

**INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
INSTRUÇÃO NORMATIVA Nº 4, DE 18 DE MAIO DE 2006.**

Aprova a versão 1.0 do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICPBRASIL O DIRETORPRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso I, do art. 1º, do anexo I, do Decreto nº 4.689, de 7 de maio de 2003, e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICPBrasil, de 21 de outubro de 2004, e

CONSIDERANDO que a versão 2.0 do DOC ICP01, aprovada pelo Comitê Gestor da ICP-Brasil em 18.04.2006, prevê a criação do presente documento, que o suplementa com relação ao assunto em pauta,

R E S O L V E :

Art. 1º Aprovar a versão 1.0 do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICPBRASIL (DOCICP01.01), na forma definida pelo anexo.

Art. 2º Esta Instrução Normativa entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI

ANEXO

**PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL DOC ICP01.01 Versão
1.0**

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.

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#7	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 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
Algoritmos criptográficos 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 DAS	DOC-ICP-04 – item 7.1.3
Algoritmo simétrico para guarda de chave privada da entidade titular e de seu backup	3-DES, IDEA, SAFER+	DOC-ICP-04 – item 6.1.1.3 DOC-ICP-04 – item 6.2.4.3 DOC-ICP-05 – item 6.2.4.4

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 1401	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 1401	DOC-ICP-04 item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Padrão FIPS 1401	DOC-ICP-04 item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Padrão FIPS 140-1 level 2	DOC-ICP-05 item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Padrão FIPS 140-1 level 2	DOC-ICP-05 – item 6.8
Parâmetros de geração de chaves assimétricas de AC	Padrão FIPS 140-1 level 2	DOC-ICP-05 – item 6.1.6
Módulo criptográfico de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-1 level 3	DOC-ICP-01 – item 6.2.1
Módulo Criptográfico para armazenamento de chave privada da AC Raiz	Padrão FIPS 140-1 level 3	DOC-ICP-01 – item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-1 level 3	DOC-ICP-01 – item 6.1.6
Processo para verificação de parâmetros 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

Documentos Referenciados

Os documentos abaixo são aprovados por Resolução do Comitê Gestor da ICPBrasil, 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 ICPBRASIL
DOC-ICP-04	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL
DOC-ICP-05	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICPBRASIL

Fonte:

http://www.iti.gov.br/twiki/pub/Certificacao/LegislacaoConsolidada/instrucoes_normativas.pdf