Infraestrutura de Chaves Públicas Brasileira

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL

(DOC ICP-01.01)

Versão 2.5

10 de julho de 2014

SUMÁRIO

Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
IN 03, de 10.07.2014 (Versão 2.5)	Acrescenta NOTA (1) às tabelas referentes a geração de chaves assimétricas, do item 2, do DOC-ICP-01.01, versão 2.4.	Esclarece a manutenção de SHA1 e tamanho de chaves RSA para preservar compatibilidade de certificados anteriores a 2012.
IN 01, de 04.06.2014 (Versão 2.4)	Tabelas de Geração de Chaves Assimétricas de AC e de usuário final (pág. 4).	Substituição das Curvas Elípticas NIST pelo ECC Brainpool.
Resolução 89, de 05.07.2012 (Versão 2.3)	Substitui s NOTA (4) e acrescenta-se a NOTA (5) ao item 3, do DOC-ICP-01.01, versão 2.2	Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de certificação digital.
Resolução 85, de 09.11.2011 (Versão 2.2)	Acrescenta as NOTAS (3) e (4) ao item 3, do DOC-ICP-01.01, versão 2.1	Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de certificação digital.
IN 8, de 01.10.2010 (Versão 2.1)		Aprova e autoriza a disponibilização no sítio do ITI, os documentos DOC-ICP-01.01 em sua Versão 2.1; DOC-ICP-10.02 em sua Versão 3.0; DOC-ICP-10.07 em sua Versão 1.0.
Resolução 65, de 09.06.2009 (Versão 2.0)		Aprova a versão 2.0 do documento Padrões e Algorítimos Criptografados da ICP-BRASIL, e o plano de migração relacionado.
IN 3, de 22.10.2008 (Versão 1.1)		Altera o documento Padrões e Algorítimos Criptografados da ICP-BRASIL
IN 4, de 18.05.2006		Aprova a versão 1.0 do

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
(Versão 1.0)		documento Padrões e Algorítimos Criptografados da ICP-BRASIL

Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ECC-Brainpool	
ETSI	*European Telecommunication Standard Institute*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
PKCS	Public Key Cryptgraphy Standards
RFC	*Request For Comments*

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 Infraestrutura 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, ECC-Brainpool (conforme RFC 5639)
Tamanho de chave	RSA 2048, RSA 4096, brainpoolP512r1

Nota (1): A função *hash* SHA-1 e os algoritmos criptográficos RSA 1024 bits para certificados de usuário final e RSA 2048 bits para certificados de AC NÃO DEVEM mais ser utilizados, a partir de 2012, nas emissões de certificados digitais, inclusive em suas requisições, conforme anexo II da Resolução n° 68. Suas previsões encontram-se nos normativos da ICP-Brasil somente para preservar a compatibilidade com os certificados emitidos até o final de 2011.

Geração de Chaves Assimétricas de Usuário Final	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.5.2
Algoritmo	RSA, ECC-Brainpool (conforme RFC 5639)
Tamanho de chave A1, A2, A3, S1, S2, S3, T3	RSA 1024, RSA 2048, brainpoolP256r1
Tamanho da chave A4, S4, T4	RSA 2048, RSA 4096, brainpoolP512r1

Ver *Nota (1)*.

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 6.1.1.4 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 mínimos 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	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	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	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	FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2 e V3)	DOC-ICP-05 item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Homologação da ICP-Brasil NSH-2	FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2 e V3)	DOC-ICP-05 item 6.8
Parâmetros de geração de chaves assimétricas de AC	Homologação da ICP-Brasil NSH-2	FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2 e V3)	DOC-ICP-05 item 6.1.6
Módulo criptográfico de	Homologação da	FIPS 140-1 nível 3 (para a	DOC-ICP-01

Utilização	Padrões Obrigatórios (1)	Padrões Transitórios (2)	Normativo
geração de chaves assimétricas da AC Raiz	ICP-Brasil NSH-3	cadeia de certificação V0); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1, V2 e V3)	item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Homologação da ICP-Brasil NSH-3	FIPS 140-1 nível 3 (para a cadeia de certificação V0); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1, V2 e V3)	DOC-ICP-01 item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Homologação da ICP-Brasil NSH-3	FIPS 140-1 nível 3 (para a cadeia de certificação V0); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1, V2 e V3)	DOC-ICP-01 item 6.1.6
Processo para verificação de parâmetros de geração de chaves assimétricas da AC Raiz	Homologação da ICP-Brasil NSH-3	FIPS 140-1 nível 3 (para a cadeia de certificação V0); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1, V2 e V3)	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 140-1 no nível exigido. No período compreendido entre 01/01/2011 e 31/12/2011, para efeitos de auditorias e fiscalizações da ICP-Brasil, é admitido a apresentação do comprovante de Certificação FIPS 140-2 ou 140-1 no nível exigido.

Nota (3): Admitir-se-á, transitoriamente, até 30/06/2012, para efeitos de auditoria e fiscalização da ICP-Brasil, o uso de equipamentos de certificação digital não homologados pela ICP-Brasil, desde que os referidos equipamentos tenham sido depositados até 31/12/2011, em laboratório de ensaios e auditoria (LEA) credenciado na ICP-Brasil, para o início do processo de avaliação de conformidade.

Nota (4): Admitir-se-á, transitoriamente, entre 06/07/2012 e 31/12/2012, a emissão de certificados digitais em equipamentos não homologados, mas em processo de avaliação de conformidade pelo Laboratório de Ensaios e Auditoria (LEA), constantes no Anexo I desta Resolução.

Nota (5): O Laboratório de Ensaios e Auditoria (LEA) deverá entregar, individualmente, assim que concluído o processo de avaliação de conformidade, até o dia 31/12/2012, cópia dos referidos laudos, mediante o envio de mensagem de correio eletrônico para o endereço homologa@iti.gov.br, assinada digitalmente com uso de certificado digital ICP-Brasil.

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.

Ref.	Nome do documento	Código
[1]	DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-01
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[3]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[5]	VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL	DOC-ICP-15
[6]	GLOSSÁRIO DA ICP-BRASIL	