



**Infraestrutura de Chaves Públicas Brasileira**

**PADRÕES E ALGORITMOS  
CRIPTOGRÁFICOS  
DA ICP-BRASIL**

**DOC ICP-01.01**

**Versão 3.2**

**06 de julho de 2017**



# Infraestrutura de Chaves Públicas Brasileira

## SUMÁRIO

CONTROLE DE ALTERAÇÕES.....	3
TABELA DE SIGLAS E ACRÔNIMOS.....	5
1. INTRODUÇÃO.....	6
2. APLICABILIDADE DOS ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS.....	7
3. PADRÕES DE HARDWARE.....	11
4. DOCUMENTOS REFERENCIADOS.....	12



## CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
<b>Resolução 123, de 06 de julho de 2017 (Versão 3.2)</b>	Item 3 (tabela)	Atualiza tabela com padrões mínimos a serem empregados nos hardware criptográficos.
<b>IN 01/2016, de 31.03. 2016. (Versão 3.1)</b>	Tabela - Geração de Chaves Simétricas de AC.	Gerenciamento de IDN - PSBio.
<b>Resolução 115, de 11.11. 2015. (versão 3.0)</b>	Tabela - Geração de Chaves Assimétricas de Usuário Final	Criação de Política de Certificado A CF - e - SAT.
<b>IN 03, de 25/08/2015 (Versão 2.6)</b>	Item 2, tabela Padrões de Assinatura ICP-Brasil.  Item 2, tabela Geração de Chaves Assimétricas	Regulamentação PAdES.  Ajuste no texto de algoritmos obrigatórios.
<b>IN 03, de 10.07.2014 (Versão 2.5)</b>	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.
<b>IN 01, de 04.06.2014 (Versão 2.4)</b>	Tabelas de Geração de Chaves Assimétricas de AC e de usuário final (pág. 4).	Substituição das Curvas Elípticas NIST pelo ECC Brainpool.
<b>Resolução 89, de 05.07.2012 (Versão 2.3)</b>	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.
<b>Resolução 85, de 09.11.2011 (Versão 2.2)</b>	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.
<b>IN 8, de 01.10.2010</b>		Aprova e autoriza a disponibilização no sítio do ITI, os documentos DOC-ICP-01.01



## Infraestrutura de Chaves Públicas Brasileira

<b>Resolução que aprovou alteração</b>	<b>Item Alterado</b>	<b>Descrição da Alteração</b>
<b>(Versão 2.1)</b>		em sua Versão 2.1; DOC-ICP-10.02 em sua Versão 3.0; DOC-ICP-10.07 em sua Versão 1.0.
<b>Resolução 65, de 09.06.2009 (Versão 2.0)</b>		Aprova a versão 2.0 do documento Padrões e Algoritmos Criptografados da ICP-BRASIL, e o plano de migração relacionado.
<b>IN 3, de 22.10.2008 (Versão 1.1)</b>		Altera o documento Padrões e Algoritmos Criptografados da ICP-BRASIL
<b>IN 4, de 18.05.2006 (Versão 1.0)</b>		Aprova a versão 1.0 do documento Padrões e Algoritmos Criptografados da ICP-BRASIL



## TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
<i>CAdES</i>	<i>CMS Advanced Eletronic Signature</i>
CBC	<i>Cipher Block Chaining</i>
CF-e	Cupom Fiscal Eletrônico
DOC-ICP	Documentos Principais da ICP-Brasil
ECC	<i>Elliptic Curve Cryptography</i>
ECDH	<i>Elliptic Curve Diddie-Hellman</i>
ECMQV	<i>Elliptic Curve Menezes-Qu-Vanstone</i>
GCM	Galois/Counter Mode
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDN	Identificador de Registro Biométrico
LEA	Laboratórios de Ensaio e Auditoria
NIST	<i>National Institute of Standards and Technology</i>
NSH	Níveis de Segurança e Homologação
<i>PAdES</i>	<i>PDF Advanced Eletronic Signature</i>
RSA	<i>Rivest, Shamir and Adleman Algorithm</i>
SAT	Sistema de Autenticação e Transmissão
SHA	<i>Secure Hash Algorithm</i>
<i>XAdES</i>	<i>XML Advanced Eletronic Signature</i>



