Infraestrutura de Chaves Públicas Brasileira

# REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL

**DOC-ICP-15.03**

**Versão 7.2**

**15 de julho de 2016**

# SUMÁRIO

CONTROLE DE ALTERAÇÕES....3
LISTA DE SIGLAS E ACRÔNIMOS....5
LISTA DE TABELAS....6
1 INTRODUÇÃO....7
2 CONTEÚDO GERAL DE UMA POLÍTICA DE ASSINATURA....9
2.1 Identificador da Política de Assinatura (6.1, 8.2)....9
2.2 Data de Emissão (5, 8.2)....9
2.3 Nome da Entidade Emissora da Política de Assinatura (6.1, 8.2)....9
2.4 Campo de Aplicação (6.1, 8.2)....9
2.5 Política de Validação da Assinatura (6.2, 8.3)....9
2.6 Informações Adicionais sobre a Política de Assinatura (6.11, 8.2)....16
BIBLIOGRAFIA....17
ANEXO 1....18
1 POLÍTICAS DE ASSINATURA-PADRÃO ICP-BRASIL....18
ANEXO 2....40
1 POLÍTICA-PADRÃO AD-RB BASEADA EM CADES....40
2 POLÍTICA-PADRÃO AD-RT BASEADA EM CADES....44
3 POLÍTICA-PADRÃO AD-RV BASEADA EM CADES....49
4 POLÍTICA-PADRÃO AD-RC BASEADA EM CADES....54
5 POLÍTICA-PADRÃO AD-RA BASEADA EM CADES....59
6 POLÍTICA-PADRÃO AD-RB BASEADA EM XADES....65
7 POLÍTICA-PADRÃO AD-RT BASEADA EM XADES....69
8 POLÍTICA-PADRÃO AD-RV BASEADA EM XADES....74
9 POLÍTICA-PADRÃO AD-RC BASEADA EM XADES....79
10 POLÍTICA-PADRÃO AD-RA BASEADA EM XADES....84
11 POLÍTICA-PADRÃO AD-RB BASEADA EM PADES....90
12 POLÍTICA-PADRÃO AD-RT BASEADA EM PADES....93
13 POLÍTICA-PADRÃO AD-RC BASEADA EM PADES....97
14 POLÍTICA-PADRÃO AD-RA BASEADA EM PADES....102
ANEXO 3....107
GERENCIAMENTO DE POLÍTICAS DE ASSINATURA NA ICP-BRASIL....107
1 INTRODUÇÃO....107
2 ADMINISTRAÇÃO E CICLO DE VIDA DE UMA PA....107
3 APROVAÇÃO DE UMA PA....107
4. PUBLICAÇÃO DA PA E DA LPA....107
5 PRORROGAÇÃO DA VALIDADE DE UMA PA APROVADA....108
6 REVOGAÇÃO DE UMA PA....108
7 PROCEDIMENTOS PARA CRIAÇÃO E VERIFICAÇÃO DA LPA....108
ANEXO 4....114
EXTENSÕES DE POLÍTICAS DE ASSINATURA PARA PAdES....114
1 INTRODUÇÃO....114
2 EXTENSÕES....114

## CONTROLE DE ALTERAÇÕES

| Resolução que aprovou alteração | Item Alterado | Descrição da Alteração |
|---|---|---|
| Instrução Normativa 06, de 15.07.2016. (Versão 7.2) | Tabelas A.20 e anexos 2 e 4. | Ajustes nas políticas PAdES, correção da entrada Cert do dicionário VRI. Novas versões das políticas PAdES AD-RC e AD-RA. |
| Instrução Normativa 03, de 01.06.2016. (Versão 7.1) | Tabelas A.6, A. 8, A.10, A.12 e A.16, anexos 2, 3 e 4. | Ajustes nas políticas PAdES e inclusão da raiz V5 em todas as Políticas de Assinatura. |
| Instrução Normativa 07, de 25.08.2015. (Versão 7.0) | 1.4, 1.10 e 4.4; anexos 1, 2 e 4; tabelas A.14, A.15, A.16, A.17, A.18, A.19, A.20 e A.21. | Regulamentação PAdES |
| Instrução Normativa Nº 14, de 19.09.2012 (Versão 6.1) | Anexo 2, capítulos 5, 6, 7, 8, 9 e 10. | Inclui as definições da versão 2.2 da PA |
| Instrução Normativa Nº 10, de 05.07.2012 (Versão 6.0) | Anexo 1, item 1;<br>Anexo 2, capítulos 5, 6, 7, 8, 9 e 10<br>Anexo 3, item 4 e 7 | Melhorias propostas pelo Grupo de trabalho de Revisão do padrão brasileiro de assinatura digital. |
| Instrução Normativa Nº 03, de 21.03.2012 (Versão 5.0) | Anexo 2 – Item 1 de todas as políticas XAdES<br><br>Inclui as Notas 1 a 4 no Item 1 do Anexo 1. | Geradas novas políticas de assinatura versão 2.1 para XAdES.<br><br>As notas contém esclarecimentos e recomendações de codificação de atributos das políticas de assinaturas baseada em CAdES. |
| Instrução Normativa Nº 02, de 05.03.2012 (Versão 4.0) | Anexo 1 - Tabela A.2<br><br>Anexo 2 - Todas as políticas CAdES Item 5.2.1.1.2 | Corrigido atributo assinado obrigatório id-aa-signingCertificateV2 para a versão 2.0.<br>Geradas novas políticas de assinatura versão 2.1 para CAdES. |
| Instrução Normativa Nº 05, de 26.12.2011 (Versão 3.0) | Item 1, Nota 1 e Anexo 2. | Itens não citados nas políticas de assinatura DEVEM ser considerados como itens proibidos.<br><br>Retirados todos os itens assinalados como "não se aplica". |
| | Anexo 1, Tabelas A2 a A13 | Corrigido as propriedades XadES citadas incorretamente; |

| Resolução que aprovou alteração | Item Alterado | Descrição da Alteração |
|---|---|---|
| | | Corrigido o título da coluna central das Tabelas;<br><br>Alterado o campo carimbo do tempo na política AD-RB de opcional para "não deve";<br><br>Retirado a obrigatoriedade do uso dos atributos referentes à certificado de atributo;<br><br>Corrigido os termos referentes à timestamp nas tabelas. |
| | Anexo 2,<br>Todas as políticas.<br><br>Item 5.2.1.1.5 | Inclusão da versão 2.0 que implementa a cadeia V2 da AC Raiz para todas as políticas de assinatura ICP-Brasil.<br><br>Obrigatoriedade de manter o certificado do signatário no caminho de certificação. |
| | Anexo 3,<br>item 4.2<br><br>Item<br>7.4 | Corrigido endereço do repositório de publicação da LPA.<br><br>Inclusão de codificação da LPA em ASN.1 e XML. |
| Instrução Normativa Nº 03, de 31.03.2010 (Versão 2.0) | Diversos | Atualização de padrões de assinatura. |
| Instrução Normativa Nº 03, de 09.01.2009 (Versão 1.0) | Diversos | Criação do DOC-ICP-15.03. |

# LISTA DE SIGLAS E ACRÔNIMOS

| SIGLA | DESCRIÇÃO |
|---|---|
| **AC** | Autoridade Certificadora |
| **ACT** | *Autoridade de Carimbo do Tempo* |
| **CAdES** | *CMS Advanced Electronic Signatures* |
| **CMS** | *Cryptgraphic Message Syntax* |
| **DSS** | *Document Security Store* |
| **e-PING** | *Padrões de Interoperabilidade de Governo Eletrônico* |
| **ETSI** | *European Telecommunication Standard Institute* |
| **ICP-Brasil** | Infraestrutura de Chaves Públicas Brasileira |
| **ITI** | Instituto Nacional de Tecnologia da Informação |
| **LCR** | Lista de Certificados Revogados |
| **OCSP** | *Online Certificate Status Protocol* |
| **PA** | Política de Assinatura |
| **PAdES** | *PDF Advanced Electronic Signatures* |
| **PDF** | *Portable Document Format* |
| **RFC** | *Request For Comments* |
| **VRI** | *Validation Related Information* |
| **XAdES** | *XML Advanced Electronic Signatures* |
| **XML** | *Extensible Markup Language* |

# LISTA DE TABELAS

Tabela A.1: Abreviações utilizadas....18
Tabela A.2: Atributos assinados no SignerInfo do Assinante....20
Tabela A.3: Presença de atributos não-assinados no SignerInfo do signatário....21
Tabela A.4: Presença de atributos assinados no SignerInfo de "contra assinatura"....22
Tabela A.5: Presença de atributos não-assinados no SignerInfo de "contra assinatura"....23
Tabela A.6: Presença de atributos assinados no TimeStampToken de "carimbo do tempo de conteúdo"....24
Tabela A.7: Presença de atributos não-assinados no TimeStampToken de "carimbo do tempo de conteúdo"....25
Tabela A.8: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura"....26
Tabela A.9: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura."....27
Tabela A.10: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo das referências"....28
Tabela A.11: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo das referências"....29
Tabela A.12: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de arquivamento"....30
Tabela A.13: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de arquivamento"....31
Tabela A.14: Atributos assinados no SignerInfo do Assinante para assinaturas PAdES....32
Tabela A.15: Presença de atributos não-assinados no SignerInfo do signatário para assinatura PAdES....33
Tabela A.16: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura" para assinaturas PAdES....34
Tabela A.17: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura" para assinaturas PAdES....35
Tabela A.18: Presença das entradas do dicionário de assinaturas do PAdES....36
Tabela A.19: Presença das entradas do dicionário DSS do PAdES....37
Tabela A.20: Presença das entradas do dicionário VRI do PAdES....38
Tabela A.21: Presença das entradas do dicionário de assinatura do Document Timestamp do PAdES....39
Tabela A.22: Presença de dicionários PDF relacionados às assinaturas PAdES....39
Tabela A.4.1 – Entradas adicionais do dicionário Document Security Store....116
Tabela A.4.2 – Entradas adicionais do dicionário VRI....116
Tabela A.4.3 - Sintaxe ASN.1 por tipos de entradas....117

# 1 INTRODUÇÃO

1.1 Este documento estabelece os requisitos a serem obrigatoriamente observados pelas entidades criadoras de Políticas de Assinatura Digital no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), em conformidade com a estrutura proposta pelos padrões ETSI TR 102 272 [1] e ETSI TR 102.038 [2].

1.2 Ele faz parte de um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da ICP-Brasil. Tal conjunto se compõe de:

a) Visão Geral sobre Assinaturas Digitais na ICP-Brasil (DOC-ICP-15) [3];
b) Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.01) [4];
c) Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.02) [5];
d) Requisitos das Políticas de Assinatura na ICP-Brasil (DOC-ICP-15.03) (este documento).

1.3 Toda Política de Assinatura elaborada no âmbito da ICP-Brasil DEVE adotar a mesma sintaxe de estrutura empregada neste documento.

1.4 Esta estrutura prevê a criação de uma única assinatura digital (também conhecida como assinatura digital simples ou primária), a criação de assinaturas digitais em paralelo (também conhecidas como coassinaturas), a criação de assinaturas digitais em série (também conhecidas como contra-assinaturas) ou a criação de assinaturas digitais seriais em arquivos PDF (múltiplas assinaturas PAdES).

1.5 As Políticas de Assinatura ICP-Brasil Aprovadas DEVEM ser escritas de uma forma inteligível por seres humanos e; opcionalmente, PODEM ser escritas de uma forma inteligível por sistemas de processamento.

1.6 No caso de políticas que sejam escritas com base no presente documento, a forma inteligível por sistemas de processamento DEVE ser *Abstract Syntax Notation.One* (ASN.1) ou eX*tensible Markup Language* (XML).

1.7 As Políticas de Assinatura Aprovadas ICP-Brasil são protegidas contra alterações indevidas por meio da publicação, no repositório da AC Raiz, de seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação (ITI).

1.8 Para facilitar a utilização de políticas de assinatura pelos usuários finais, o ITI criou 14 Políticas de Assinatura-padrão, que estão detalhadas no **Anexo 2** deste documento.

1.9 O processo de gerenciamento das Políticas de Assinatura pela AC Raiz da ICP-Brasil está descrito no **Anexo 3** deste documento.

1.10 O restante deste documento está organizado da seguinte forma. O Capítulo 2 apresenta o conteúdo de uma Política de Assinatura. O Anexo 1 apresenta as tabelas dos atributos disponíveis para cada perfil de política de assinatura. O Anexo 2 lista as Políticas de Assinatura Padrão da

ICP-Brasil baseadas em CMS *Advanced Electronic Signatures* (CAdES), em XML *Advanced Electronic Signatures* (XAdES) e em PDF *Advanced Electronic Signatures* (PAdES). O Anexo 3 descreve o processo de gerenciamento de PAs na ICP-Brasil. O Anexo 4 explica as extensões das políticas de assinatura utilizadas no padrão PAdES e as entradas PDF inseridas nos dicionários de validação do PDF.

NOTA 1: Itens não citados nas políticas de assinatura padrão ICP-Brasil DEVEM ser considerados como itens proibidos.

# 2 CONTEÚDO GERAL DE UMA POLÍTICA DE ASSINATURA

A seguir são apresentados os itens que DEVEM fazer parte de uma Política de Assinatura Aprovada ICP-Brasil. De maneira a permitir que a AC-Raiz ao criar uma PA tenha informações detalhadas, em conformidade com os documentos ETSI TR 102 038 e ETSI TR 102 272 nos quais os conteúdos são descritos na íntegra.

## 2.1 Identificador da Política de Assinatura (6.1, 8.2)

Neste item DEVE ser informado o identificador (OID) da PA.

## 2.2 Data de Emissão (5, 8.2)

Neste item DEVE ser informada a data em que a PA foi emitida.

## 2.3 Nome da Entidade Emissora da Política de Assinatura (6.1, 8.2)

DEVE ser informado o nome da entidade responsável pela emissão da PA.

## 2.4 Campo de Aplicação (6.1, 8.2)

Neste item DEVE ser definido, em termos gerais, o campo de aplicação da assinatura digital gerada conforme a Política de Assinatura, bem como os propósitos específicos para os quais a assinatura digital é aplicável. Adicionalmente, deverão estar relacionadas, quando cabível, as aplicações para as quais existam restrições ou proibições para o uso da PA.

## 2.5 Política de Validação da Assinatura (6.2, 8.3)

2.5.1 Período para Assinatura (6.2, 8.2)

Neste item DEVE ser definido o período de validade (data e hora) inicial e, opcionalmente, final de abrangência das regras definidas na Política de Assinatura aplicáveis às assinaturas digitais que se utilizarem da Política.

2.5.2 Regras Comuns (6.3, 8.4)

2.5.2.1 Regras do Signatário e do Verificador (6.5, 8.7)

Nota: item opcional

2.5.2.1.1 Regras do Signatário (6.5.1, 8.7.1)

2.5.2.1.1.1 Dados Externos ou Internos a Assinatura (6.5.1, 8.7.1)

Neste item DEVE ser definido se o conteúdo assinado (documento eletrônico) e externo a assinatura digital. Uma das opções abaixo DEVE ser escolhida:

a) o conteúdo assinado é externo a assinatura; ou
b) o conteúdo assinado é interno a assinatura; ou
c) o conteúdo assinado pode ser tanto externo quanto interno a assinatura.

d)2.5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios (6.5.1, 8.7.1)

Neste item DEVEM ser relacionados os atributos ou propriedades que DEVEM constar, obrigatoriamente, no pacote da assinatura digital no âmbito desta Política de Assinatura e que são assinados juntamente com o documento eletrônico. O documento DOC-ICP-15.02, capítulo 2 e 3, define os atributos ou propriedades sugeridos para os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios (6.5.1, 8.7.1)

Neste item DEVEM ser relacionados os atributos ou propriedades que DEVEM constar, obrigatoriamente, no pacote da assinatura digital no âmbito desta Política de Assinatura, e que não são assinados juntamente com o documento eletrônico. O documento DOC-ICP-15.02, capítulo 2 e 3, define os atributos ou propriedades sugeridos para os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.4 Referências Obrigatórias de Certificados (6.5.1, 8.7.1)

Neste item DEVE ser definido quais certificados do caminho de certificação do signatário DEVEM ser referenciados nas assinaturas digitais criadas com base nesta Política de Assinatura. Uma das opções abaixo DEVE ser escolhida:

a) o certificado do signatário; ou
b) os certificados do caminho de certificação completo do signatário.

2.5.2.1.1.5 Informações Obrigatórias de Certificados (6.5.1, 8.7.1)

Neste item DEVE ser definido quais certificados do caminho de certificação do signatário devem constar obrigatoriamente nas assinaturas digitais. Uma das opções abaixo DEVE ser escolhida:

a) nenhum certificado; ou
b) o certificado do signatário; ou
c) os certificados do caminho de certificação completo do signatário.

2.5.2.1.1.6 Regras Adicionais do Signatário (6.11, 8.2)

Caso haja a necessidade de incluir regras adicionais relacionadas ao processo de Assinatura Digital executado pelo signatário, estas DEVEM ser incluídas neste item.

2.5.2.1.2 Regras do Verificador (6.5.2, 8.7.2)

2.5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios (6.5.2, 8.7.2)

Este item DEVE conter os identificadores dos atributos ou propriedades descritos no item 2.5.2.1.1.3, que, caso não incluídos pelo signatário, DEVEM ser adicionados à assinatura pelo verificador.

2.5.2.1.2.2 Regras Adicionais do Verificador (6.11, 8.2)

Caso haja a necessidade de regras adicionais relacionadas ao verificador, essas DEVEM ser incluídas neste item.

2.5.2.2 Condições de Confiabilidade dos Certificados dos Signatários (6.7, 8.8)

Nota: item opcional.

2.5.2.2.1 Requisitos de Certificados (6.7, 8.8.2)

Nota: este item PODE se repetir de acordo com o número de raízes confiáveis.

2.5.2.2.1.1 Raiz Confiável (6.6.1, 8.8.2)

Neste item DEVE constar um certificado autoassinado que deve ser adotado como âncora de confiança no processo de validação do caminho de certificação do signatário.

2.5.2.2.1.2 Restrição do Comprimento do Caminho de Certificação (6.6.1, 8.8.2)

Neste item PODE constar o número máximo de certificados de Autoridade Certificadora (AC) abaixo da âncora de confiança do caminho de certificação do signatário. No caso da ICP-Brasil, este número é, no máximo, 2 (dois).

2.5.2.2.1.3 Conjunto de Políticas de Certificação Aceitáveis (6.6.1, 8.8.2)

Neste item PODEM constar os OIDs das políticas de certificação aceitáveis.

2.5.2.2.1.4 Restrições de Nome (6.6.1, 8.8.2)

Neste item PODEM constar as restrições de nomes aplicáveis.

2.5.2.2.1.5 Restrições de Políticas de Certificação (6.6.1, 8.8.2)

Nota: item opcional.

2.5.2.2.1.5.1 Necessidade da Identificação de Políticas (6.6.1, 8.8.2)

Neste item PODE ser definido a partir de qual nível do caminho de certificação é necessária a identificação das políticas de certificação aceitáveis.

2.5.2.2.1.5.2 Proibição do Mapeamento de Políticas

Neste item PODE ser definido a partir de qual nível do caminho de certificação é proibido o mapeamento de políticas de certificação.

2.5.2.2.2 Requisitos de revogação (6.7, 8.8.3)

2.5.2.2.2.1 Requisitos de Revogação para Certificados Finais (6.6.2, 8.8.3)

2.5.2.2.2.1.1 Mecanismos de Revogação para Certificados (6.6.2, 8.8.3)

Neste item DEVE constar uma das opções de mecanismo de verificação do status de revogação dos certificados:

a) Lista de Certificados Revogados (LCR); ou
b) *Online Certificate Status Protocol* (OCSP); ou
c) LCR e OCSP; ou

d) LCR ou OCSP; ou
e) nenhuma verificação; ou
f) outro mecanismo de verificação.

2.5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados (6.1.1, 8.2)

Caso haja a necessidade de regras adicionais a revogação de certificados, essas devem ser incluídas neste item.

2.5.2.2.2.2 Requisitos de Revogação para Certificados de ACs (6.6.2, 8.8.3)

2.5.2.2.2.2.1 Mecanismos de Revogação para Certificados (6.6.2, 8.8.3)

Neste item DEVE constar uma das opções de mecanismo de verificação do status de revogação dos certificados:

a) LCR; ou
b) OCSP; ou
c) LCR e OCSP; ou
d) LCR ou OCSP; ou
e) nenhuma verificação; ou
f) outro mecanismo de verificação.

2.5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados (6.11, 8.2)

Caso haja a necessidade de regras adicionais para revogação de certificados, essas devem ser incluídas neste item.

2.5.2.3 Condições de Confiabilidade do Carimbo do Tempo (6.11, 8.2)

Nota: item opcional.

2.5.2.3.1 Requisitos de Certificados

Nota: caso este item não esteja presente, então as regras definidas no item 5.2.2.1 se aplicam aos certificados de Autoridade de Carimbo do Tempo (ACT).

2.5.2.3.1.1 Raiz Confiável (6.6.1, 8.8.2)

Neste item DEVE constar um certificado autoassinado que deve ser adotado como âncora de confiança no processo de validação do caminho de certificação da ACT.

2.5.2.3.1.2 Requisitos de Certificados (6.8, 8.9)

Neste item PODE constar o numero máximo de certificados de Autoridade Certificadora (AC) abaixo da ancora de confiança do caminho de certificação do signatário. No caso da ICP-Brasil, este número e, no máximo, 2 (dois).

2.5.2.3.1.3 Conjunto de Políticas de Certificação Aceitáveis (6.6.1, 8.8.2)

Neste item PODEM constar os OIDs das políticas de certificação aceitáveis.

2.5.2.3.1.4 Restrições de Nome (6.6.1, 8.8.2)

Neste item PODEM constar as restrições de nomes aplicáveis.

2.5.2.3.1.5 Restrições de Políticas de Certificação (6.6.1, 8.8.2)

Nota: Item OPCIONAL.

2.5.2.2.3.1.5.1 Necessidade da Identificação de Políticas (6.6.1, 8.8.2)

Neste item PODE ser definido a partir de qual nível do caminho de certificação é necessária a identificação das políticas de certificação aceitáveis.

2.5.2.2.3.1.5.2 Proibição do Mapeamento de Políticas (6.6.1, 8.8.2)

Neste item PODE ser definido a partir de qual nível do caminho de certificação é proibido o mapeamento de políticas de certificação.

2.5.2.3.2 Requisitos de Revogação (6.8, 8.9)

2.5.2.3.2.1 Requisitos de Revogação para Certificados Finais (6.6.2, 8.8.3)

2.5.2.3.2.1.1 Mecanismos de Revogação para Certificados (6.6.2, 8.8.3)

Neste item DEVE constar uma das opções de mecanismo de verificação do status de revogação dos certificados:

a) LCR; ou
b) OCSP; ou
c) LCR e OCSP; ou
d) LCR ou OCSP; ou
e) nenhuma verificação; ou
f) outro mecanismo de verificação.

2.5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados (6.11, 8.2)

Caso haja a necessidade de regras adicionais à revogação de certificados, essas devem ser incluídas neste item.

2.5.2.3.2.2 Requisitos de Revogação para Certificados de ACs (6.6.2, 8.8.3)

2.5.2.3.2.2.1 Mecanismos de Revogação para Certificados (6.6.2, 8.8.3)

Neste item DEVE constar uma das opções de mecanismo de verificação do status de revogação dos certificados:

a) LCR; ou
b) OCSP; ou
c) LCR e OCSP; ou
d) LCR ou OCSP; ou
e) nenhuma verificação; ou
f) outro mecanismo de verificação.

2.5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados (6.11, 8.2)

Caso haja a necessidade de regras adicionais à revogação de certificados, essas devem ser incluídas neste item.

2.5.2.3.3 Restrições de Nome (6.8, 8.9)

Neste item PODEM constar as restrições de nomes aplicáveis.
Nota: caso este item não esteja presente, então as regras definidas no item 5.2.3.1.4. se aplicam aos certificados de (ACT).

2.5.2.3.4 Período de Cautela (6.8, 8.9)

Neste item PODE constar o período de tempo, após o instante de assinatura, que o verificador deve aguardar antes de obter o status de revogação necessário para validar a chave do signatário.

2.5.2.3.5 Atraso do Carimbo do Tempo (6.8, 8.9)

Neste item pode constar o período máximo de tempo aceitável entre o instante informado pelo carimbo do tempo e o instante da assinatura.

2.5.2.4 Condições de Confiabilidade dos Atributos (6.9, 8.10)

Nota: item OPCIONAL.

2.5.2.5 Conjunto de Restrições de Algoritmos (6.10, 8.11)

Nota: na necessidade de se incluir um conjunto de restrições de algoritmos, estes DEVEM ser escolhidos entre os listados no documento Padrões e Algoritmos Criptográficos da ICP-Brasil - DOC-ICP-01.01 [6].

2.5.2.5.1 Restrições de Algoritmos para Signatários (6.10, 8.11)

Nota: item OPCIONAL.

2.5.2.5.1.1 Restrições de Algoritmos (6.10, 8.11)

Nota: este item PODE se repetir de acordo com o número de restrições de algorítimos necessárias.

2.5.2.5.1.1.1 Identificador de Algoritmo (6.10, 8.11)

Neste item DEVE constar o OID do algoritmo a ser restringido.

2.5.2.5.1.1.2 Tamanho Mínimo de Chaves (6.10, 8.11)

Neste item PODE constar o tamanho mínimo de chave em bits.

2.5.2.5.1.1.3 Regras Adicionais de Restrições (6.11, 8.2)

Caso haja a necessidade de regras adicionais a restrições de algoritmos, essas devem ser incluídas neste item.

2.5.2.5.2 Restrições de Algoritmos para AC Final (6.10, 8.11)

Nota: item OPCIONAL.

2.5.2.5.2.1 Restrições de Algoritmos (6.10, 8.11)

Nota: este item PODE se repetir de acordo com o número de restrições de algoritmos necessárias.

2.5.2.5.2.1.1 Identificador de Algoritmo (6.10, 8.11)

Neste item DEVE constar o OID do algoritmo a ser restringido.

2.5.2.5.2.1.2 Tamanho Mínimo de Chaves (6.10, 8.11)

Neste item PODE constar o tamanho mínimo de chave em bits.

2.5.2.5.2.1.3 Regras Adicionais de Restrições (6.11, 8.2)

Caso haja a necessidade de regras adicionais a restrições de algoritmos, essas devem ser incluídas neste item.

2.5.2.5.3 Restrições de Algoritmos para AC Intermediária (6.10, 8.11)

Nota: item OPCIONAL.

2.5.2.5.3.1 Restrições de Algoritmos (6.10, 8.11)

Nota: este item PODE se repetir de acordo com o número de restrições necessárias.

2.5.2.5.3.1.1 Identificador de Algoritmo (6.10, 8.11)

Neste item DEVE constar o OID do algoritmo a ser restringido.

2.5.2.5.3.1.2 Tamanho Mínimo de Chaves (6.10, 8.11)

Neste item PODE constar o tamanho mínimo de chave em bits.

2.5.2.5.3.1.3 Regras Adicionais de Restrições (6.11, 8.2)

Caso haja a necessidade de regras adicionais a restrições de algoritmos, essas devem ser incluídas neste item.

2.5.2.5.4 Restrições de Algoritmos para Autoridades de Atributo (6.10, 8.11)

Nota: item OPCIONAL.

2.5.2.5.5 Restrições de Algoritmos para Autoridades de Carimbo do Tempo (6.10, 8.11)

Nota: item OPCIONAL.

2.5.2.5.5.1 Restrições de Algoritmos (6.10, 8.11)

Nota: este item PODE se repetir de acordo com o número de restrições de algoritmos necessárias.

2.5.2.5.5.1.1 Identificador de Algoritmo (6.10, 8.11)

Neste item DEVE constar o OID do algoritmo a ser restringido.
2.5.2.5.5.1.2 Tamanho Mínimo de Chaves (6.10, 8.11)

Neste item PODE constar o tamanho mínimo de chave em bits.

2.5.2.5.5.1.3 Regras Adicionais de Restrições (6.11, 8.2)

Caso haja a necessidade de regras adicionais a restrições de algoritmos, essas devem ser incluídas neste item.

2.5.2.6 Regras Adicionais (6.11, 8.2)

Caso haja a necessidade de incluir regras adicionais para geração ou verificação de assinaturas digitais, essas DEVEM ser incluídas neste item.

g)2.5.3 Informações Adicionais sobre a Validação das Assinaturas (6.11, 8.2)

Caso haja a necessidade de informações adicionais quanto a validação das assinaturas digitais no âmbito desta Política de Assinatura, ela DEVEM ser incluídas neste item.

**2.6 Informações Adicionais sobre a Política de Assinatura (6.11, 8.2)**

Caso haja a necessidade de informações adicionais sobre a Política de Assinatura, elas DEVEM estar incluídas neste item.

# BIBLIOGRAFIA

[1] ETSI. *ASN.1 Format for Signature Policies*. Number TR 102 272. v.1.1.1, dez. 2003.

[2] ETSI. *XML Format for Signature Policies*. Number TR 102 038. v.1.1.1, abr. 2002.

[3] ITI. *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil.* Instituto Nacional de Tecnologia da Informação, Brasília, v.1.0. DOC-ICP-15.

[4] ITI. *Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil*. Instituto Nacional de Tecnologia da Informação, Brasília, v.1.0. DOC-ICP-15.01.

[5] ITI. *Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil*. Instituto Nacional de Tecnologia da Informação, Brasília, v.1.0. DOC-ICP-15.02.

[6] ITI. *Padrões e Algoritmos Criptográficos da ICP-Brasil*. Instituto Nacional de Tecnologia da Informação, Brasília, v.2.0, jun. 2009. DOC-ICP-01.01.

[7] ITI. *Requisitos para as Políticas de Certificado na ICP-Brasil*. Instituto Nacional de Tecnologia da Informação, Brasília, v.3.0, dez. 2008. DOC-ICP-04.

[8] ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3. V1.2.1. 2010.

[9] ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4. V1.1.1. 2009.

# ANEXO 1

## 1 POLÍTICAS DE ASSINATURA-PADRÃO ICP-BRASIL

Para facilitar a utilização de Políticas de Assinatura pelos usuários finais, o ITI criou 14 políticas de assinatura. Essas políticas foram criadas a partir do cruzamento do Perfil de Uso Geral para Assinaturas Digitais ICP-Brasil, definido no documento DOC-ICP-15.02, com os cinco formatos de assinatura digital da ICP-Brasil, derivados dos padrões CMS *Advanced Electronic Signature* (CAdES), XML *Advanced Electronic Signature* (XAdES) e PDF *Advanced Electronic Signature* (PAdES), citados no documento DOC-ICP-15.01, a saber:

a) Assinatura Digital com Referência do Tempo (AD-RT);
b) Assinatura Digital com Referência Básica (AD-RB);
c) Assinatura Digital com Referências para Validação (AD-RV);
d) Assinatura Digital com Referências Completas (AD-RC);
e) Assinatura Digital com Referências para Arquivamento (AD-RA).

As Tabelas A.2 a A.13 mostram a combinação dos elementos aplicada aos diferentes contextos de assinatura. A Tabela A.1 mostra o significado das abreviações utilizadas nas tabelas seguintes. Nos documentos 2 até 15 têm-se as 14 Políticas de Assinatura-padrão.

| Abreviação | Significado |
|---|---|
| ND | Não deve (proibido) |
| O | Obrigatório |
| P | Pode (opcional) |
| R | Recomendável |

*Tabela A.1: Abreviações utilizadas.*

**Nota 1**: Na codificação do atributo "SignaturePolicyIdentifier" (id-aa-ets-sigPolicyId {1.2.840.113549.1.9.16.2.15}), recomenda-se o uso do campo "sigPolicyQualifiers" para a indicação da Política de Assinatura, em Linguagem de Máquina, empregada nesta assinatura. Quando utilizado, o campo "sigPolicyQualifiers" somente deverá conter um único qualificador do tipo "spuri" (id-spq-ets-uri {1.2.840.113549.1.9.16.5.1}), cujo conteúdo deverá ser uma URI, ou URL, apontando para a Política de Assinatura, em Linguagem de Máquina, usada na assinatura.

**Nota 2**: O hash da política de assinatura no atributo id-aa-ets-sigPolicyId da assinatura deve ser o hash interno que está na própria PA e não o hash da PA que se encontra publicada na LPA.

**Nota 3**: Em atenção à RFC 3370 (Cryptographic Message Syntax (CMS) Algorithms), item "2.1 SHA-1"; e RFC 5754 (Using SHA2 Algorithms with Cryptographic Message Syntax), item "2 - Message Digest Algorithms", recomenda-se a ausência do campo "parameters" na estrutura "AlgorithmIdentifier", usada na indicação do algoritmo de hash, presentes nas estruturas ASN.1 "SignedData.digestAlgorithms", "SignerInfo.digestAlgorithm" e "SignaturePolicyId.sigPolicyHash.hashAlgorithm".

```
AlgorithmIdentifier ::= SEQUENCE {
algorithm   OBJECT IDENTIFIER,
parameters  ANY DEFINED BY algorithm OPTIONAL }.
```

**Nota 4**: Para o atributo ESSCertIDv2, utilizado nas versões 2.1 das políticas de assinatura baseadas em CAdES, as aplicações NÃO DEVEM codificar o campo "hashAlgorithm" caso utilize o mesmo algoritmo definido como valor *default* (SHA-256), conforme ISO 8825-1.

**Nota 5**: Quando do uso da codificação *MIME* no campo *eContent*, alerta-se para a necessidade de cuidado com a conversão do arquivo (*attached/detached*), pois esta conversão poderá invalidar a assinatura digital.

**Nota 6**: Recomenda-se o uso do *MimeType* caso seja codificado a propriedade *DataObjectFormat*, para as políticas XAdES.

**Nota 7:** Para as políticas PAdES deve-se observar as restrições de uso de atributos impostas nas Tabelas A.14 à A.21. Essas restrições são baseadas nos perfis ETSI PAdES-EPES [8] e ETSI PAdES-LTV [9].

**Nota 8:** Nas assinaturas PAdES-ICP-Brasil, deve-se usar as extensões de dicionários condizentes com as estruturas PDF para que uma aplicação leitora aderente reconheça e seja capaz de validar corretamente as assinaturas. Para todas as assinaturas deve-se usar as extensões indicadas no item 4.4.4.2, do DOC-ICP 15.02.

**Nota 9:** As tabelas A.14 à A.21 definem os atributos do CAdES, contidos na entrada *Contents* do dicionário de assinatura, assim como as entradas dos dicionários de assinatura, DSS, VRI e *Document Time-stamp*.

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O | O |
| | | | | | | |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O | O |
| | | | | | | |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate [1]**<br>**id-aa-signingCertificateV2 [2]** | O | O | O | O | O |
| | SigningCertificate | | | | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | O | O | O | O | O |
| | SignaturePolicyIdentifier | | | | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | P | P | P | P | P |
| | SignerRoles | | | | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | P | P | P | P | P |
| | SigningTime | | | | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | P | P | P | P | P |
| | SignerProductionPlace | | | | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | P | P | P | P | P |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | | | | |

*Tabela A.2: Atributos assinados no SignerInfo do Assinante*

*[1] – Atributo a ser adotado para as versões 1.0, 1.1 e 2.0;*
*[2] – Atributo a ser adotado a partir da versão 2.1.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | P | P | P | P | P |
| | CounterSignature | | | | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | O | O | O | ND |
| | SignatureTimeStamp | | | | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | P | P | O | O | O |
| | CompleteCertificateRefs | | | | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | P | P | O | O | O |
| | CompleteRevocationRefs | | | | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | P | P | P | P | P |
| | AttributeCertificateRefs | | | | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | P | P | P | P | P |
| | AttributeRevocationRefs | | | | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | P | O | O | ND |
| | SigAndRefsTimesStamp | | | | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | P | P | P | O | O |
| | CertificateValues | | | | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | P | P | P | O | O |
| | RevocationValues | | | | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND | O |
| | ArchiveTimeStamp | | | | | |

*Tabela A.3: Presença de atributos não-assinados no SignerInfo do signatário*

***Nota:*** *Contra-assinaturas NÃO DEVEM ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento, devido à interferência no processo de validação.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Tipo de conteúdo (*content type*) | **id-contentType** | ND | ND | ND | ND | ND |
| | | | | | | |
| Resumo criptográfico da mensagem (message digest) | **id-messageDigest** | O | O | O | O | O |
| | | | | | | |
| Certificado do signatário v1 (*ESS signing certificate*) | **id-aa-signingCertificate** | O | O | O | O | O |
| | SigningCertificate | | | | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | O | O | O | O | O |
| | SignaturePolicyIdentifier | | | | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | P | P | P | P | P |
| | SignerRoles | | | | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | P | P | P | P | P |
| | SigningTime | | | | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | P | P | P | P | P |
| | SignerProductionPlace | | | | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND | ND | ND | ND |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | | | | |

*Tabela A.4: Presença de atributos assinados no SignerInfo de "contra assinatura"*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **CT** | **RV** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | P | P | P | P | P |
| | CounterSignature | | | | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | O | O | O | ND |
| | SignatureTimeStamp | | | | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | P | P | O | O | O |
| | CompleteCertificateRefs | | | | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | P | P | O | O | O |
| | CompleteRevocationRefs | | | | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | P | P | P | P | P |
| | AttributeCertificateRefs | | | | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | P | P | P | P | P |
| | AttributeRevocationRefs | | | | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | P | O | O | ND |
| | SigAndRefsTimesStamp | | | | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | P | P | P | O | O |
| | CertificateValues | | | | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | P | P | P | O | O |
| | RevocationValues | | | | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND | ND |
| | ArchiveTimeStamp | | | | | |

*Tabela A.5: Presença de atributos não-assinados no SignerInfo de "contra assinatura"*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O | O |
| | | | | | | |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O | O |
| | | | | | | |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate [1]**<br>**id-aa-signingCertificateV2 [2]** | O | O | O | O | O |
| | SigningCertificate | | | | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | ND | ND | ND | ND | ND |
| | SignaturePolicyIdentifier | | | | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | ND | ND | ND | ND | ND |
| | SignerRoles | | | | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND | ND | ND | ND |
| | SigningTime | | | | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND | ND | ND | ND |
| | SignerProductionPlace | | | | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND | ND | ND | ND |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | | | | |

*Tabela A.6: Presença de atributos assinados no TimeStampToken de "carimbo do tempo de conteúdo"*

*[1] – Atributo a ser adotado para as versões 1.0, 1.1 e 2.0;*
*[2] – Atributo a ser adotado a partir da versão 2.1.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND | ND | ND | ND |
| | CounterSignature | | | | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | ND | ND | ND | ND |
| | SignatureTimeStamp | | | | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | R* | R* | O* | O* | O* |
| | CompleteCertificateRefs | | | | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | R* | R* | O* | O* | O* |
| | CompleteRevocationRefs | | | | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND | ND | ND | ND |
| | AttributeCertificateRefs | | | | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND | ND | ND | ND |
| | AttributeRevocationRefs | | | | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND | ND | ND | ND |
| | SigAndRefsTimesStamp | | | | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | R* | R* | R* | O* | O* |
| | CertificateValues | | | | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | R* | R* | R* | O* | O* |
| | RevocationValues | | | | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND | ND |
| | ArchiveTimeStamp | | | | | |

*Tabela A.7: Presença de atributos não-assinados no TimeStampToken de "carimbo do tempo de conteúdo"*

***Nota** *: Como o atributo "carimbo do tempo de conteúdo" é assinado, antes da assinatura do signatário devem ser incluídos os atributos não-assinados necessários para o perfil de AD mais complexo considerando seu ciclo de vida completo, pois não poderão ser incluídos posteriormente.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O | O |
| | | | | | | |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O | O |
| | | | | | | |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate [1]**<br>**id-aa-signingCertificateV2 [2]** | O | O | O | O | O |
| | SigningCertificate | | | | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | ND | ND | ND | ND | ND |
| | SignaturePolicyIdentifier | | | | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | ND | ND | ND | ND | ND |
| | SignerRoles | | | | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND | ND | ND | ND |
| | SigningTime | | | | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND | ND | ND | ND |
| | SignerProductionPlace | | | | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND | ND | ND | ND |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | | | | |

*Tabela A.8: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura".*

*[1] – Atributo a ser adotado para as versões 1.0, 1.1 e 2.0;*
*[2] – Atributo a ser adotado a partir da versão 2.1.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND | ND | ND | ND |
| | CounterSignature | | | | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | ND | ND | ND | ND |
| | SignatureTimeStamp | | | | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | P | P | O | O | O |
| | CompleteCertificateRefs | | | | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | P | P | O | O | O |
| | CompleteRevocationRefs | | | | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND | ND | ND | ND |
| | AttributeCertificateRefs | | | | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND | ND | ND | ND |
| | AttributeRevocationRefs | | | | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND | ND | ND | ND |
| | SigAndRefsTimesStamp | | | | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | P | P | P | O | O |
| | CertificateValues | | | | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | P | P | P | O | O |
| | RevocationValues | | | | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND | ND |
| | ArchiveTimeStamp | | | | | |

*Tabela A.9: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura."*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O | O |
| | | | | | | |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O | O |
| | | | | | | |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate [1]**<br>**id-aa-signingCertificateV2 [2]** | O | O | O | O | O |
| | SigningCertificate | | | | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | ND | ND | ND | ND | ND |
| | SignaturePolicyIdentifier | | | | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | ND | ND | ND | ND | ND |
| | SignerRoles | | | | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND | ND | ND | ND |
| | SigningTime | | | | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND | ND | ND | ND |
| | SignerProductionPlace | | | | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND | ND | ND | ND |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | | | | |

*Tabela A.10: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo das referências"*

*[1] – Atributo a ser adotado para as versões 1.0, 1.1 e 2.0;*
*[2] – Atributo a ser adotado a partir da versão 2.1.*

| Nome do atributo / Propriedade | Identificação do atributo | Perfil AD | | | | |
|---|---|---|---|---|---|---|
| | **Propriedade** | **RB** | **RT** | **RV** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND | ND | ND | ND |
| | CounterSignature | | | | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | ND | ND | ND | ND |
| | SignatureTimeStamp | | | | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | P | P | O | O | O |
| | CompleteCertificateRefs | | | | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | P | P | O | O | O |
| | CompleteRevocationRefs | | | | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND | ND | ND | ND |
| | AttributeCertificateRefs | | | | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND | ND | ND | ND |
| | AttributeRevocationRefs | | | | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND | ND | ND | ND |
| | SigAndRefsTimesStamp | | | | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | P | P | P | O | O |
| | CertificateValues | | | | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | P | P | P | O | O |
| | RevocationValues | | | | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND | ND |
| | ArchiveTimeStamp | | | | | |

*Tabela A.11: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo das referências"*

| Nome do atributo / Propriedade | Identificação do atributo | Carimbo | |
|---|---|---|---|
| | Propriedade | Anterior | Corrente |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O |
| | | | |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O |
| | | | |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate [1]**<br>**id-aa-signingCertificateV2 [2]** | O | O |
| | SigningCertificate | | |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | ND | ND |
| | SignaturePolicyIdentifier | | |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | ND | ND |
| | SignerRoles | | |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND |
| | SigningTime | | |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND |
| | SignerProductionPlace | | |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND |
| | AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp | | |

*Tabela A.12: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de arquivamento"*

*[1] – Atributo a ser adotado para as versões 1.0, 1.1 e 2.0;*
*[2] – Atributo a ser adotado a partir da versão 2.1.*

| Nome do atributo / Propriedade | Identificação do atributo | Carimbo | |
|---|---|---|---|
| | Propriedade | Anterior | Corrente |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND |
| | CounterSignature | | |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | ND |
| | SignatureTimeStamp | | |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | O | O |
| | CompleteCertificateRefs | | |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | O | O |
| | CompleteRevocationRefs | | |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND |
| | AttributeCertificateRefs | | |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND |
| | AttributeRevocationRefs | | |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND |
| | SigAndRefsTimesStamp | | |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | O | P |
| | CertificateValues | | |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | O | P |
| | RevocationValues | | |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND |
| | ArchiveTimeStamp | | |

*Tabela A.13: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de arquivamento"*

| Nome do Atributo | Identificação do Atributo | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O |
| Certificado do signatário (*ESS signing certificate*) | **Id-aa-signingCertificate** | ND | ND | ND | ND |
| | **Id-aa-signingCertificate V2** | O | O | O | O |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | O | O | O | O |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | P | P | P | P |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND | ND | ND |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND | ND | ND |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | P | P | P | P |
| Informações de Revogação (*adbe Revocation Information*) | **adbe-revocationInfoArchival** | ND | ND | ND | ND |

*Tabela A.14: Atributos assinados no SignerInfo do Assinante para assinaturas PAdES*

| Nome do Atributo | Identificação do Atributo | Perfil AD | | | |
|---|---|---|---|---|---|
| | | **RB** | **RT** | **RC** | **RA** |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND | ND | ND |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | P | O | O | O |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | ND | ND | ND | ND |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | ND | ND | ND | ND |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND | ND | ND |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND | ND | ND |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND | ND | ND |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | ND | ND | ND | ND |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | ND | ND | ND | ND |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND |

*Tabela A.15: Presença de atributos não-assinados no SignerInfo do signatário para assinatura PAdES*

| Nome do Atributo | Identificação do Atributo | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Tipo de conteúdo (*content type*) | **id-contentType** | O | O | O | O |
| Resumo criptográfico da mensagem (*message digest*) | **id-messageDigest** | O | O | O | O |
| Certificado do signatário (*ESS signing certificate*) | **id-aa-signingCertificate** | ND | ND | ND | ND |
| | **id-aa-signingCertificateV2** | O | O | O | O |
| Identificador da política de assinatura (*signature policy identifier*) | **id-aa-ets-sigPolicyId** | ND | ND | ND | ND |
| Atributos do signatário (*signer attributes*) | **id-aa-ets-signerAttr** | ND | ND | ND | ND |
| Instante da assinatura (*signing time*) | **id-signingTime** | ND | ND | ND | ND |
| Localização do signatário (*signer location*) | **id-aa-ets-signerLocation** | ND | ND | ND | ND |
| Carimbo do tempo de conteúdo (*content time stamp*) | **id-aa-ets-contentTimeStamp** | ND | ND | ND | ND |

*Tabela A.16: Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura" para assinaturas PAdES.*

| Nome do Atributo | Identificação do Atributo | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Contra assinatura (*countersignature*) | **id-countersignature** | ND | ND | ND | ND |
| Carimbo do tempo de assinatura (*signature time stamp*) | **id-aa-signatureTimeStampToken** | ND | ND | ND | ND |
| Referências completas aos certificados (*complete certificate references*) | **id-aa-ets-certificateRefs** | ND | ND | ND | ND |
| Referências completas à revogação *(complete revogation references)* | **id-aa-ets-revocationRefs** | ND | ND | ND | ND |
| Referências aos certificados de atributo (*attribute certificate references*) | **id-aa-ets-attrCertificateRefs** | ND | ND | ND | ND |
| Referências à revogação de atributo (*attribute revogation references*) | **id-aa-ets-attrRevocationRefs** | ND | ND | ND | ND |
| Carimbo do tempo das referências (*time-stamped certificate crls references*) | **id-aa-ets-escTimeStamp** | ND | ND | ND | ND |
| Valores dos certificados (*certificate values*) | **id-aa-ets-certValues** | ND | ND | ND | ND |
| Valores de revogação (*revocation values*) | **id-aa-ets-revocationValues** | ND | ND | ND | ND |
| Carimbo do tempo de arquivamento (*archive time-stamp)* | **id-aa-ets-archiveTimestampV2** | ND | ND | ND | ND |

*Tabela A.17: Presença de atributos não-assinados no SignerInfo do TimeStampToken de "carimbo do tempo de assinatura" para assinaturas PAdES.*

| Entrada | Valor padrão | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Type | Sig | O | O | O | O |
| Filter | PBAD_PAdES | O | O | O | O |
| SubFilter | PBAD.PAdES | O | O | O | O |
| Contents | Não aplicável | O | O | O | O |
| Cert | Não aplicável | ND | ND | ND | ND |
| ByteRange | Não aplicável | O | O | O | O |
| Reference | Não aplicável | P | P | P | P |
| Changes | Não aplicável | P | P | P | P |
| Name | Não aplicável | P | P | P | P |
| M | Não aplicável | P | P | P | P |
| Location | Não aplicável | P | P | P | P |
| Reason | Não aplicável | P | P | P | P |
| ContactInfo | Não aplicável | P | P | P | P |
| R | Não aplicável | ND | ND | ND | ND |
| V | 0 | P | P | P | P |
| Prop_Build | Não aplicável | P | P | P | P |
| Prop_AuthTime | Não aplicável | P | P | P | P |
| Prop_AuthType | Não aplicável | ND | ND | ND | ND |

*Tabela A.18: Presença das entradas do dicionário de assinaturas do PAdES.*

**Nota**: É possível associar um Seed Value Dictionary a um dicionário de assinatura, esse dicionário pode ser usado para indicar qual política de assinatura um assinante deverá usar. Para isso, devem ser usadas as modificações descritas no documento ETSI TS 102 773-3. É importante perceber que o uso desse dicionário não substitui o uso de políticas de assinatura, pois esse dicionário é apenas uma condição para a geração da assinatura, enquanto uma PA são regras acordadas entre assinante e verificador as quais ambos devem seguir.

| Entrada | Valor Padrão | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Type | DSS | O | O | O | O |
| VRI | Não aplicável | O | O | O | O |
| Certs | Não aplicável | O | O | O | O |
| OCSPs | Não aplicável | P* | P* | P* | P* |
| CRLs | Não aplicável | P* | P* | P* | P* |
| PBAD_PolicyArtifacts | Não aplicável | P | P | P | O |
| PBAD_LpaArtifacts | Não aplicável | P | P | P | O |
| PBAD_LpaSignatures | Não aplicável | P | P | P | O |

*Tabela A.19: Presença das entradas do dicionário DSS do PAdES.*

**Nota ***: As entradas OCSPs e CRLs DEVEM constar no DSS. Nota-se que o uso de ambas ao mesmo tempo não é proibido.

| Entrada | Valor Padrão | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Type | VRI | O | O | O | O |
| Cert | Não aplicável | O | O | O | O |
| OCSP | Não aplicável | P[1] | P[1] | P[1] | P[1] |
| CRL | Não aplicável | P[1] | P[1] | P[1] | P[1] |
| TU | Não aplicável | P[2] | P[2] | P[2] | P[2] |
| TS | Não aplicável | P[2] | P[2] | P[2] | P[2] |
| PBAD_PolicyArtifact | Não aplicável | P | P | P | O |
| PBAD_LpaArtifact | Não aplicável | P | P | P | O |
| PBAD_LpaSignature | Não aplicável | P | P | P | O |

*Tabela A.20: Presença das entradas do dicionário VRI do PAdES.*

**Nota 1:** As entradas OCSP e CRL DEVEM constar no VRI. Nota-se que o uso de ambas ao mesmo tempo não é proibido.

**Nota 2**: As entradas TU e TS são mutuamente exclusivas, ou seja, se um for codificado o outro não deve ser codificado.

| Entrada | Valor Padrão | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Type | DocTimeStamp | O | O | O | O |
| SubFilter | ETSI.RFC3161 | O | O | O | O |
| Contents | Não aplicável | O | O | O | O |
| V | 0 | P | P | P | P |

*Tabela A.21: Presença das entradas do dicionário de assinatura do Document Timestamp do PAdES.*

| Dicionário | Identificação do Dicionário | Perfil AD | | | |
|---|---|---|---|---|---|
| | | RB | RT | RC | RA |
| Dicionário de assinatura | Signature Dictionary | O | O | O | O |
| DSS | DSS Dicionary | P | P | O | O |
| VRI | VRI Dictionary | P* | P* | O | O |
| Document Time-stamp | Document Time-stamp Dictionary | P | P | O | O |

Tabela A.22: Presença de dicionários PDF relacionados às assinaturas PAdES.

**Nota**: Caso seja utilizado DSS para os formatos RB e RT deve-se usar o VRI.

# ANEXO 2

## 1 POLÍTICA-PADRÃO AD-RB BASEADA EM CADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO CMS, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO CMS, versão 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.1.1.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO CMS, versão 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO CMS, versão 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO CMS, versão 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.2.2.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 2.0: 26/12/2011;
d) para a versão 2.1: 06/03/2012;
e) para a versão 2.2: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

### 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócio nos quais a assinatura digital agrega segurança à autenticação de entidades e verificação de integridade, permitindo sua validação durante o prazo de validade dos certificados dos signatários.

Uma vez que não são usados carimbos do tempo, a validação posterior só será possível se existirem referências temporais que identifiquem o momento em que ocorreu a assinatura digital.

Nessas situações, deve existir legislação específica ou um acordo prévio entre as partes definindo as referências a serem utilizadas.

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

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 29/02/2012.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 06/03/2012 a 02/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c.1) **Para as versões 1.0, 1.1 e 2.0, id-aa-signingCertificate;**
c.2) **A partir da versão 2.1, inclusive, id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

###### 5.2.1.1.3 Certificados Obrigatoriamente Referenciados

O atributo **signingCertificate** deve conter referência apenas ao certificado do signatário.

###### 5.2.1.1.4 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: nenhum certificado.
Para as versões 1.1, 2.0, 2.1 e 2.2: o certificado do signatário.

#### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

##### 5.2.2.1 Requisitos de Certificados

###### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em :

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

### 5.2.2.2 Requisitos de Revogação

#### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.2.2.2 Requisitos de Revogação para Certificados ACs

##### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Conjunto de Restrições de Algoritmos

#### 5.2.3.1 Restrições de Algoritmos para Signatários

##### 5.2.3.1.1 Restrições de Algoritmos

###### 5.2.3.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha1withRSAEncryption(1 2 840 113549 1 1 5);
b) para a versão 1.1: sha1withRSAEncryption(1 2 840 113549 1 1 5) ou sha256WithRSAEncryption(1.2.840.113549.1.1.11);
c) para as versões 2.0 e 2.1: sha256WithRSAEncryption(1.2.840.113549.1.1.11);

d) para a versão 2.2: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

#### 5.2.3.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 1024 bits;
b) para a versão 1.1: 1024 bits;
c) para as versões 2.0, 2.1 e 2.2: 2048 bits.

## 2 POLÍTICA-PADRÃO AD-RT BASEADA EM CADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO CMS, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO CMS, versão 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.1.1.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO CMS, versão 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO CMS, versão 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO CMS, versão 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.2.2.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 2.0: 26/12/2011;
d) para a versão 2.1: 06/03/2012;
e) para a versão 2.2: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

### 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócios nos quais a assinatura digital necessita de segurança em relação à irretratabilidade do momento de sua geração.

Como esse tipo de assinatura não traz, de forma autocontida, referências ou valores dos certificados e das informações de revogação (LCRs ou respostas OCSP) necessários para sua validação posterior, ele deve ser utilizado somente quando esses dados puderem ser obtidos por meios externos, de forma inequívoca. Uma assinatura desse tipo pode ter sua capacidade probante diminuída, no caso de comprometimento da chave da AC que emitiu qualquer um dos certificados da cadeia de certificação.
Segundo esta PA, é permitido o emprego de múltiplas assinaturas.

# 5 Política de Validação da Assinatura

## 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 06/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

## 5.2 Regras Comuns

### 5.2.1 Regras de Signatário e Verificador

#### 5.2.1.1 Regras do Signatário

##### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

##### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, os seguintes atributos assinados:

a) **id-contentType**;
b) **id-messageDigest**;
c.1) **Para as versões 1.0, 1.1 e 2.0, id-aa-signingCertificate;**
c.2) **A partir da versão 2.1, inclusive, id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

##### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, o atributo não assinado **id-aa-signatureTimeStampToken**.

##### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **signingCertificate** deve conter referência apenas ao certificado do signatário.

##### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: nenhum certificado
Para as versões 1.1, 2.0, 2.1 e 2.2: o certificado do signatário.

#### 5.2.1.2 Regras do Verificador

##### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenha sido incluído pelo signatário, o atributo **id-aa-signatureTimeStampToken** DEVE ser incluído pelo verificador.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

##### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade de Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de

confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

### 5.2.3.2 Requisitos de Revogação

#### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

#### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

#### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatários

#### 5.2.4.1.1 Restrições de Algoritmos

#### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha1withRSAEncryption(1 2 840 113549 1 1 5);
b) para a versão 1.1: sha1withRSAEncryption(1 2 840 113549 1 1 5) ou sha256WithRSAEncryption(1.2.840.113549.1.1.11);

c) para as versões 2.0 e 2.1: sha256WithRSAEncryption(1.2.840.113549.1.1.11);
d) para a versão 2.2: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

#### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 1024 bits;
b) para a versão 1.1: 1024 bits;
c) para as versões 2.0, 2.1 e 2.2: 2048 bits.

## 3 POLÍTICA-PADRÃO AD-RV BASEADA EM CADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO CMS, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.3.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO CMS, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.3.1.1.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO CMS, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.3.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO CMS, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.3.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO CMS, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.3.2.2.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 2.0: 26/12/2011;
d) para a versão 2.1: 06/03/2012;
e) para a versão 2.2: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

### 4 Campo de Aplicação

Este tipo de assinatura inclui, no seu próprio corpo, referências sobre os certificados que compõem a cadeia de certificação e sobre as informações de revogação do certificado digital do signatário. Um carimbo do tempo provê a ligação entre essas informações e o conteúdo assinado.

Ele deve ser usado em aplicações onde se necessita verificar a assinatura a qualquer momento e onde os dados necessários para isso (que estão referenciados no corpo da assinatura), estejam disponíveis para recuperação.

Além de oferecer segurança quanto à irretratabilidade, ele permite que se verifique a validade da

assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo do tempo sobre as referências tenha sido colocado antes desse comprometimento.
Segundo esta PA, é permitido o emprego de múltiplas assinaturas.

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 06/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos à Assinatura

O conteúdo assinado pode ser tanto interno quanto externo à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, os seguintes atributos assinados:

a) **id-contentType**;
b) **id-messageDigest**;
c.1) **Para as versões 1.0, 1.1 e 2.0, id-aa-signingCertificate;**
c.2) **A partir da versão 2.1, inclusive, id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

###### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, os seguintes atributos não assinados:

a) **id-aa-signatureTimeStampToken**;
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-escTimeStamp**.

###### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **signingCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios da Cadeia de Certificação

Para a versão 1.0: nenhum certificado
Para as versões 1.1, 2.0, 2.1 e 2.2: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

a) **id-aa-signatureTimeStampToken**;
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-escTimeStamp**.

## 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em :

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade de Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2 Requisitos de Revogação de Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatário

##### 5.2.4.1.1 Restrições de Algoritmos

###### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha1withRSAEncryption(1 2 840 113549 1 1 5);
b) para a versão 1.1: sha1withRSAEncryption(1 2 840 113549 1 1 5) ou sha256WithRSAEncryption(1.2.840.113549.1.1.11);
c) para as versões 2.0 e 2.1 : sha256WithRSAEncryption(1.2.840.113549.1.1.11);
d) para a versão 2.2: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

###### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 1024 bits;
b) para a versão 1.1: 1024 bits;
c) para as versões 2.0, 2.1 e 2.2: 2048 bits.

## 4 POLÍTICA-PADRÃO AD-RC BASEADA EM CADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO CMS, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.4.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO CMS, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.4.1.1.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO CMS, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.4.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO CMS, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.4.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO CMS, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.4.2.2.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 2.0: 26/12/2011;
d) para a versão 2.1: 06/03/2012;
e) para a versão 2.2: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

### 4 Campo de Aplicação

Este tipo de assinatura inclui, no seu próprio corpo, além das referências, os certificados que compõem a cadeia de certificação e as informações de revogação do certificado digital do signatário. Ele demanda uma maior capacidade de armazenamento.

Ele deve ser usado em situações onde é necessária a verificação completa da validade da assinatura digital a qualquer momento, pois os dados necessários estão autocontidos na assinatura.

Além de oferecer segurança quanto à irretratabilidade, ele permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o

certificado do signatário, desde que o carimbo do tempo sobre as referências/valores dos certificados tenha sido colocado antes desse comprometimento.

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

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 06/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c.1) **Para as versões 1.0, 1.1 e 2.0, id-aa-signingCertificate;**
c.2) **A partir da versão 2.1, inclusive, id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

###### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

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

a) **id-aa-signatureTimeStampToken**;
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-escTimeStamp**;
e) **id-aa-ets-certValues**;
f) **id-aa-ets-revocationValues**.

###### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **signingCertificate** deve conter referência apenas para o certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios no Caminho de Certificação

Para a versão 1.0: os certificados do caminho de certificação completo do signatário;
Para as versões 1.1, 2.0, 2.1 e 2.2: o certificado do signatário.

#### 5.2.1.1.6 Regras Adicionais do Signatário

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

a) **id-aa-signatureTimeStampToken**;
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-escTimeStamp**;
e) **id-aa-ets-certValues**;
f) **id-aa-ets-revocationValues**.

## 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

**5.2.2.2.1.1** Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

#### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0 e 2.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

### 5.2.4.1 Restrições de Algoritmos para Signatário

#### 5.2.4.1.1 Restrições de Algoritmos

##### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha1withRSAEncryption(1 2 840 113549 1 1 5);
b) para a versão 1.1: sha1withRSAEncryption(1 2 840 113549 1 1 5) ou sha256WithRSAEncryption(1.2.840.113549.1.1.11);
c) para as versões 2.0 e 2.1: sha256WithRSAEncryption(1.2.840.113549.1.1.11);
d) para a versão 2.2: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

##### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 1024 bits;
b) para a versão 1.1: 1024 bits;
c) para as versões 2.0, 2.1 e 2.2: 2048 bits.

## 5 POLÍTICA-PADRÃO AD-RA BASEADA EM CADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.5.2.3.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;

b) para a versão 1.1: 26/12/2011;

c) para a versão 1.2: 21/09/2012;

d) para a versão 2.0: 26/12/2011;

e) para a versão 2.1: 06/03/2012;

f) para a versão 2.2: 21/09/2012;

g) para a versão 2.3: 27/04/2016.

### 3 Nome da Entidade emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura é adequado para aplicações que necessitam realizar o arquivamento do conteúdo digital assinado por longos períodos, sabendo-se que podem surgir fraquezas, vulnerabilidades ou exposição a fragilidades dos algoritmos, funções e chaves criptográficas utilizadas no processo de geração de assinatura digital.

Ele provê proteção contra fraqueza dos algoritmos, funções e tamanho de chaves criptográficas, desde que o carimbo do tempo de arquivamento seja realizado tempestivamente e utilize algoritmos, funções e tamanhos de chave considerados seguros no momento de sua geração.

Além disso, oferece segurança quanto à irretratabilidade, e permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário (desde que o carimbo do tempo sobre as referências/valores dos certificados tenha sido colocado antes desse comprometimento).

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2011 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 06/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c.1) **Para as versões 1.0, 1.1 e 2.0, id-aa-signingCertificate;**
c.2) **Para as versões 1.2, 2.1, 2.2 e 2.3 id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

#### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

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

Para as versões 1.0, 1.1, 2.0 e 2.1:

**a) id-aa-signatureTimeStampToken;**
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-certValues**;
e) **id-aa-ets-revocationValues**;
f) **id-aa-ets-archiveTimestampV2**.

Para as versões 1.2, 2.2 e 2.3:

a) **id-aa-ets-certificateRefs**;
b) **id-aa-ets-revocationRefs**;
c) **id-aa-ets-certValues**;
d) **id-aa-ets-revocationValues**;
e) **id-aa-ets-archiveTimestampV2**.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **signingCertificate** deve conter referência apenas para o certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: os certificados do caminho de certificação completo do signatário;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

Para as versões 1.0, 1.1, 2.0 e 2.1:

**a) id-aa-signatureTimeStampToken;**
b) **id-aa-ets-certificateRefs**;
c) **id-aa-ets-revocationRefs**;
d) **id-aa-ets-certValues**;
e) **id-aa-ets-revocationValues**;
f) **id-aa-ets-archiveTimestampV2**.

Para as versões 1.2, 2.2 e 2.3:

a) **id-aa-ets-certificateRefs**;
b) **id-aa-ets-revocationRefs**;
c) **id-aa-ets-certValues**;
d) **id-aa-ets-revocationValues**;
e)**id-aa-ets-archiveTimestampV2**.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

##### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de

confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para as versões 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

### 5.2.3.2 Requisitos de Revogação

#### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2Requisitos de Revogação para Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

### 5.2.4.1 Restrições de Algoritmos para Signatário

#### 5.2.4.1.1 Restrições de Algoritmos

##### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha1withRSAEncryption(1 2 840 113549 1 1 5);
b) para a versão 1.1 e 1.2: sha1withRSAEncryption(1 2 840 113549 1 1 5) ou sha256WithRSAEncryption(1.2.840.113549.1.1.11);

c) para as versões 2.0, 2.1 e 2.2: sha256WithRSAEncryption(1.2.840.113549.1.1.11);
d) para a versão 2.3: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

#### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 1024 bits;
b) para a versão 1.1 e 1.2: 1024 bits;
c) para as versões 2.0, 2.1, 2.2 e 2.3: 2048 bits.

# 6 POLÍTICA-PADRÃO AD-RB BASEADA EM XADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO XML-DSig, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.6.2.3.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 1.2: 21/09/2012;
d) para a versão 2.0: 26/12/2011;
e) para a versão 2.1: 22/03/2012;
f) para a versão 2.2: 21/09/2012;
g) para a versão 2.3: 27/04/2016.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócio nos quais a assinatura digital agrega segurança à autenticação de entidades e verificação de integridade, permitindo sua validação durante o prazo de validade dos certificados dos signatários.
Uma vez que não são usados carimbos do tempo, a validação posterior só será possível se existirem referências temporais que identifiquem o momento em que ocorreu a assinatura digital. Nessas situações, deve existir legislação específica ou um acordo prévio entre as partes definindo as referências a serem utilizadas.

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

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2012 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 22/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:

a) **DataObjectFormat (em assinaturas do tipo *detached*);**
b)**SigningCertificate**;
c) **SignaturePolicyIdentifier**.

Para as versões 1.2, 2.2 e 2.3:

a) **SigningCertificate**;
b) **SignaturePolicyIdentifier**.

###### 5.2.1.1.3 Certificados Obrigatoriamente Referenciados

A propriedade **SigningCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.4 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: nenhum certificado;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em :

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

#### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

#### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

#### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Conjunto de Restrições de Algoritmos

#### 5.2.3.1 Restrições de Algoritmos para Signatário

##### 5.2.3.1.1 Restrições de Algoritmos

###### 5.2.3.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0 e 1.2: http://www.w3.org/2000/09/xmldsig#rsa-sha1;
b) para a versão 1.1: http://www.w3.org/2000/09/xmldsig#rsa-sha1 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
c) para a versão 2.0, 2.1 e 2.2: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
d) para a versão 2.3: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha512.

###### 5.2.3.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0, 1.1 e 1.2: 1024 bits;
b) para a versão 2.0, 2.1, 2.2 e 2.3: 2048 bits.

# 7 POLÍTICA-PADRÃO AD-RT BASEADA EM XADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO XML-DSig, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.7.2.3.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 1.2: 21/09/2012;
d) para a versão 2.0: 26/12/2011;
e) para a versão 2.1: 22/03/2012;
f) para a versão 2.2: 21/09/2012;
g) para a versão 2.3: 27/04/2016.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócios nos quais a assinatura digital necessita de segurança em relação à irretratabilidade do momento de sua

geração.

Como esse tipo de assinatura não traz, de forma autocontida, referências ou valores dos certificados e das informações de revogação (LCRs ou respostas OCSP) necessários para sua validação posterior, ele deve ser utilizado somente quando esses dados puderem ser obtidos por meios externos, de forma inequívoca. Uma assinatura desse tipo pode ter sua capacidade probante diminuída, no caso de comprometimento da chave da AC que emitiu qualquer um dos certificados da cadeia de certificação.

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

## 5 Política de Validação da Assinatura

Os campos a seguir definem os processos para geração e verificação de assinaturas realizadas segundo esta PA.

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2012 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 22/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:
Para as versões 1.0, 1.1, 2.0 e 2.1:

a) **DataObjectFormat (em assinaturas do tipo *detached*);**
b) **SigningCertificate**;
c) **SignaturePolicyIdentifier**.

Para as versões 1.2, 2.2 e 2.3:

a) **SigningCertificate**;
b) **SignaturePolicyIdentifier**.

#### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades não assinadas:

**a) SignatureTimeStamp**

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

A propriedade **SigningCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: nenhum certificado;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenha sido incluída pelo signatário, a seguinte propriedade DEVE ser incluída pelo verificador:

a) **SignatureTimeStamp**.

## 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em :

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID

2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatário

##### 5.2.4.1.1 Restrições de Algoritmos

###### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0 e 1.2: http://www.w3.org/2000/09/xmldsig#rsa-sha1;
b) para a versão 1.1: http://www.w3.org/2000/09/xmldsig#rsa-sha1 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
c) para a versão 2.0, 2.1 e 2.2: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
d) para a versão 2.3: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha512.

###### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0, 1.1 e 1.2: 1024 bits;
b) para a versão 2.0, 2.1, 2.2 e 2.3: 2048 bits.

## 8 POLÍTICA-PADRÃO AD-RV BASEADA EM XADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA VALIDACAO NO FORMATO XML-DSig, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.8.2.3.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 1.2: 21/09/2012;
d) para a versão 2.0: 26/12/2011;
e) para a versão 2.1: 22/03/2012;
f) para a versão 2.2: 21/09/2012;
g) para a versão 2.3: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

### 4 Campo de Aplicação

Este tipo de assinatura inclui, no seu próprio corpo, referências sobre os certificados que compõem a cadeia de certificação e sobre as informações de revogação do certificado digital do

signatário. Um carimbo do tempo provê a ligação entre essas informações e o conteúdo assinado. Ele deve ser usado em aplicações onde se necessita verificar a assinatura a qualquer momento e onde os dados necessários para isso (que estão referenciados no corpo da assinatura), estejam disponíveis para recuperação.

Além de oferecer segurança quanto à irretratabilidade, ele permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo do tempo sobre as referências tenha sido colocado antes desse comprometimento.

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

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2012 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 22/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:

a) **DataObjectFormat (em assinaturas do tipo *detached*);**
b) **SigningCertificate**;
c) **SignaturePolicyIdentifier**.

Para as versões 1.2, 2.2 e 2.3:

a) **SigningCertificate**;
b) **SignaturePolicyIdentifier.**

###### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades não

assinadas:

a) **SignatureTimeStamp**;
b) **CompleteCertificateRefs**;
c) **CompleteRevocationRefs**;
d) **SigAndRefsTimeStamp**.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

A propriedade **SigningCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: nenhum certificado;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídas pelo signatário, as seguintes propriedades DEVEM ser incluídas pelo verificador:

**a) SignatureTimeStamp;**
**b) CompleteCertificateRefs;**
**c) CompleteRevocationRefs;**
**d) SigAndRefsTimeStamp.**

## 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

### 5.2.2.2 Requisitos de Revogação

#### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatário

##### 5.2.4.1.1 Restrições de Algoritmos

###### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0 e 1.2: http://www.w3.org/2000/09/xmldsig#rsa-sha1;
b) para a versão 1.1: http://www.w3.org/2000/09/xmldsig#rsa-sha1 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
c) para a versão 2.0, 2.1 e 2.2: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
d) para a versão 2.3: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha512.

###### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0, 1.1 e 1.2: 1024 bits;
b) para a versão 2.0, 2.1, 2.2 e 2.3: 2048 bits.

# 9 POLÍTICA-PADRÃO AD-RC BASEADA EM XADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO XML-DSig, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.9.2.3.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 1.2: 21/09/2012;
d) para a versão 2.0: 26/12/2011;
e) para a versão 2.1: 22/03/2012;
f) para a versão 2.2: 21/09/2012;
g) para a versão 2.3: 27/04/2016.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura inclui, no seu próprio corpo, além das referências, os certificados que compõem a cadeia de certificação e as informações de revogação do certificado digital do

signatário. Ele demanda uma maior capacidade de armazenamento.

