# POLÍTICA DE ASSINATURA

# ICP-BRASIL PADRÃO CADES

## DOC-ICP-15.04

**Versão 1.0**

# Lista de Abreviaturas e Siglas

| | |
|---|---|
| **AC** | Autoridade Certificadora |
| **CMS** | Cryptographic Message Syntax |
| **ICP** | Infra-estrutura de Chaves Públicas |
| **ITI** | Instituto Nacional de Tecnologia da Informação |
| **LCR** | Lista de Certificados Revogados |
| **OCSP** | Online Certificate Status Protocol |
| **OID** | Object Identifier |
| **PA** | Politica de Assinatura |
| **RFC** | Request For Coments |
| **SHA** | Secure Hash Algorithm |
| **XMLDsig** | eXtensible Markup Language digital SIGnature |

# Sumário

## 1.INFORMAÇÕES GERAIS

1.1 Este documento define uma política de assinatura da ICP-Brasil, para uso geral, elaborada com vistas a facilitar a adoção de políticas de assinaturas digitais e a estabelecer um patamar de segurança para os procedimentos de geração e validação de uma assinatura digital.

1.2 Ele está associado a um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da Infra-estrutura de Chaves Públicas Brasileira -ICP-Brasil. Tal conjunto se compõe de:

a) ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15

b) PERFIL PARA ASSINATURAS CADES ICP-BRASIL – DOC-ICP-15.01

c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03

d) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES – DOC-ICP-15.04

1.3 Recomenda-se a leitura prévia do documento listado no item a) para melhor compreensão do contexto deste normativo. A política de assinatura (PA) aqui apresentada foi elaborada com base no formato de **assinatura digital ICP-Brasil sem carimbo de tempo (EPES),** descrito naquele documento.

1.4 A partir desta PA podem ser criadas assinaturas mais sofisticadas, que utilizem campos não descritos nesta PA, sabendo-se que pelo menos os requisitos mínimos de segurança para geração e validação da assinatura serão observados.

1.5 A partir desta PA também podem ser criadas outras políticas de assinatura pelas entidades que o desejarem, desde que observado o padrão definido no DOC-ICP-15.03.

1.6 Este documento adota como referência, além das normas da ICP-Brasil, os padrões internacionais, relacionados ao fim deste documento, que devem ser consultados para se obter detalhamento da implementação da política de assinatura aqui regulamentada.

## 2.POLÍTICA DE ASSINATURA

### 2.1.Identificador da Política de Assinatura

2.1.1 O nome desta Política de Assinatura é POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES, versão 1.0.

2.1.2 O *Object Identifier* (OID) desta PA, atribuído pelo Instituto Nacional de Tecnologia da Informação (ITI) é: 2.16.76.1.5.1.1.1.

2.1.3 Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.5.1.1.n+1.

2.1.4 Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br) do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo *SHA256 com RSA*.

### 2.2.Data da Criação

A data de criação desta PA é 03.03.2008.

### 2.3.Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI).

### 2.4.Campo de Aplicação

2.4.1 Esta PA se aplica as assinaturas digitais de transações eletrônicas ou outras situações em que as informações de verificação das assinaturas digitais, necessárias para dirimir eventuais contendas futuras, podem ser obtidas por outras formas, como, por exemplo, podem ser providas por uma das partes, que as tenha registrado em seu sistema. Nessas situações, é recomendável que exista um acordo prévio, assinado por ambas as partes, concordando com essa guarda unilateral de dados complementares.

2.4.2 Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

2.4.3 Segundo esta PA, é permitido o emprego de múltiplas assinaturas.

### 2.5.Política de Validação da Assinatura

#### 2.5.1.Período para Assinatura

Esta PA terá validade de 03.03.2008 até 03.03.2010.

**2.5.2.Regras Comuns**

**2.5.2.1.Regras de Signatário e Verificador**

**2.5.2.1.1.Regras do Signatário**

**2.5.2.1.1.1.Dados Externos ou Internos à Assinatura**

As assinaturas realizadas segundo esta PA podem ser do tipo *attached* (que inclui o conteúdo assinado na assinatura digital) ou *detached* (que não inclui o conteúdo assinado na assinatura digital).

**2.5.2.1.1.2.Atributos Assinados Obrigatórios**

As assinaturas feitas segundo esta PA definem como obrigatórios os seguintes atributos assinados:

- *Message Digest ?????*
- *Id-contentType*
- *Id-messageDigest*
- *Id-aa-signingCertificateV2*
- *Id-signingTime*
- *Id-aa-sigPolicyId*

**2.5.2.1.1.3.Atributos Não-Assinados Obrigatórios**

Não se aplica.

