



Infraestrutura de Chaves Públicas Brasileira

REQUISITOS DAS POLÍTICAS DE ASSINATURA

DIGITAL NA ICP-BRASIL

DOC-ICP-15.03

Versão 2.0

05 de abril de 2010

SUMÁRIO

SUMÁRIO.....	2
1 INTRODUÇÃO.....	3
2 CONTEÚDO GERAL DE uma POLÍTICA DE ASSINATURA.....	5
BIBLIOGRAFIA.....	15
ANEXO 1.....	16
1 POLÍTICAS DE ASSINATURA-PADRÃO ICP-BRASIL.....	16
ANEXO 2.....	29
1 POLÍTICA-PADRÃO AD-RB BASEADA EM CADES.....	29
2 POLÍTICA-PADRÃO AD-RT BASEADA EM CADES.....	34
3 POLÍTICA-PADRÃO AD-RV BASEADA EM CADES.....	40
4 POLÍTICA-PADRÃO AD-RC BASEADA EM CADES.....	46
5 POLÍTICA-PADRÃO AD-RA BASEADA EM CADES.....	52
6 POLÍTICA-PADRÃO AD-RB BASEADA EM XADES.....	58
7 POLÍTICA-PADRÃO AD-RT BASEADA EM XADES.....	63
8 POLÍTICA-PADRÃO AD-RV BASEADA EM XADES.....	69
9 POLÍTICA-PADRÃO AD-RC BASEADA EM XADES.....	75
10 POLÍTICA-PADRÃO AD-RA BASEADA EM XADES.....	81
ANEXO 3.....	88
GERENCIAMENTO DE POLÍTICAS DE ASSINATURA NA ICP-BRASIL	88
1 INTRODUÇÃO.....	88
2 ADMINISTRAÇÃO E CICLO DE VIDA DE UMA PA.....	88
3 APROVAÇÃO DE UMA PA.....	88
4. PUBLICAÇÃO DA PA E DA LPA.....	89
5 PRORROGAÇÃO DA VALIDADE DE UMA PA APROVADA.....	89
6 REVOGAÇÃO DE UMA PA.....	89
7 PROCEDIMENTOS PARA CRIAÇÃO E VERIFICAÇÃO DA LPA.....	90



Infraestrutura de Chaves Públicas Brasileira

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.



Infraestrutura de Chaves Públicas Brasileira

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* (CAeS) e em *XML-DSig Advanced Electronic Signatures* (XAeS). O Anexo 3 descreve o processo de gerenciamento de PAs na ICP-Brasil.

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)



Infraestrutura de Chaves Públicas Brasileira

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.



Infraestrutura de Chaves Públicas Brasileira

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

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

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

2.5.2.2.1.4 Restrições de Nome (6.6.1, 8.8.2)

Neste item PODEM constar as restrições de nomes aplicáveis.

2.5.2.2.1.5 Restrições de Políticas de Certificação (6.6.1, 8.8.2)

Nota: item opcional.

2.5.2.2.1.5.1 Necessidade da Identificação de Políticas (6.6.1, 8.8.2)

Neste item PODE ser definido a partir de qual nível do caminho de certificação 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.

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

2.5.2.3.1.3 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-



Infraestrutura de Chaves Públicas Brasileira

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 algoritmos 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.



Infraestrutura de Chaves Públicas Brasileira

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.



Infraestrutura de Chaves Públicas Brasileira

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* (CAeS) e XML-DSig *Advanced Electronic Signature* (XAeS), 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.

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Tipo de conteúdo (<i>content type</i>)	id-contentType	O	O	O	O	O
	ContentType					
Resumo criptográfico da mensagem (<i>message digest</i>)	id-messageDigest	O	O	O	O	O
	MessageDigest					
Certificado do signatário v1 (<i>ESS signing certificate</i>)	id-aa-signingCertificate	O	O	O	O	O
	SigningCertificate					
Identificador da política de assinatura (<i>signature policy identifier</i>)	id-aa-ets-sigPolicyId	O	O	O	O	O
	SignaturePolicyIdentifier					
Atributos do signatário (<i>signer attributes</i>)	id-aa-ets-signerAttr	P	P	P	P	P
	SignerAttribute					
Instante da assinatura (<i>signing time</i>)	id-signingTime	P	P	P	P	P
	SigningTime					
Localização do signatário (<i>signer location</i>)	id-aa-ets-signerLocation	P	P	P	P	P
	SignerLocation					
Carimbo do tempo de conteúdo (<i>content time stamp</i>)	id-aa-ets-contentTimeStamp	P	P	P	P	P
	ContentTimeStamp					