Ele deve ser usado em situações onde é necessária a verificação completa da validade da assinatura digital a qualquer momento, pois os dados necessários estão autocontidos na assinatura.

Além de oferecer segurança quanto à irretratabilidade, ele permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo do tempo sobre as referências/valores dos certificados tenha sido colocado antes desse comprometimento.

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

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2012 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 22/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:

a) **DataObjectFormat (em assinaturas do tipo *detached*);**
b) **SigningCertificate**;
c) **SignaturePolicyIdentifier**.

Para as versões 1.2, 2.2 e 2.3:

a) **SigningCertificate**;
b) **SignaturePolicyIdentifier**.

###### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades não assinadas:

a) **SignatureTimeStamp**;
b) **CompleteCertificateRefs**;
c) **CompleteRevocationRefs**;
d) **SigAndRefsTimeStamp**;
e) **CertificateValues**;
f) **RevocationValues**.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

A propriedade **SigningCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: os certificados do caminho de certificação completo do signatário;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídas pelo signatário, as seguintes propriedades DEVEM ser incluídas pelo verificador:

a) **SignatureTimeStamp**;
b) **CompleteCertificateRefs**;
c) **CompleteRevocationRefs**;
d) **SigAndRefsTimeStamp**;
e) **CertificateValues**;
f) **RevocationValues**.

## 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em :

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

### 5.2.2.2 Requisitos de Revogação

#### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e

http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

### 5.2.3.2 Requisitos de Revogação

#### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

## 5.2.4 Conjunto de Restrições de Algoritmos

### 5.2.4.1 Restrições de Algoritmos para Signatário

#### 5.2.4.1.1 Restrições de Algoritmos

##### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0 e 1.2: http://www.w3.org/2000/09/xmldsig#rsa-sha1;
b) para a versão 1.1: http://www.w3.org/2000/09/xmldsig#rsa-sha1 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
c) para a versão 2.0, 2.1, 2.2: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
d) para a versão 2.3: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha512.

##### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0, 1.1 e 1.2: 1024 bits;
b) para a versão 2.0, 2.1, 2.2 e 2.3: 2048 bits.

## 10 POLÍTICA-PADRÃO AD-RA BASEADA EM XADES

### 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 1.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.1.1.

O nome desta Política de Assinatura para a versão 1.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 1.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.1.2.

O nome desta Política de Assinatura para a versão 2.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 2.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.2.

O nome desta Política de Assinatura para a versão 2.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.2.1.

O nome desta Política de Assinatura para a versão 2.2 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 2.2 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.2.2.

O nome desta Política de Assinatura para a versão 2.3 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig, versao 2.3 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.10.2.3.

### 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 31/10/2008;
b) para a versão 1.1: 26/12/2011;
c) para a versão 1.2: 21/09/2012;
d) para a versão 2.0: 26/12/2011;
e) para a versão 2.1: 22/03/2012;
f) para a versão 2.2: 21/09/2012;
g) para a versão 2.3: 27/04/2016.

### 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura é adequado para aplicações que necessitam realizar o arquivamento do conteúdo digital assinado por longos períodos, sabendo-se que podem surgir fraquezas, vulnerabilidades ou exposição a fragilidades dos algoritmos, funções e chaves criptográficas utilizadas no processo de geração de assinatura digital.

Ele provê proteção contra fraqueza dos algoritmos, funções e tamanho de chaves criptográficas, desde que o carimbo do tempo de arquivamento seja realizado tempestivamente e utilize algoritmos, funções e tamanhos de chave considerados seguros no momento de sua geração.

Além disso, oferece segurança quanto à irretratabilidade, e permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário (desde que o carimbo do tempo sobre as referências/valores dos certificados tenha sido colocado antes desse comprometimento).

## 5 Política de Validação da Assinatura

Os campos a seguir definem os processos para geração e verificação de assinaturas realizadas segundo esta PA.

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 31/10/2008 a 31/12/2014.
Para a versão 1.1, o período para assinatura desta PA é de 26/12/2011 a 31/12/2014.
Para a versão 1.2, o período para assinatura desta PA é de 21/09/2012 a 31/12/2014.
Para a versão 2.0, o período para assinatura desta PA é de 26/12/2011 a 21/06/2023.
Para a versão 2.1, o período para assinatura desta PA é de 22/03/2012 a 21/06/2023.
Para a versão 2.2, o período para assinatura desta PA é de 21/09/2012 a 21/06/2023.
Para a versão 2.3, o período para assinatura desta PA é de 27/04/2016 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

#### 5.2.1.1 Regras do Signatário

##### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado pode ser tanto externo quanto interno à assinatura

##### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:

a) **DataObjectFormat (em assinaturas do tipo *detached*);**
b) **SigningCertificate**;
c) **SignaturePolicyIdentifier**.

Para as versões 1.2, 2.2 e 2.3:

a) **SigningCertificate**;
b) **SignaturePolicyIdentifier.**

#### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades não assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:

**a) SignatureTimeStamp;**
b) **CompleteCertificateRefs**;
c) **CompleteRevocationRefs**;
d) **CertificateValues**;
e) **RevocationValues**;
f) **ArchiveTimeStamp**.

Para as versões 1.2, 2.2 e 2.3:

a) **CompleteCertificateRefs**;
b) **CompleteRevocationRefs**;
c) **CertificateValues**;
d) **RevocationValues**;
e) **ArchiveTimeStamp**.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

A propriedade **SigningCertificate** deve conter apenas referência ao certificado do signatário.

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: os certificados do caminho de certificação completo do signatário;
Para as versões 1.1, 1.2, 2.0, 2.1, 2.2 e 2.3: o certificado do signatário.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídas pelo signatário, as seguintes propriedades DEVEM ser incluídas pelo verificador:

Para as versões 1.0, 1.1, 2.0 e 2.1:

**a) SignatureTimeStamp;**
b) **CompleteCertificateRefs**;
c) **CompleteRevocationRefs**;
d) **CertificateValues**;
e) **RevocationValues**;
f) **ArchiveTimeStamp**.

Para as versões 1.2, 2.2 e 2.3:

a) **CompleteCertificateRefs**;
b) **CompleteRevocationRefs**;
c) **CertificateValues**;
d) **RevocationValues**;
e) **ArchiveTimeStamp**.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

##### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0 e 1.2:
http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt;

b) para a versão 1.1:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

c) para a versão 2.0, 2.1 e 2.2:
http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt;

d) para a versão 2.3:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatário

##### 5.2.4.1.1 Restrições de Algoritmos

##### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o

algoritmo :

a) para a versão 1.0 e 1.2: http://www.w3.org/2000/09/xmldsig#rsa-sha1;
b) para a versão 1.1: http://www.w3.org/2000/09/xmldsig#rsa-sha1 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
c) para a versão 2.0, 2.1 e 2.2: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256;
d) para a versão 2.3: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 ou http://www.w3.org/2001/04/xmldsig-more#rsa-sha512.

#### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0, 1.1 e 1.2: 1024 bits;
b) para a versão 2.0, 2.1, 2.2 e 2.3: 2048 bits.

# 11 POLÍTICA-PADRÃO AD-RB BASEADA EM PADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA BASICA NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.11.1.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 25/08/2015.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócio nos quais a assinatura digital agrega segurança à autenticação de entidades e verificação de integridade, permitindo sua validação durante o prazo de validade dos certificados dos signatários.

Uma vez que não são usados carimbos do tempo, a validação posterior só será possível se existirem referências temporais que identifiquem o momento em que ocorreu a assinatura digital. Nessas situações, deve existir legislação específica ou um acordo prévio entre as partes definindo as referências a serem utilizadas.

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

Esse tipo de PA é aplicável apenas em arquivos do tipo PDF.

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 25/08/2015 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado deve ser externo à assinatura.

###### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c) **id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

#### 5.2.1.1.3 - Atributos ou Propriedades Não-Assinados Obrigatórios

Não possui atributos não-assinados obrigatórios.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

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

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: o certificado do signatário.

#### 5.2.1.1.6 Regras Adicionais do Signatário

#### 5.2.1.1.6.1 Extensão br_ext_mandatedPdfSigDicEntries.

#### 5.2.1.1.6.1.1 Entradas obrigatórias do Dicionário de Assinaturas:

a) Type;
b) Filter;
c) SubFilter;
d) Contents;
e) ByteRange.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em :

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do

OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Conjunto de Restrições de Algoritmos

#### 5.2.3.1 Restrições de Algoritmos para Signatários

##### 5.2.3.1.1 Restrições de Algoritmos

###### 5.2.3.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo:

a) para a versão 1.0: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

###### 5.2.3.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 2048 bits.

# 12 POLÍTICA-PADRÃO AD-RT BASEADA EM PADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIA DO TEMPO NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.12.1.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 25/08/2015.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura deve ser utilizado em aplicações ou processos de negócios nos quais a assinatura digital necessita de segurança em relação à irretratabilidade do momento de sua geração.

Como esse tipo de assinatura não traz, de forma autocontida, referências ou valores dos certificados e das informações de revogação (LCRs ou respostas OCSP) necessários para sua validação posterior, ele deve ser utilizado somente quando esses dados puderem ser obtidos por meios externos, de forma inequívoca. Uma assinatura desse tipo pode ter sua capacidade probante diminuída, no caso de comprometimento da chave da AC que emitiu qualquer um dos certificados da cadeia de certificação.

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

Esse tipo de PA é aplicável apenas em arquivos do tipo PDF.

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 25/08/2015 a 02/03/2029.

### 5.2 Regras Comuns

#### 5.2.1 Regras de Signatário e Verificador

##### 5.2.1.1 Regras do Signatário

###### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado deve ser externo à assinatura.

#### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, os seguintes atributos assinados:

a) **id-contentType**;
b) **id-messageDigest**;
c) **id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

#### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA devem conter, obrigatoriamente, o atributo não assinado **id-aa-signatureTimeStampToken**.

#### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

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

#### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: o certificado do signatário.

#### 5.2.1.1.6 Regras Adicionais do Signatário

#### 5.2.1.1.6.1 - Extensão br_ext_mandatedPdfSigDicEntries.

#### 5.2.1.1.6.1.1 - Entradas obrigatórias do Dicionário de Assinaturas:

a) Type;
b) Filter;
c) SubFilter;
d) Contents;
e) ByteRange.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

**a) id-aa-signatureTimeStampToken.**

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

##### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICPBrasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade de Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatários

##### 5.2.4.1.1 Restrições de Algoritmos

###### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo :

a) para a versão 1.0: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

###### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 2048 bits.

# 13 POLÍTICA-PADRÃO AD-RC BASEADA EM PADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.13.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS COMPLETAS NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.13.1.1.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 25/08/2015.
b) para a versão 1.1: 15/07/2016.

## 3 Nome da Entidade Emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura inclui, no seu próprio corpo, uma referência do tempo da assinatura, os certificados que compõem a cadeia de certificação e as informações de revogação do certificado digital do signatário. Além disso, será acrescentado ou logicamente conectado, sobre todo o conjunto de dados, um carimbo do tempo.

Deve ser usado em situações onde é necessária a verificação completa da validade da assinatura digital a qualquer momento, pois os dados necessários estão auto contidos na assinatura. Este tipo de assinatura demanda uma maior capacidade de armazenamento.

Além de oferecer segurança quanto à irretratabilidade, ele permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo do tempo que foi aplicado sobre todo o conjunto de dados tenha sido colocado antes desse comprometimento.

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

Esse tipo de PA é aplicável apenas em arquivos do tipo PDF.

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 25/08/2015 a 02/03/2029.
Para a versão 1.1, o período para assinatura desta PA é de 15/07/2016 a 02/03/2029.

## 5.2 Regras Comuns

### 5.2.1 Regras de Signatário e Verificador

#### 5.2.1.1 Regras do Signatário

##### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado deve ser externo à assinatura.

##### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c) **id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

##### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

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

a) **id-aa-signatureTimeStampToken.**

##### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **id-aa-signingCertificateV2** deve conter referência apenas para o certificado do signatário.

##### 5.2.1.1.5 Certificados Obrigatórios no Caminho de Certificação

Para a versão 1.0: o certificado do signatário.

##### 5.2.1.1.6 Regras Adicionais do Signatário

##### 5.2.1.1.6.1 - Extensão br_ext_mandatedPdfSigDicEntries.

##### 5.2.1.1.6.1.1 - Entradas obrigatórias do Dicionário de Assinaturas:

a) Type;
b) Filter;
c) SubFilter;
d) Contents;
e) ByteRange.

##### 5.2.1.1.6.2 Extensão br_ext_dss

##### 5.2.1.1.6.2.1 Entradas obrigatórias do campo dssDictionary

a) Type;

b) VRI;

c) Certs;

d) OCSPs ou CRLs (ValidationValues, anexo4).

#### 5.2.1.1.6.2.2 Entradas obrigatórias do campo vriDictionary

a) Type;

b) Cert;

c) OCSP ou CRL (ValidationValues, anexo4).

#### 5.2.1.1.6.3 Extensão br_ext_mandatedDocTSEntries

Entradas obrigatórios do DocumentTimestamp:

a) Type;

b) SubFilter;

c) Contents.

### 5.2.1.2 Regras do Verificador

#### 5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

**a) id-aa-signatureTimeStampToken.**

#### 5.2.1.2.2 Regras Adicionais do Verificador

##### 5.2.1.2.2.1 Extensão br_ext_dss

###### 5.2.1.2.2.1.1 Entradas obrigatórias do campo dssDictionary

a) Type;
b) VRI;
c) Certs;
d) OCSPs ou CRLs (ValidationValues, anexo4).

###### 5.2.1.2.2.1.2 Entradas obrigatórias do campo vriDictionary

a) Type;
b) Cert;
c) OCSP ou CRL (ValidationValues, anexo4).

##### 5.2.1.2.2.2 Extensão br_ext_mandatedDocTSEntries

Entradas obrigatórios do DocumentTimestamp:

a) Type;
b) SubFilter;
c) Contents.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

##### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

##### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

##### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

##### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

#### 5.2.3.2 Requisitos de Revogação

##### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

###### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

##### 5.2.3.2.2 Requisitos de Revogação para Certificados de ACs

###### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

#### 5.2.4.1 Restrições de Algoritmos para Signatário

##### 5.2.4.1.1 Restrições de Algoritmos

###### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo:

a) para a versão 1.0: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

###### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 2048 bits.

