Infraestrutura de Chaves Públicas Brasileira

REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL

DOC-ICP-15.03

Versão 6.1

19 de setembro de 2012

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Instrução Normativa Nº 11, de 19.9.2012 (Versão 6.1)		
Instrução Normativa Nº 10, de 5.7.2012 (Versão 6.0)	Anexo 1, item 1; Anexo 2, capítulos 5, 6, 7, 8, 9 e 10 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 Inclui as Notas 1 a 4 no Item 1 do Anexo 1.	Geradas novas políticas de assinatura versão 2.1 para XadES. 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 Anexo 2 - Todas as políticas CAdES Item 5.2.1.1.2	Corrigido atributo assinado obrigatório id-aa-signingCertificateV2 para a versão 2.0. 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. Retirados todos os itens assinalados como “não se aplica”.
	Anexo 1, Tabelas A2 a A13	Corrigido as propriedades XadES citadas incorretamente; Corrigido o título da coluna central das Tabelas; Alterado o campo carimbo do tempo na política AD-RB de opcional para “não deve”; Retirado a obrigatoriedade do uso dos atributos referentes à certificado de atributo; Corrigido os termos referentes à timestamp nas tabelas.
	Anexo 2, Todas as políticas.	Inclusão da versão 2.0 que implementa a cadeia V2 da AC Raiz para todas as políticas de assinatura ICP-Brasil.

Resolução que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
	Item 5.2.1.1.5	Obrigatoriedade de manter o certificado do signatário no caminho de certificação.
	Anexo 3, item 4.2	Corrigido endereço do repositório de publicação da LPA.
	Item 7.4	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.

1 INTRODUÇÃO

1.1 Este documento estabelece os requisitos a serem obrigatoriamente observados pelas entidades criadoras de Políticas de Assinatura Digital no âmbito da Infra-Estrutura 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 co-assinaturas) ou a criação de assinaturas digitais em série (também conhecidas como contra-assinaturas).

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 *Extensible 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 10 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 lista as Políticas de Assinatura Padrão da ICP-Brasil baseadas em CMS *Advanced Electronic Signatures* (CAdES) e em XML-DSig *Advanced Electronic Signatures* (XAdES). O Anexo 3 descreve o processo de gerenciamento de PAs na ICP-Brasil.

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)

2.1.1 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)

2.4.1 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)

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

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 auto-assinado 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 numero máximo de certificados de Autoridade Certificadora (AC)

abaixo da âncora de confiança do caminho de certificação do signatário. No caso da ICP-Brasil, este numero e, 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 e 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 e 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 a 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 auto-assinado 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.

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.

ANEXO 1

1 POLÍTICAS DE ASSINATURA-PADRÃO ICP-BRASIL

Para facilitar a utilização de Políticas de Assinatura pelos usuários finais, o ITI criou 10 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) e XML-DSig *Advanced Electronic Signature* (XAdES), citados no documento DOC-ICP-15.01, a saber:

a) Assinatura Digital com Referência Básica (AD-RB);
b) Assinatura Digital com Referência do Tempo (AD-RT);
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 11 têm-se as 10 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, utilizada 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.

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]** **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 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**	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"

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
	t					
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**	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".

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 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**	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"

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 v1 (*ESS signing certificate*)	**id-aa-signingCertificate**	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"

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"

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, versao 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, versao 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, versao 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, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.1.2. 1.

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.

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 21/06/2023.

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 e 2.1: 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

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).

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;
b) para as versões 2.0 e 2.1: 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, versao 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, versao 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, versao 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, versao 2.1 e o seu *Object Identifier* (OID) é 2.16.76.1.7.1.2.2.1.

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.

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 auto-contida, 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.

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 **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 e 2.1: 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

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

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).

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 e 2.1: 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.

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.

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.

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 e 2.1: 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

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

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).

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 e 2.1: 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.

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.

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 auto-contidos 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.

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 e 2.1: 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

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

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).

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 e 2.1: 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.

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.

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.

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 e 2.2 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 e 2.2:
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 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:

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 e 2.2:
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

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

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).

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 e 2.2: 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.

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.

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.

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 e 2.2:
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 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 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

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

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 e 2.1: 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.

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.

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 auto-contida, 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.

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 e 2.2:
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 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 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

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

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

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 e 2.2: 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.

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.

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.

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 e 2.2:
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 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 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

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

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

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 e 2.2: 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.

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.

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 auto-contidos 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.

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 e 2.2:

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 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 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

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

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

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 e 2.2: 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.

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.

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.

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 e 2.2:
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 e 2.2:
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 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 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 e 2.2:
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

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

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

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 e 2.2: 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 resumidos sobre a 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 previa 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 endereço web http://www.iti.gov.br/twiki/bin/view/Certificacao/artefatos.

4.3 As LPAs são atualizadas pela AC Raiz **a cada 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 XMLdSIG para XAdES, ambos assinados 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) nome;
b) uma breve descrição da política: os aplicativos assinadores poderão exibir essa informação para que o usuário decida qual PA empregar;
c) período de validade da Política;
d) data de revogação, se for o caso;
e) URLs da PA em formato textual e processável por máquina (XML/DER);
f) resumos criptográficos dos arquivos da PA, no formato textual e processável por máquina (XML/DER);
g) assinatura digital PKCS #7 para o formato ASN.1 e XMLdSIG para o formato XML.

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) campo **NOME**: contém o nome da PA, conforme definido no item 4.1.1.b;
b) campo **APLICACAO:** descreve as situações em que a PA pode ser empregada, conforme conteúdo constante no campo *CAMPO DE APLICAÇÃO*, existente no corpo da PA;
c) campo **PERÍODO PARA ASSINATURA**: contém a datas de início e de final do período de validade da PA;
d) campo **DATA DE REVOGAÇÃO**: contém a data de revogação da PA, se for o caso;
e) campo **URL TEXTUAL**: contém a URL do repositório da AC Raiz da ICP-Brasil em que está publicada a PA aprovada, em formato textual;
f) 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;
g) campo **RESUMO CRIPTOGRÁFICO TEXTUAL**: contém o resumo criptográfico da PA em formato textual;
h) campo **RESUMO CRIPTOGRÁFICO MÁQUINA**: contém o resumo criptográfico da PA codificada em DER ou XML;
i) assinatura digital PKCS #7 para o formato ASN.1 e XMLdSIG para o formato XML.

7.2 A LPA contém as PAs aprovadas, 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

```
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

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**

```
<?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>


<xsd:schema targetNamespace="http://www.iti.gov.br/LPA/v2#"
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="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:ObjectIdentiferType"/>
                <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>
```