# Infraestrutura de Chaves Públicas Brasileira

## 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 Ensaio 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	
<b>Normativo ICP-Brasil</b>	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
<b>Formato</b>	Padrão PKCS#10

Entrega de Certificados Emitidos pela AC	
<b>Normativo ICP-Brasil</b>	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
<b>Formato</b>	Padrão PKCS#7

Geração de Chaves Assimétricas de AC	
<b>Normativo ICP-Brasil</b>	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
<b>Algoritmo</b>	RSA ou ECC-Brainpool (conforme RFC 5639)
<b>Tamanho de chave</b>	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 nº 68. Suas previsões encontram-se nos normativos da ICP-Brasil somente para preservar a compatibilidade com os certificados emitidos até o final de 2011.



## Infraestrutura de Chaves Públicas Brasileira

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

Ver *Nota (1)*.

<b>Assinatura de Certificados de AC</b>	
<b>Normativo ICP-Brasil</b>	DOC-ICP-01 - item 7.1.3 DOC-ICP-01 - item 7.2.3 DOC-ICP-05 - item 7.2.3
<b>Suíte de Assinatura</b>	sha1WithRSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

<b>Assinatura de Certificados de Usuário Final</b>	
<b>Normativo ICP-Brasil</b>	DOC-ICP-04 - item 7.1.3
<b>Suíte de Assinatura</b>	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

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



## Infraestrutura de Chaves Públicas Brasileira

<b>Guarda da Chave Privada da Entidade Titular e de seu <i>Backup</i></b>	
<b>Normativo ICP-Brasil</b>	DOC-ICP-04 - item 6.1.1.4 DOC-ICP-04 - item 6.2.4.3 DOC-ICP-05 - item 6.2.4.4
<b>Algoritmo e Tamanho de chave</b>	3DES – 112 bits AES – 128 ou 256 bits
<b>Modo de operação</b>	CBC ou GCM

<b>Assinaturas Digitais ICP-Brasil <i>CADES, XAdES e PAdES</i></b>	
<b>Normativo ICP-Brasil</b>	DOC-ICP-15, item 6.1
<b>Função resumo</b>	SHA - 1 SHA - 256 SHA - 512
<b>Suíte de Assinatura</b>	sha1WithRSAEncryption sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

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

<b>Esquemas de Acordos de Chaves</b>	
	ECDH256 ou ECMQV256
	ECDH512 ou ECMQV512
	RSA 1024
	RSA 2048
	RSA 4096



## Infraestrutura de Chaves Públicas Brasileira

<b>Esquema de Envelopes Criptográficos</b>
3desWithRSA1024Encryption
3desWithRSA2048Encryption
aes128WithRSA2048Encryption
aes256WithRSA4096Encryption
aes128WithECIES256Encryption
aes256WithECIES512Encryption

<b>Geração de Chaves Simétricas para IDN</b>	
<b>Normativo ICP-Brasil</b>	DOC-ICP-05-04 - item 1.1
<b>Algoritmo e Tamanho de chave</b>	AES – 256 bits
<b>Modo de operação</b>	CBC



## Infraestrutura de Chaves Públicas Brasileira

### 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	Normativo
Módulo criptográfico de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil ou Certificação INMETRO	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 ou Certificação INMETRO	DOC-ICP-04 item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-04 item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.8
Parâmetros de geração de chaves assimétricas de AC	Com NSH-2, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-05 item 6.1.6
Módulo criptográfico de geração de chaves Assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	DOC-ICP-01 item 6.1.6
Processo para verificação de parâmetros de geração de chaves assimétricas da AC Raiz	Com NSH-3, Homologação da ICP-Brasil ou Certificação INMETRO	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 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	