# 14 POLÍTICA-PADRÃO AD-RA BASEADA EM PADES

## 1 Identificador da Política de Assinatura

O nome desta Política de Assinatura para a versão 1.0 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.14.1.

O nome desta Política de Assinatura para a versão 1.1 é POLITICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERENCIAS PARA ARQUIVAMENTO NO FORMATO PDF, versão 1.0 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.14.1.1.

## 2 Data de Emissão

A data de emissão de cada PA é:

a) para a versão 1.0: 25/08/2015.

b) para a versão 1.1: 15/07/2016.

## 3 Nome da Entidade emissora da Política de Assinatura

A entidade emissora desta PA é identificada pelo *Distinguished Name* "C=BR, O=ICP-Brasil, OU=Instituto Nacional de Tecnologia da Informacao – ITI".

## 4 Campo de Aplicação

Este tipo de assinatura é adequado para aplicações que necessitam realizar o arquivamento do conteúdo digital assinado por longos períodos, sabendo-se que podem surgir fraquezas, vulnerabilidades ou exposição a fragilidades dos algoritmos, funções e chaves criptográficas utilizadas no processo de geração de assinatura digital.

Ele provê proteção contra fraqueza dos algoritmos, funções e tamanho de chaves criptográficas, desde que o carimbo do tempo de arquivamento seja realizado tempestivamente e utilize algoritmos, funções e tamanhos de chave considerados seguros no momento de sua geração.

Além disso, oferece segurança quanto à irretratabilidade, e permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário (desde que o carimbo do tempo sobre as referências/valores dos certificados tenha sido colocado antes desse comprometimento).

Esse tipo de PA é aplicável apenas em arquivos do tipo PDF.

## 5 Política de Validação da Assinatura

### 5.1 Período para Assinatura

Para a versão 1.0, o período para assinatura desta PA é de 25/08/2015 a 02/03/2029.
Para a versão 1.1, o período para assinatura desta PA é de 15/07/2016 a 02/03/2029.

## 5.2 Regras Comuns

### 5.2.1 Regras de Signatário e Verificador

#### 5.2.1.1 Regras do Signatário

##### 5.2.1.1.1 Dados Externos ou Internos a Assinatura

O conteúdo assinado deve ser externo à assinatura.

##### 5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

a) **id-contentType**;
b) **id-messageDigest**;
c) **id-aa-signingCertificateV2**;
d) **id-aa-ets-sigPolicyId**.

##### 5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

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

a) **id-aa-signatureTimeStampToken.**

##### 5.2.1.1.4 Certificados Obrigatoriamente Referenciados

O atributo **id-aa-signingCertificateV2** deve conter referência apenas para o certificado do signatário.

##### 5.2.1.1.5 Certificados Obrigatórios do Caminho de Certificação

Para a versão 1.0: o certificado do signatário.

##### 5.2.1.1.6 Regras Adicionais do Signatário

###### 5.2.1.1.6.1 - Extensão br_ext_mandatedPdfSigDicEntries.

###### 5.2.1.1.6.1.1 - Entradas obrigatórias do Dicionário de Assinaturas:

a) Type;
b) Filter;
c) SubFilter;
d) Contents;
e) ByteRange.

###### 5.2.1.1.6.2 Extensão br_ext_dss

###### 5.2.1.1.6.2.1 Entradas obrigatórias do campo dssDictionary

a) Type;
b) VRI;
c) Certs;

d) OCSPs ou CRLs (ValidationValues, anexo4);
e) PBAD_PolicyArtifacts;
f) PBAD_LpaArtifacts;
g) PBAD_LpaSignatures.

**5.2.1.1.6.2.2 Entradas obrigatórias do campo vriDictionary**

a) Type;
b) Cert;
c) OCSP ou CRL (ValidationValues, anexo4);
d) PBAD_PolicyArtifact;
e) PBAD_LpaArtifact;
f) PBAD_LpaSignature.

**5.2.1.1.6.3 Extensão br_ext_mandatedDocTSEntries**

Entradas obrigatórios do DocumentTimestamp:

a) Type;
b) SubFilter;
c) Contents.

**5.2.1.2 Regras do Verificador**

**5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios**

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

**a) id-aa-signatureTimeStampToken.**

**5.2.1.2.2 Regras Adicionais do Verificador**

**5.2.1.2.2.1 Extensão br_ext_dss**

**5.2.1.2.2.1.1 Entradas obrigatórias do campo dssDictionary**

a) Type;
b) VRI;
c) Certs;
d) OCSPs ou CRLs (ValidationValues, anexo4);
e) PBAD_PolicyArtifacts;
f) PBAD_LpaArtifacts;
g) PBAD_LpaSignatures.

**5.2.1.2.2.1.2 Entradas obrigatórias do campo vriDictionary**

a) Type;
b) Cert;
c) OCSP ou CRL (ValidationValues, anexo4);
d) PBAD_PolicyArtifact;
e) PBAD_LpaArtifact;
f) PBAD_LpaSignature.

#### 5.2.1.2.2.2 Extensão br_ext_mandatedDocTSEntries

Entradas obrigatórios do DocumentTimestamp:

a) Type;
b) SubFilter;
c) Contents.

### 5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

#### 5.2.2.1 Requisitos de Certificados

#### 5.2.2.1.1 Raiz Confiável

A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.2.1.2 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada ao certificado ICP-Brasil tipo A1 (do OID 2.16.76.1.2.1.1 ao OID 2.16.76.1.2.1.100), tipo A2 (do OID 2.16.76.1.2.2.1 ao OID 2.16.76.1.2.2.100), do tipo A3 (do OID 2.16.76.1.2.3.1 ao OID 2.16.76.1.2.3.100) e do tipo A4 (do OID 2.16.76.1.2.4.1 ao OID 2.16.76.1.2.4.100), conforme definido em DOC-ICP-04.

#### 5.2.2.2 Requisitos de Revogação

#### 5.2.2.2.1 Requisitos de Revogação para Certificados Finais

#### 5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.2.2.2 Requisitos de Revogação para Certificados de ACs

#### 5.2.2.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.3 Condições de Confiabilidade do Carimbo do Tempo

#### 5.2.3.1 Requisitos de Certificados

#### 5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo do tempo deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em:

a) para a versão 1.0:
http://acraiz.icpbrasil.gov.br/ICP-Brasilv2.crt e
http://acraiz.icpbrasil.gov.br/ICP-Brasilv5.crt.

#### 5.2.3.1.2 Conjunto de Políticas de Certificado Aceitável

Os carimbos do tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (do OID é 2.16.76.1.2.303.1 ao OID 2.16.76.1.2.303.100 ) ou T4 (do OID é 2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

### 5.2.3.2 Requisitos de Revogação

#### 5.2.3.2.1 Requisitos de Revogação para Certificados Finais

##### 5.2.3.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

#### 5.2.3.2.2Requisitos de Revogação para Certificados de ACs

##### 5.2.3.2.2.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

### 5.2.4 Conjunto de Restrições de Algoritmos

### 5.2.4.1 Restrições de Algoritmos para Signatário

#### 5.2.4.1.1 Restrições de Algoritmos

##### 5.2.4.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo:

a) para a versão 1.0: sha256WithRSAEncryption(1.2.840.113549.1.1.11) ou sha512WithRSAEncryption(1.2.840.113549.1.1.13).

##### 5.2.4.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de :

a) para a versão 1.0: 2048 bits.

# ANEXO 3

## GERENCIAMENTO DE POLÍTICAS DE ASSINATURA NA ICP-BRASIL

## 1 INTRODUÇÃO

1.1 Na verificação da validade de uma Assinatura Digital ICP-Brasil diversos atributos e propriedades devem ser checados. É preciso verificar, por exemplo, se a assinatura contém apenas algoritmos e parâmetros permitidos pelas normas da ICP-Brasil.

1.2 Além disso, é necessário validar também se a assinatura foi criada com a utilização de uma Política de Assinatura (PA) aprovada pela AC Raiz da ICP-Brasil.

1.3 O objetivo do presente documento é introduzir regras claras e transparentes para determinar a validade das PAs aprovadas e definir processos de prorrogação e revogação de uma PA.

1.4 Para facilitar a verificação da validade de uma PA aprovada e para permitir a criação de sistemas que decidam de forma automatizada se uma determinada PA foi aprovada, a AC Raiz, além de publicá-la em seu repositório web, gera e assina digitalmente uma Lista de Políticas de Assinatura Aprovadas (LPA), contendo dados que identificam uma PA.

1.5 O formato da LPA e a forma de utilizá-la estão definidos no presente documento, bem como os procedimentos de administração de PAs aprovadas, o que inclui: a forma de publicação das PAs e os procedimentos a serem adotados em caso de término da validade, prorrogação da validade e revogação de PAs aprovadas.

## 2 ADMINISTRAÇÃO E CICLO DE VIDA DE UMA PA

2.1 PAs aprovadas são gerenciadas pela AC Raiz da ICP-Brasil com base neste documento.

2.2 Uma Política de Assinatura passa pelas seguintes etapas de vida:

a) criação;
b) aprovação;
c) publicação;
d) expiração (se for o caso);
e) prorrogação de validade (se for o caso);
f) revogação (se for o caso).

## 3 APROVAÇÃO DE UMA PA

As PAs aprovadas pela AC-Raiz devem ser submetidas a avaliação prévia do CG-ICP-Brasil.

## 4. PUBLICAÇÃO DA PA E DA LPA

4.1 Os arquivos com as PAs aprovadas são publicados no repositório da AC Raiz da ICP-Brasil e são utilizados para a criação da LPA.

4.2 As LPAs são assinadas e publicadas pela AC Raiz da ICP-Brasil, de forma segura, no seu repositório no seguinte endereço web:

http://www.iti.gov.br/component/content/article/190-repositorio/artefatos-de-assinatura-digital/4725-lpa

4.3 As LPAs são atualizadas pela AC Raiz pelo prazo **máximo de 90 dias** e contêm em seus corpos a data da sua próxima atualização.

4.4 As LPAs são assinadas com Assinaturas Digitais ICP-Brasil, utilizando PKCS #7 para CAdES e PAdES e XMLDSig para XAdES, todas assinadas por um certificado de pessoa jurídica do ITI, emitido por uma das autoridades certificadoras credenciadas na ICP-Brasil.

4.5 As LPAs são codificadas em linguagem de máquina (ASN.1 e XML) e trazem, para cada PA aprovada, os seguintes dados:

a) período de validade da Política;
b) data de revogação, se for o caso;
c) URLs da PA em formato processável por máquina (XML/DER);
d) resumos criptográficos dos arquivos da PA, processável por máquina (XML/DER);
e) assinatura digital PKCS #7 para o formato ASN.1 e XMLdSIG para o formato XML;
f) Identificador da política de assinatura;

4.6 PAs aprovadas são válidas pelo período indicado no campo de período para assinatura se ela não tiver sido revogada.

## 5 PRORROGAÇÃO DA VALIDADE DE UMA PA APROVADA

5.1 A validade de uma PA pode ser prorrogada desde que não tenham sido encontradas fragilidades na PA, as quais não sejam tecnicamente aceitáveis para o novo período de validade.

5.2 A prorrogação feita por meio da publicação de uma nova versão da PA contendo os dados alterados sobre data de publicação, começo e término da validade da PA. A publicação é feita utilizando os procedimentos citados no capítulo anterior.

## 6 REVOGAÇÃO DE UMA PA

6.1 PAs aprovadas PODEM ser revogadas pela AC Raiz da ICP-Brasil a qualquer tempo, a partir da emissão de uma nova LPA na qual o campo "data de revogação", relativo àquela PA esteja atualizado com a data da emissão da LPA.

## 7 PROCEDIMENTOS PARA CRIAÇÃO E VERIFICAÇÃO DA LPA

7.1 A estrutura do arquivo LPA é a seguinte:

a) identificador da política de assinatura;
b) campo **PERÍODO PARA ASSINATURA**: contém a datas de início e de final do período de validade da PA;
c) campo **DATA DE REVOGAÇÃO**: contém a data de revogação da PA, se for o caso;
d) campo **URL MÁQUINA**: contém a URL do repositório da AC Raiz da ICP-Brasil em que está publicada a PA aprovada, em formato DER ou XML;
e) campo **RESUMO CRIPTOGRÁFICO MÁQUINA**: contém o resumo criptográfico da PA codificada em DER ou XML;

f) assinatura digital PKCS #7 para o formato ASN.1 e XMLDSig para o formato XML.

7.2 A LPA contém as PAs aprovadas vigentes, expiradas e revogadas, característica esta necessária à verificação de Assinaturas Digitais ICP-Brasil criadas no passado por meio de PAs aprovadas que tenham sido válidas por um período, mas que posteriormente tenham expirado ou sido revogadas.

7.3 A LPA DEVE ser verificada em relação ao momento atual, validando-se a assinatura da LPA assim como o certificado do signatário da LPA.

7.4 Codificação de especificações da LPA:

**7.4.1 ASN.1**

7.4.1.1 LPA versão 1

```
ListaDePAsAprovadas
    { joint(2) country(16) br(76) iti(1) lpa(9) }
--CryptographicMessageSyntax2004
--    { iso(1) member-body(2) us(840) rsadsi(113549)
--      pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Estrutura principal
LPA ::= SEQUENCE {
          policyInfos PolicyInfos,
          nextUpdate Time }

Time ::= CHOICE {
  utcTime UTCTime,
  generalTime GeneralizedTime }

PolicyInfos ::= SEQUENCE OF PolicyInfo

PolicyInfo ::= SEQUENCE {
    policyName        DirectoryString,
    fieldOfApplication DirectoryString,
    signingPeriod     SigningPeriod,
    revocationDate    Time OPTIONAL,
    policiesURI       PoliciesURI,
    policiesDigest    PoliciesDigest }


-- Periodo para Assinatura
SigningPeriod ::= SEQUENCE {
    notBefore GeneralizedTime,
    notAfter  GeneralizedTime OPTIONAL }

-- URLs da PA
PoliciesURI ::= SEQUENCE {
```

```
    textualPolicyURI [0] IA5String,
    asn1PolicyURI    [1] IA5String OPTIONAL,
    xmlPolicyURI     [2] IA5String OPTIONAL }

-- Resumos Criptograficos
PoliciesDigest ::= SEQUENCE {
    textualPolicyDigest [0] OtherHashAlgAndValue,
    asn1PolicyDigest    [1] OtherHashAlgAndValue OPTIONAL,
    xmlPolicyDigest     [2] OtherHashAlgAndValue OPTIONAL }

OtherHashAlgAndValue ::= SEQUENCE {
    hashAlgorithm   AlgorithmIdentifier,
    hashValue       OtherHashValue }

OtherHashValue ::= OCTET STRING

DirectoryString ::= CHOICE {
     teletexString       TeletexString   (SIZE (1..MAX)),
     printableString     PrintableString (SIZE (1..MAX)),
     universalString     UniversalString (SIZE (1..MAX)),
     utf8String          UTF8String      (SIZE (1..MAX)),
     bmpString           BMPString       (SIZE (1..MAX)) }

AlgorithmIdentifier  ::=  SEQUENCE  {
    algorithm             OBJECT IDENTIFIER,
    parameters             ANY DEFINED BY algorithm OPTIONAL  }
                       -- contains a value of the type
                       -- registered for use with the
                       -- algorithm object identifier value

END
```

7.4.1.2 LPA versão 2

```
ListaDePAsAprovadasV2
        { joint(2) country(16) br(76) iti(1) lpa(9) v2(1) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

        IMPORTS
                -- Electronic Signature Formats for long term electronic signatures: RFC 3126
                OtherHashAlgAndValue
                FROM  ETS-ElectronicSignatureFormats-88syntax  {  iso(1)  member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) 5}
                -- Electronic Signature Policies: RFC 3125
                SigningPeriod
                FROM  ETS-ElectronicSignaturePolicies-88syntax  {  iso(1)  member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) 7};
```

```
-- Estrutura principal
LPA ::= SEQUENCE {
        version         Version DEFAULT v2,
        policyInfos     PolicyInfos,
        nextUpdate      GenerelizedTime }

Version  ::=  INTEGER  {  v2(0) }

PolicyInfos ::= SEQUENCE OF PolicyInfo

PolicyInfo ::= SEQUENCE {
    signingPeriod     SigningPeriod,
    revocationDate    GeneralizedTime OPTIONAL,
    policyOID         OBJECT IDENTIFIER,
    policyURI         IA5String,
    policyDigest      OtherHashAlgAndValue }

END
```

### 7.4.2 XML

7.4.2.1 LPA versão 1

```
<?xml version="1.0" encoding="UTF-8"?>
        <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.iti.gov.br/LPA#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://www.iti.gov.br/LPA#" elementFormDefault="qualified">

        <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>

        <!-- Lista  de Politicas de Assinatura Aprovadas -->
        <xsd:element name="ApprovedSignaturePoliciesList"
type="ApprovedSignaturePoliciesListType" />
      <xsd:complexType name="ApprovedSignaturePoliciesListType">
          <xsd:sequence>
              <xsd:element name="NextUpdate" type="xsd:date" />
                  <xsd:element  name="PolicyInfo"  type="PolicyInfoType"
maxOccurs="unbounded"/>
          </xsd:sequence>
      </xsd:complexType>

        <!-- Informacoes da Politica -->
        <xsd:complexType name="PolicyInfoType">
              <xsd:sequence>
                  <xsd:element name="PolicyName" type="xsd:string" />
                  <xsd:element name="FieldOfApplication" type="xsd:string" />
                  <xsd:element name="SigningPeriod" type="SigningPeriodType" />
```

```
                        <xsd:element minOccurs="0" name="RevocationDate"
type="xsd:date" />
                        <xsd:element name="TextualPolicyDigestAndURI"
type="PolicyDigestAndURIType" />
                        <xsd:element minOccurs="0" name="XMLPolicyDigestAndURI"
type="PolicyDigestAndURIType" />
                </xsd:sequence>
        </xsd:complexType>

        <!-- Periodo para Assinatura -->
        <xsd:complexType name="SigningPeriodType">
                <xsd:sequence>
                        <xsd:element name="NotBefore" type="xsd:date" />
                        <xsd:element minOccurs="0" name="NotAfter" type="xsd:date" />
                </xsd:sequence>
        </xsd:complexType>

        <!-- Resumos Criptograficos e URLs da PA -->
        <xsd:complexType name="PolicyDigestAndURIType">
                <xsd:sequence>
                        <xsd:element name="PolicyURI" type="xsd:anyURI" />
                        <xsd:element name="PolicyDigest" type="DigestType" />
                </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="DigestType">
                <xsd:sequence>
                        <xsd:element name="DigestMethod" type="ds:DigestMethodType" />
                        <xsd:element name="DigestValue" type="ds:DigestValueType" />
                </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

7.4.2.2 LPA versão 2

```
<xsd:schema targetNamespace="http://www.iti.gov.br/LPA/v2#"
elementFormDefault="qualified">
        <xsd:import namespace="http://uri.etsi.org/01903/v1.3.2#"
        schemaLocation="http://uri.etsi.org/01903/v1.3.2/XAdES.xsd"/>
        <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
        <!-- Lista de Politicas de Assinatura Aprovadas -->
        <xsd:element name="ApprovedSignaturePoliciesList"
        type="ApprovedSignaturePoliciesListType"/>
        <xsd:complexType name="ApprovedSignaturePoliciesListType">
                <xsd:sequence>
                <xsd:element name="Version" type="xsd:integer" default="0"/>
                <xsd:element name="NextUpdate" type="xsd:dateTime"/>
```

```
                <xsd:element name="PolicyInfo" type="PolicyInfoType"
                maxOccurs="unbounded"/>
                </xsd:sequence>
        </xsd:complexType>
        <!-- Informacoes da Politica -->
        <xsd:complexType name="PolicyInfoType">
                <xsd:sequence><xsd:element name="SigningPeriod"
                type="SigningPeriodType"/>
                <xsd:element minOccurs="0" name="RevocationDate" type="xsd:dateTime"/>
                <xsd:element name="policyOID" type="XAdES:ObjectIdentifierType"/>
                <xsd:element name="PolicyDigestAndURI"
                type="PolicyDigestAndURIType"/>
                </xsd:sequence></xsd:complexType>
        <!-- Periodo para Assinatura -->
        <xsd:complexType name="SigningPeriodType">
                <xsd:sequence>
                <xsd:element name="NotBefore" type="xsd:dateTime"/>
                <xsd:element minOccurs="0" name="NotAfter" type="xsd:dateTime"/>
                </xsd:sequence></xsd:complexType>
        <!-- Resumos Criptograficos e URLs da PA -->
        <xsd:complexType name="PolicyDigestAndURIType">
                <xsd:sequence>
                <xsd:element name="PolicyURI" type="xsd:anyURI"/>
                <xsd:element name="PolicyDigest" type="DigestType"/>
                </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="DigestType">
                <xsd:sequence><xsd:element name="DigestMethod"
                type="ds:DigestMethodType"/>
                <xsd:element name="DigestValue" type="ds:DigestValueType"/>
                </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

# ANEXO 4

## EXTENSÕES DE POLÍTICAS DE ASSINATURA PARA PAdES

## 1 INTRODUÇÃO

Para que a estrutura das PAs, descrita em [1], consiga apontar os campos da estrutura do PDF é necessário expandir essa estrutura. Essa expansão é feita através da descrição de novas extensões de PA, conforme o item 6.11 de [1]. Essas extensões servirão como guia de implementação dos dicionários PDF utilizados para criar uma assinatura PAdES.

Estas extensões deverão ser adicionadas no campo de extensões (*signPolExtensions*) das regras do signatário (item 6.5.1 de [1]) e no campo de extensões (*signPolExtensions*) das regras do verificador (item 6.5.2 de [1]).

## 2 EXTENSÕES

### 2.1 – DICIONÁRIO DE ASSINATURA

Essa extensão tem função similar à tabela de atributos assinados obrigatórios. Nela constarão todas as entradas obrigatórias e, opcionalmente, seu valor que deverá constar na assinatura.

#### 2.1.1 – SINTAXE ASN.1

```
br-ext-mandatedPdfSigDicEntries   OBJECT IDENTIFIER ::= { 2.16.76.1.8.1 }

MandatedPdfSigDicEntries ::= SEQUENCE OF PdfEntry

PdfEntry   ::= SEQUENCE {
   id          UTF8String (SIZE (1..MAX)),
   value     OCTET STRING OPTIONAL -- contém a codificação DER do conteúdo obrigatório
da entrada
}
```

O campo MandatedPdfSigDicEntries representa a lista de entradas obrigatórias que uma assinatura deverá ter no dicionário de assinaturas. Esse campo é formado por uma lista de entradas PDF, representadas pela estrutura PdfEntry. O PdfEntry, por sua vez, traz o nome da entrada PDF que deverá constar no dicionário e, opcionalmente, o valor que deverá ser empregado nessa entrada. Tal valor será codificado em DER de acordo com o tipo da entrada identificada por "id". A tabela A.4.3 apresenta as entradas obrigatórias e a formatação do valor.

### 2.2 – DICIONÁRIO *DOCUMENT SECURITY STORE* (DSS)

Quando esta extensão estiver presente, ela indicará que o DSS DEVE ser codificado na assinatura. As entradas indicadas por essa extensão serão consideradas obrigatórias.

### 2.2.1 – SINTAXE ASN.1

```
br-ext-dss   OBJECT IDENTIFIER ::= { 2.16.76.1.8.2 }

  DssDictionary ::= SEQUENCE{

  mandatedEntries     SEQUENCE OF PdfEntry,

  vriMandatedEntries  SEQUENCE OF PdfEntry OPTIONAL
}
```

O campo DssDictionary representa o dicionário DSS, descrito em ETSI PAdES-LTV [9]. Esse campo é formado por uma lista de entradas obrigatórias no dicionário DSS e pelo campo vriDictionary, que é a indicação do uso do dicionário *Validation Related Information* (VRI) [9].

O campo VriDictionary apresenta quais entradas do dicionário VRI são obrigatórias para cada assinatura que usá-lo.

## 2.3 – DICIONÁRIO *DOCUMENT TIME-STAMP*

Define os campos obrigatórios do carimbo do tempo do documento, que é inserido como uma assinatura a parte no PDF. As entradas presentes nessa extensão são obrigatórias.

### 2.3.1 – SINTAXE ASN.1

```
br-ext-mandatedDocTSEntries  OBJECT IDENTIFIER ::= { 2.16.76.1.8.3 }

MandatedDocTSEntries  ::= SEQUENCE OF PdfEntry
```

O campo mandatedDocTSEntries apresenta uma lista de entradas para o dicionário do carimbo do tempo do documento, ou *Document Timestamp*, que é um dicionário similar ao dicionário de assinaturas, mas a entrada *Contents* possui um carimbo do tempo ao invés de uma assinatura tradicional.

## 2.4 – Artefatos de PA e LPA na estrutura PDF

A indicação da codificação dos artefatos de políticas de assinatura (PA, LPA e assinatura da LPA) será formada por 3 entradas no *Document Time-stamp*. Essas entradas funcionarão de forma parecida com a codificação dos certificados, LCRs e OCSPs presentes no DSS. Ou seja, serão referências indiretas aos respectivos objetos codificados em BER.

| ENTRADA | TIPO | VALOR |
|---|---|---|
| PBAD_PolicyArtifacts | Referência | Uma referência para o objeto PDF que contém as PAs codificadas em BER. Essa entrada contém as políticas de assinatura que devem ser usadas para a validação das assinaturas contidas no documento PDF |
| PBAD_LpaArtifacts | Referência | Uma referência para o objeto PDF que contém as LPAs codificadas em BER. Essa entrada contém as LPAs que devem ser usadas para validar as políticas de assinatura usadas nas assinaturas contidas no documento PDF |
| PBAD_LpaSignatures | Referência | Uma referência para o objeto PDF que contém as assinaturas das LPAs. |

Tabela A.4.1 – Entradas adicionais do dicionário *Document Security Store*.

A Tabela A.4.1 descreve as entradas a serem adicionadas ao DSS, descrito em [9]. Essas entradas guardam todos os dados necessários para validar uma política de assinatura localmente. A entrada PBAD_PolicyArtifcats e PBAD_LpaArtifacts são arrays de objetos indiretos (ver ISO 32000-1) contendo todas as PAs e LPAs, respectivamente, utilizadas no documento PDF assinado no padrão PAdES. A entrada PBAD_LpaSignatures é um array de objetos indiretos contendo as assinaturas das LPAs incluídas na entrada PBAD_LpaArtifacts.

| ENTRADA | TIPO | VALOR |
|---|---|---|
| PBAD_PolicyArtifact | Referência | Uma referência para o objeto PDF que contém uma PA codificada em BER. Essa entrada contém a política de assinatura que deve ser usada para a validação da assinatura |
| PBAD_LpaArtifact | Referência | Uma referência para o objeto PDF que contém uma LPA codificada em BER. Essa entrada contém a LPA que deve ser usada para validar a política de assinatura usada na assinatura |
| PBAD_LpaSignature | Referência | Uma referência para o objeto PDF que contém a assinatura da LPA. |

Tabela A.4.2 – Entradas adicionais do dicionário VRI.

A Tabela A.4.2 descreve as entradas a serem adicionadas no dicionário VRI, descrito em ETSI PAdES-LTV [9]. Essas entradas adicionais servem para indicar qual PA e qual LPA devem ser utilizadas na validação da assinatura à qual determinado VRI faz referência. A entrada PaArtifact deve conter um objeto indireto à PA utilizada para realizar a assinatura. A entrada LpaArtifact deve conter um objeto indireto à LPA vigente durante o período de realização da assinatura. A entrada LpaSignature deve conter a assinatura da LPA.

### 2.5 - Relação dos tipos de PdfEntry

Definição em ASN.1 dos valores de cada tipo de entrada de dicionário. As entradas não descritas aqui não possuem um valor fixo aplicável, portanto, dispensa a codificação de um valor. Sua presença indica sua obrigatoriedade.

| Entrada (id) | Sintaxe ASN.1 (value) |
|---|---|
| Type | UTF8String (SIZE (1..MAX)) |
| Filter | UTF8String (SIZE (1..MAX)) |
| SubFilter | UTF8String (SIZE (1..MAX)) |
| ValidationValues | ValidationReq |

Tabela A.4.3 - Sintaxe ASN.1 por tipos de entradas.

A entrada de dicionário *ValidationValues*, não reflete a uma entrada do DSS ou VRI de fato, mas indica qual tipo de artefato de revogação deve ser incluido nessas estruturas. Essa estrutura pode indicar se um DSS ou VRI deve conter apenas LCR, apenas OCSP, qualquer um dos dois ou obrigatoriamente os dois.

```
ValidationReq ::= ENUMERATED {
    crlsOnly (0), -- indica que apenas a entrada CRLs/CRL pode ser usada
    ocspsOnly (1), -- indica que apenas a entrada OCSPs/OCSP pode ser usada
    either (2), -- indica que podem ser usadas LCRs/LCR ou OCSPs/OCSP no DSS/VRI
    both (3) -- indica que devem ser usadas LCRs/LCR e OCSPs/OCSP no DSS/VRI
}
```