RESOLUÇÃO Nº 65, DE 09 DE JUNHO DE 2009.

APROVA A VERSÃO 2.0 DO DOCUMENTO PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL, E O PLANO DE MIGRAÇÃO RELACIONADO.

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL, no exercício do cargo de Coordenador do referido Comitê, no uso das atribuições legais previstas nos incisos I, V e VI do art. 4° da Medida Provisória n° 2.200-2, de 24 de agosto de 2001,

CONSIDERANDO a necessidade de atualização dos Padrões e Algoritmos Criptográficos da ICP-Brasil (DOC-ICP-01.01), e

CONSIDERANDO a necessidade de definição de prazos limítrofes para as atualizações previstas na versão 2.0 dos Padrões e Algoritmos Criptográficos da ICP-Brasil,

RESOLVE:

Art. 1º Aprovar a versão 2.0 dos PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC-ICP-01-01, Anexo I).

Art. 2º Aprovar o Plano de Migração para Atualização dos Algoritmos Criptográficos da ICP-Brasil (Anexo II).

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI

ANEXO I

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS
DA ICP-BRASIL (DOC ICP-01.01)
Versão 2.0
09 de junho de 2009

1. INTRODUÇÃO

Este documento regulamenta os padrões de hardware, os algoritmos e parâmetros criptográficos a serem empregados em todos os processos realizados no âmbito da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), que incluem, entre outros:

a) geração de chaves criptográficas;

b) solicitação, emissão e revogação de certificados digitais;

c) geração e verificação de assinaturas digitais;

d) cifração de mensagens;

e) autenticação com certificados digitais.

As diretrizes aqui constantes devem ser obrigatoriamente observadas pelas Autoridades Certificadoras, Autoridades de Registro, Prestadores de Serviço de Suporte, Empresas de Auditoria Independente, Laboratórios de Ensaios e Auditoria, e outras entidades credenciadas ou cadastradas na ICP-Brasil, bem como pelos titulares finais e desenvolvedores de aplicativos que utilizam certificados digitais da ICP-Brasil.

2. APLICABILIDADE DOS ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS

Esta Seção relaciona os principais procedimentos que envolvem criptografia, no âmbito da ICP-Brasil, com os algoritmos e parâmetros que devem ser utilizados, **obrigatoriamente**, para sua execução, e também com os documentos normativos que tratam desses procedimentos.

Solicitação de certificados à AC	
Normativo ICP-Brasil	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
Formato	Padrão PKCS#10

Entrega de certificados emitidos pela AC	
Normativo ICP-Brasil	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	Padrão PKCS#7

Geração de chaves assimétricas de AC	
Normativo ICP-Brasil	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	RSA, ECDSA (conforme RFC 5480)

Tamanho de chave	RSA 2048, RSA 4096, ECDSA 512

Geração de chaves assimétricas de usuário final	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.5.2
Algoritmo	RSA, ECDSA (conforme RFC 5480)
Tamanho da chave A1, A2, A3, S1, S2, S3, T3	RSA 1024, RSA 2048, ECDSA 256
Tamanho da chave A4, S4, T4	RSA 2048, RSA 4096, ECDSA 512

Assinatura de certificados de AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 7.1.3 DOC-ICP-01 - item 7.2.3 DOC-ICP-05 - item 7.2.3
Suíte de Assinatura	sha1WithRSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

Assinatura de certificados de usuário final	
Normativo ICP-Brasil	DOC-ICP-04 - item 7.1.3
Suíte de Assinatura	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

Assinatura de Listas de Certificados Revogados e Respostas OCSP	
Normativo ICP-Brasil	DOC-ICP-01 - item 7.3 DOC-ICP-04 - item 7.2 DOC-ICP-05 - item 7.3
Algoritmo de Assinatura	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

Guarda da chave privada da entidade titular e de seu *backup*	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.1.3 DOC-ICP-04 - item 6.2.4.3 DOC-ICP-05 - item 6.2.4.4
Algoritmo e Tamanho de chave	3DES – 112 bits AES – 128 ou 256 bits
Modo de operação	CBC ou GCM

Assinaturas digitais ICP-Brasil CaDES e XaDES	
Normativo ICP-Brasil	DOC-ICP-15, item 6.1
Função resumo	SHA - 1 SHA - 256 SHA - 512

Suíte de Assinatura	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

Assinatura de Pedidos e Respostas de Carimbos do Tempo	
Normativo ICP-Brasil	DOC-ICP-12, item 7.2
Função resumo	SHA - 1 SHA - 256 SHA - 512
Suíte de Assinatura	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

Esquemas de Acordos de Chaves
ECDH256 ou ECMQV256
ECDH512 ou ECMQV512
RSA 1024
RSA 2048
RSA 4096

Esquema de Envelopes Criptográficos
3desWithRSA1024Encryption
3desWithRSA2048Encryption
aes128WithRSA2048Encryption
aes256WithRSA4096Encryption
aes128WithECIES256Encryption
aes256WithECIES512Encryption