Tabela A.2 – Atributos assinados no SignerInfo do Assinante

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Contra assinatura (<i>countersignature</i>)	id-countersignature	P	P	P	P	P
	CounterSignature					
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	P	O	O	O	O
	SignatureTimeStampToken					
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	P	P	O	O	O
	CompleteCertificateRefs					
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	P	P	O	O	O
	CompleteRevocationRefs					
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	P	P	O	O	O
	AttributeCertificateRefs					
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	P	P	O	O	O
	AttributeRevocationRefs					
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	P	P	O	O	P
	TimestampedCertsCRLs					
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	P	P	P	O	O
	CertificateValues					
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	P	P	P	O	O
	RevocationValues					
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND	ND	ND	O
	ArchiveTimeStampToken					

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

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

Tabela A.4: Presença de atributos assinados no SignerInfo de “contra assinatura”

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	CT	RV	RC	RA
Contra assinatura (<i>countersignature</i>)	id-countersignature	P	P	P	P	P
	CounterSignature					
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	P	O	O	O	O
	SignatureTimeStampToken					
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	P	P	O	O	O
	CompleteCertificateRefs					
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	P	P	O	O	O
	CompleteRevocationRefs					
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	P	P	O	O	O
	AttributeCertificateRefs					
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	P	P	O	O	O
	AttributeRevocationRefs					
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	P	P	O	O	O
	TimestampedCertsCRLs					
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	P	P	P	O	O
	CertificateValues					
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	P	P	P	O	O
	RevocationValues					
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND	ND	ND	ND
	ArchiveTimeStampToken					

Tabela A.5: Presença de atributos não-assinados no SignerInfo de “contra assinatura”

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Tipo de conteúdo (<i>content type</i>)	id-contentType	O	O	O	O	O
	ContentType					
Resumo criptográfico da mensagem (<i>message digest</i>)	id-messageDigest	O	O	O	O	O
	MessageDigest					
Certificado do signatário v1 (<i>ESS signing certificate</i>)	id-aa-signingCertificate	O	O	O	O	O
	SigningCertificate					
Identificador da política de assinatura (<i>signature policy identifier</i>)	id-aa-ets-sigPolicyId	ND	ND	ND	ND	ND
	SignaturePolicyIdentifier					
Atributos do signatário (<i>signer attributes</i>)	id-aa-ets-signerAttr	ND	ND	ND	ND	ND
	SignerAttribute					
Instante da assinatura (<i>signing time</i>)	id-signingTime	ND	ND	ND	ND	ND
	SigningTime					
Localização do signatário (<i>signer location</i>)	id-aa-ets-signerLocation	ND	ND	ND	ND	ND
	SignerLocation					
Carimbo do tempo de conteúdo (<i>content time stamp</i>)	id-aa-ets-contentTimeStamp	ND	ND	ND	ND	ND
	ContentTimeStamp					

Tabela A.6: Presença de atributos assinados no TimeStampToken de “carimbo do tempo de conteúdo”

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Contra assinatura (<i>countersignature</i>)	id-countersignature	ND	ND	ND	ND	ND
	CounterSignature					
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	ND	ND	ND	ND	ND
	SignatureTimeStampToken					
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	R*	R*	O*	O*	O*
	CompleteCertificateRefs					
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	R*	R*	O*	O*	O*
	CompleteRevocationRefs					
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	ND	ND	ND	ND	ND
	AttributeCertificateRefs					
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	ND	ND	ND	ND	ND
	AttributeRevocationRefs					
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	R*	R*	O*	O*	O*
	TimestampedCertsCRLs					
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	R*	R*	R*	O*	O*
	CertificateValues					
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	R*	R*	R*	O*	O*
	RevocationValues					
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND	ND	ND	ND
	ArchiveTimeStampToken					

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	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Tipo de conteúdo (<i>content type</i>)	id-contentType	O	O	O	O	O
	ContentType					
Resumo criptográfico da mensagem (<i>message digest</i>)	id-messageDigest	O	O	O	O	O
	MessageDigest					
Certificado do signatário v1 (<i>ESS signing certificate</i>)	id-aa-signingCertificate	O	O	O	O	O
	SigningCertificate					
Identificador da política de assinatura (<i>signature policy identifier</i>)	id-aa-ets-sigPolicyId	ND	ND	ND	ND	ND
	SignaturePolicyIdentifier					
Atributos do signatário (<i>signer attributes</i>)	id-aa-ets-signerAttr	ND	ND	ND	ND	ND
	SignerAttribute					
Instante da assinatura (<i>signing time</i>)	id-signingTime	ND	ND	ND	ND	ND
	SigningTime					
Localização do signatário (<i>signer location</i>)	id-aa-ets-signerLocation	ND	ND	ND	ND	ND
	SignerLocation					
Carimbo do tempo de conteúdo (<i>content time stamp</i>)	id-aa-ets-contentTimeStamp	ND	ND	ND	ND	ND
	ContentTimeStamp					