**2.5.2.1.1.4.Referências a Cadeia de Certificação**

O atributo Id-aa-signingCertificateV2 deve conter apenas referência ao certificado do signatário.

**2.5.2.1.1.5.Valores da Cadeia de Certificação**

Não se aplica.

**2.5.2.1.1.6.Regras Adicionais do Signatário**

2.5.2.1.1.6.1 Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 2.5.2.5. As formas possíveis de múltiplas assinaturas são:

a) Co-assinaturas: quando a ordem de inserção das assinaturas não faz diferença; ou
b) Contra-assinaturas: quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento com a primeira assinatura já presente.

2.5.2.1.1.6.2 No caso de co-assinaturas haverá múltiplas estruturas *SignerInfo*.

2.5.2.1.1.6.3 Para contra-assinaturas, deverão ser empregados atributos *Id-countersignature*.

2.5.2.1.1.6.4 Deve-se utilizar a codificação MIME para o valor do campo *eContent* da estrutura *EncapsulatedContentInfo*, e o MIME *type* para identificação do formato de apresentação dos dados.

2.5.2.1.1.6.5 O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.

**2.5.2.1.2.Regras do Verificador**

**2.5.2.1.2.1.Atributos Não-Assinados Obrigatórios**

Não se aplica.

**2.5.2.1.2.2.Regras Adicionais do Verificador**

Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 2.5.2.2.

**2.5.2.2.Condições de Confiabilidade dos Certificados dos Signatários**

**2.5.2.2.1.Validação da Cadeia de Certificação**

**2.5.2.2.1.1.Raiz Confiável**

A validação deve ser feita tomando como ponto de confiança o certificado da AC-Raiz da ICP-Brasil, disponível em http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt. Para fins de conferência adicional, o certificado da AC-Raiz também se encontra publicado no Diário Oficial da União do dia 03.12.2001.

**2.5.2.2.1.2.Restrição do Caminho de Certificação**

O número máximo de certificados de AC, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).

**2.5.2.2.1.3.Conjunto de Políticas de Certificado Aceitável**

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificado ICP-Brasil de assinatura, conforme definido no DOC-ICP-04, com os seguintes OID:

| Tipo | OID |
|---|---|
| A1 | OID 2.16.76.1.2.1.n |
| A2 | OID 2.16.76.1.2.2.n |
| A3 | OID 2.16.76.1.2.3.n |
| A4 | OID 2.16.76.1.2.4.n |

**2.5.2.2.1.4.Restrições de Nome**

Não se aplica.

**2.5.2.2.1.5.Restrições de Políticas de Certificado**

Não se aplica.

**2.5.2.2.2.Forma de Verificação do Status da Cadeia de Certificação (Revogação)**

Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do estado dos certificados deve ser realizada através de consulta à LCR (Lista de Certificados Revogados), usando os procedimentos definidos na RFC 3280, ou por meio de consulta OCSP (*Online Certificate Status Protocol*), usando os procedimentos definidos na RFC 2560.

**2.5.2.3.Condições de Confiabilidade do Carimbo de Tempo**

Não se aplica

**2.5.2.4.Condições de Confiabilidade dos Atributos**

Não se aplica.

**2.5.2.5.Conjunto de Restrições de Algoritmos**

Para geração de assinaturas segundo esta política, podem ser utilizados os seguintes algoritmos:

a) *RSA/SHA256*

*b) RSA/SHA-1*

#### 2.5.2.6.Regras Adicionais

Não se aplica.

### 2.5.3.Regras para Propósitos Específicos de Assinatura

Não se aplica.

### 2.5.4.Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

## 2.6.Informações Adicionais sobre a Política de Assinatura

Não se aplica.

**3.BIBLIOGRAFIA**

[1] HOUSLEY, R. Cryptographic Message Syntax (CMS). Internet Engineering Task Force (IETF). Jul. 2004.

[2] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures (ESI): CMS Advanced Electronic Signatures (CAdES). Technical Specification. ETSI TS 101 733 v1.7.3, Jan. 2007.

[3] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES). Technical Specification. ETSI TS v1.1.1. Feb. 2007.

[4] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. Technical Report. ETSI TR 102 272 v1.1.1. Dez. 2003.

[5] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Signature Policies Report. Technical Report. ETSI TR 102 041 v1.1.1. Feb. 2002.

[6] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model. Technical Report. ETSI TR 102 045 v1.1.1. Mar. 2003.

[7] ITI. REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL DOC-ICP-04 - Instituto Nacional de Tecnologia da Informação. Versão 2.0; Brasília: ICP-Brasil, 2006.