



Infra-Estrutura de Chaves Públicas Brasileira

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS

DA ICP-BRASIL

(DOC ICP-01.01)

Versão 1.0

18 de maio de 2006

1. Disposições Gerais

Os padrões e algoritmos criptográficos a serem empregados em todos os processos que envolvem geração de chaves criptográficas, solicitação, emissão e revogação de certificados digitais no âmbito da ICP-Brasil devem observar o disposto neste documento.

2. Formatos de Arquivos e Algoritmos Criptográficos

A tabela a seguir relaciona os padrões de formatos de arquivos e algoritmos criptográficos com sua utilização na ICP-Brasil e com os documentos normativos que tratam dessa utilização.

Utilização	Algoritmo / Padrão	Normativo
Formato para entrega de certificados emitidos pela AC	Padrão PKCS#7	DOC-ICP-01 - item 4.2.4 DOC-ICP-01 - item 6.1.4.1 DOC-ICP-04 - item 6.1.4 DOC-ICP-05 - item 6.1.4
Formato de solicitação de certificados à AC	Padrão PKCS#10	DOC-ICP-01 - item 4.1.2 DOC-ICP-01 - item 6.1.3.1 DOC-ICP-04 - item 6.1.3 DOC-ICP-05 - item 4.1.3
Algoritmo criptográfico e tamanho das chaves para geração de chaves assimétricas de AC	RSA 2048 bits	DOC-ICP-01 - item 6.1.1.3 DOC-ICP-04 - item 6.1.1.3 DOC-ICP-01 - item 6.1.5 DOC-ICP-05 - item 6.1.5
Algoritmo criptográfico e tamanhos mínimos para geração de chaves assimétricas de usuário final	RSA 1024 bits: A1, A2, A3, S1, S2, S3 RSA 2048 bits: A4, S4	DOC-ICP-04 - item 6.1.5.2
Algoritmos criptográficos para assinatura de certificados de AC	SHA-1 com RSA	DOC-ICP-01 - item 7.1.3 DOC-ICP-01 - item 7.2.3 DOC-ICP-05 - item 7.2.3
Algoritmos criptográficos para assinatura de certificados de usuário final	SHA-1 com RSA SHA-1 com DSA	DOC-ICP-04 - item 7.1.3
Algoritmo simétrico para guarda da chave	3-DES, IDEA,	DOC-ICP-04 - item 6.1.1.3

Utilização	Algoritmo / Padrão	Normativo
privada da entidade titular e de seu <i>backup</i>	SAFER+	DOC-ICP-04 - item 6.2.4.3 DOC-ICP-05 - item 6.2.4.4

3. Padrões de Hardware

A tabela a seguir relaciona os padrões a serem empregados nos hardwares criptográficos com sua utilização na ICP-Brasil e com os documentos normativos que tratam dessa utilização.

Utilização	Padrões	Normativo
Módulo criptográfico de geração de geração de chaves assimétricas de usuário final	Padrão FIPS 140-1	DOC-ICP-04 - item 6.2.1 DOC-ICP-05 - item 6.2.1.2
Módulo criptográfico para armazenamento da chave privada de titular do certificado	Padrão FIPS 140-1	DOC-ICP-04 - item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Padrão FIPS 140-1	DOC-ICP-04 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Padrão FIPS 140-1 <i>level 2</i>	DOC-ICP-05 - item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Padrão FIPS 140-1 <i>level 2</i>	DOC-ICP-05 - item 6.8
Parâmetros de geração de chaves assimétricas de AC	Padrão FIPS 140-1 <i>level 2</i>	DOC-ICP-05 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-1 <i>level 3</i>	DOC-ICP-01 - item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Padrão FIPS 140-1 <i>level 3</i>	DOC-ICP-01 - item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-1 <i>level 3</i>	DOC-ICP-01 - item 6.1.6

Utilização	Padrões	Normativo
Processo para verificação de parâmetros de geração de chaves assimétricas	Processo de Homologação da ICP-Brasil	DOC-ICP-01 - item 6.1.7 DOC-ICP-04 - item 6.1.7 DOC-ICP-05 - item 6.1.7

4. Documentos Referenciados

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil, 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 as Resoluções que os aprovaram.

Código	Nome do documento
DOC-ICP-01	DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL
DOC-ICP-04	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL
DOC-ICP-05	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL