Infra-Estrutura de Chaves Públicas Brasileira

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