaves Públicas Brasileira

## 1. DISPOSIÇÕES GERAIS

1.1 Este documento se aplica aos processos de homologação de cartões criptográficos (smart cards), leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil.

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

2.2. Os requisitos técnicos a serem observados no processo de homologação de leitora de cartões inteligentes são:

- a) aderência às recomendações de segurança estabelecidas e detalhadas pelo documento citado no parágrafo 3.2;
- b) aderência aos requisitos de interoperabilidade estabelecidos, derivados e complementares aos padrões ISO/IEC 7816 e PC/SC versão 1.0, de acordo com o estabelecido pelo documento citado no parágrafo 3.2;
- c) aderência aos requisitos de documentação estabelecidos e detalhados pelo documento citado no parágrafo 3.2.

2.3. 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



## Infraestrutura de Chaves Públicas Brasileira

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 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 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 os documentos:

- 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].

3.3. Os documentos referidos no parágrafo anterior poderão ser atualizados, a qualquer tempo, pelo ITI, de forma a melhor explicitar e explicar os requisitos técnicos e recomendações a serem observados nas avaliações de conformidade dos dispositivos 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 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].



## Infraestrutura de Chaves Públicas Brasileira

- 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].

4.2. Os documentos referidos no parágrafo anterior poderão 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 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 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 [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	DOC-ICP-10.01



## Infraestrutura de Chaves Públicas Brasileira

Ref.	Nome do documento	Código
	SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	
[10]	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 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
[8]	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	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