3. PADRÕES DE HARDWARE

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

Utilização	Padrões Obrigatórios (1)	Padrões Transitórios (2)	Normativo
Módulo criptográfico de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil	Homologação da ICP-Brasil ou Padrão FIPS 140-1 ou FIPS 140-2	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	Homologação da ICP-Brasil	Homologação da ICP-Brasil ou Padrão FIPS 140-1 ou FIPS 140-2	DOC-ICP-04 - item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil	Homologação da ICP-Brasil ou Padrão FIPS 140-1 ou FIPS 140-2	DOC-ICP-04 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Homologação da ICP-Brasil NSH-2	Homologação da ICP-Brasil NSH-2 ou Padrão FIPS 140-1 nível 2 ou FIPS 140-2 nível 3	DOC-ICP-05 - item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Homologação da ICP-Brasil NSH-2	Homologação da ICP-Brasil NSH-2 ou Padrão FIPS 140-1 nível 2 ou FIPS 140-2 nível 3	DOC-ICP-05 - item 6.8
Parâmetros de geração de chaves assimétricas de AC	Homologação da ICP-Brasil NSH-2	Homologação da ICP-Brasil NSH-2 ou Padrão FIPS 140-1 nível 2 ou FIPS 140-2 nível 3	DOC-ICP-05 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas da AC Raiz	Homologação da ICP-Brasil NSH-3	Homologação da ICP-Brasil NSH-3 ou Padrão FIPS 140-1 nível 3 ou FIPS 140-2 nível 3	DOC-ICP-01- item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Homologação da ICP-Brasil NSH-3	Homologação da ICP-Brasil NSH-3 ou Padrão FIPS 140-1 nível 3 ou FIPS 140-2 nível 3	DOC-ICP-01- item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Homologação da ICP-Brasil NSH-3	Homologação da ICP-Brasil NSH-3 ou Padrão FIPS 140-1 nível 3 ou FIPS 140-2 nível 3	DOC-ICP-01- item 6.1.6
Processo para verificação de parâmetros de geração de chaves assimétricas	Homologação da ICP-Brasil NSH-3	Homologação da ICP-Brasil NSH-3 ou Padrão FIPS 140-1 nível 3 ou FIPS 140-2 nível 3	DOC-ICP-01 - item 6.1.7 DOC-ICP-04 - item 6.1.7 DOC-ICP-05 - item 6.1.7

Nota (1): A partir da data de publicação desta Resolução passa a ser requisito obrigatório a homologação dos dispositivos de hardware acima discriminados junto à ICP-Brasil, observados, ainda, os Níveis de Segurança de Homologação (NSH) mínimos estabelecidos;

Nota (2): Tendo em vista a necessidade de se conceder prazo para que o mercado se adeque às exigências ora estabelecidas, admitir-se-á, transitoriamente, até 31/12/2010, para efeitos de auditorias e fiscalizações da ICP-Brasil, a apresentação de Protocolo de Habilitação Jurídica e Relatório de Análise Qualitativa emitido pelo LEA, referentes a Processo de Homologação da ICP-Brasil condizente com o NSH exigido ou ainda comprovante de Certificação FIPS 140-2 ou FIPS 140-1 no nível exigido.

4. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil e podem ser alterados, quando necessário, pelo mesmo dispositivo legal. O sítio http://www.iti.gov.br disponibiliza as versões atualizadas de todos os 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
DOC-ICP-12	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL (documento em fase de aprovação)
DOC-ICP-15	ASSINATURAS DIGITAIS NA ICP-BRASIL (documento em fase de aprovação) GLOSSÁRIO DA ICP-BRASIL

ANEXO II

PLANO DE MIGRAÇÃO

1. Primeira etapa – data limite: 09.06.2009

1.1. Alterar os normativos da ICP-Brasil para permitir a emissão de certificados para AC e usuários finais contendo chaves ECC. Permitir que esses certificados usem também função *hash* SHA 256 ou SHA 512 para realização de assinaturas. O objetivo dessa ação é permitir que o mercado comece a se adaptar aos novos padrões.
1.2. Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

2. Segunda etapa – data limite: 31.01.2010

2.1. Criar, na AC Raiz, nova cadeia (V2), que implemente os padrão RSA 4096 bits e função *hash* SHA 512.
2.2. Criar na AC Raiz, nova cadeia (V3) que implemente os padrão ECDSA 512 bits e função *hash* SHA 512.
2.3. Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

3. Terceira etapa – data limite: 30.06.2010

3.1. Avaliar a adesão dos sistemas de mercado e de AC, à adoção de esquemas criptográficos mais seguros e se necessário, adotar ações para ampliação do uso.
3.2. A partir de 01.02.2010, as AC devem adotar as ações necessárias ao inicio do processo de emissão de certificados vinculados à AC Raiz sob a nova hierarquia (V2 ou V3), e adaptar seus sistemas para uso dos novos padrões.
3.3. Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

4. Quarta etapa – data limite: 01.01.2011

4.1. A partir dessa data é recomendado criar certificados que usem pelo menos padrão RSA 2048 bits e função *hash* SHA 256.

5. Quinta etapa – data limite: 31.12.2011

5.1. A partir desta data, todas as AC já devem estar emitindo certificados vinculados à AC Raiz sob a nova hierarquia (V2 e V3), adaptando seus sistemas para o uso dos novos padrões.
5.2. Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

6. Sexta etapa – data limite: 01.01.2012

6.1. A partir dessa data, nenhum novo certificado de AC ou de usuários finais poderá ser gerado sob as hierarquias anteriores (V0 e V1).
6.2. Definir e adotar ações para viabilizar a realização da próxima etapa no prazo previsto.

7. Sétima etapa – data limite: 31.12.2014

7.1. A partir dessa data, nenhum certificado ICP-Brasil emitido sob as cadeias anteriores (V0 e V1) deverá estar válido, exceto certificados de AC, cuja revogação deve ser avaliada.