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

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Contra assinatura (<i>countersignature</i>)	id-countersignature	ND	ND	ND	ND	ND
	CounterSignature					
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	ND	ND	ND	ND	ND
	SignatureTimeStampToken					
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	P	P	O	O	O
	CompleteCertificateRefs					
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	P	P	O	O	O
	CompleteRevocationRefs					
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	ND	ND	ND	ND	ND
	AttributeCertificateRefs					
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	ND	ND	ND	ND	ND
	AttributeRevocationRefs					
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	P	P	O	O	O
	TimestampedCertsCRLs					
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	P	P	P	O	O
	CertificateValues					
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	P	P	P	O	O
	RevocationValues					
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND	ND	ND	ND
	ArchiveTimeStampToken					

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

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Tipo de conteúdo (<i>content type</i>)	id-contentType	O	O	O	O	O
	ContentType					
Resumo criptográfico da mensagem (<i>message digest</i>)	id-messageDigest	O	O	O	O	O
	MessageDigest					
Certificado do signatário v1 (<i>ESS signing certificate</i>)	id-aa-signingCertificate	O	O	O	O	O
	SigningCertificate					
Identificador da política de assinatura (<i>signature policy identifier</i>)	id-aa-ets-sigPolicyId	ND	ND	ND	ND	ND
	SignaturePolicyIdentifier					
Atributos do signatário (<i>signer attributes</i>)	id-aa-ets-signerAttr	ND	ND	ND	ND	ND
	SignerAttribute					
Instante da assinatura (<i>signing time</i>)	id-signingTime	ND	ND	ND	ND	ND
	SigningTime					
Localização do signatário (<i>signer location</i>)	id-aa-ets-signerLocation	ND	ND	ND	ND	ND
	SignerLocation					
Carimbo do tempo de conteúdo (<i>content time stamp</i>)	id-aa-ets-contentTimeStamp	ND	ND	ND	ND	ND
	ContentTimeStamp					

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

Nome do atributo	Identificação do atributo	Perfil AD				
	Tipo do conteúdo	RB	RT	RV	RC	RA
Contra assinatura (<i>countersignature</i>)	id-countersignature	ND	ND	ND	ND	ND
	CounterSignature					
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	ND	ND	ND	ND	ND
	SignatureTimeStampToken					
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	P	P	O	O	O
	CompleteCertificateRefs					
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	P	P	O	O	O
	CompleteRevocationRefs					
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	ND	ND	ND	ND	ND
	AttributeCertificateRefs					
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	ND	ND	ND	ND	ND
	AttributeRevocationRefs					
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	P	P	O	O	O
	TimestampedCertsCRLs					
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	P	P	P	O	O
	CertificateValues					
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	P	P	P	O	O
	RevocationValues					
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND	ND	ND	ND
	ArchiveTimeStampToken					

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

Nome do atributo	Identificação do atributo	Carimbo	
	Tipo do conteúdo	Anterior	Corrente
Tipo de conteúdo (<i>content type</i>)	id-contentType	O	O
	ContentType		
Resumo criptográfico da mensagem (<i>message digest</i>)	id-messageDigest	O	O
	MessageDigest		
Certificado do signatário v1 (<i>ESS signing certificate</i>)	id-aa-signingCertificate	O	O
	SigningCertificate		
Identificador da política de assinatura (<i>signature policy identifier</i>)	id-aa-ets-sigPolicyId	ND	ND
	SignaturePolicyIdentifier		
Atributos do signatário (<i>signer attributes</i>)	id-aa-ets-signerAttr	ND	ND
	SignerAttribute		
Instante da assinatura (<i>signing time</i>)	id-signingTime	ND	ND
	SigningTime		
Localização do signatário (<i>signer location</i>)	id-aa-ets-signerLocation	ND	ND
	SignerLocation		
Carimbo do tempo de conteúdo (<i>content time stamp</i>)	id-aa-ets-contentTimeStamp	ND	ND
	ContentTimeStamp		

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

Nome do atributo	Identificação do atributo	Carimbo	
	Tipo do conteúdo	Anterior	Corrente
Contra assinatura (<i>countersignature</i>)	id-countersignature	ND	ND
	CounterSignature		
Carimbo do tempo de assinatura (<i>signature time stamp</i>)	id-aa-signatureTimeStampToken	ND	ND
	SignatureTimeStampToken		
Referências completas aos certificados (<i>complete certificate references</i>)	id-aa-ets-certificateRefs	O	O
	CompleteCertificateRefs		
Referências completas à revogação (<i>complete revocation references</i>)	id-aa-ets-revocationRefs	O	O
	CompleteRevocationRefs		
Referências aos certificados de atributo (<i>attribute certificate references</i>)	id-aa-ets-attrCertificateRefs	ND	ND
	AttributeCertificateRefs		
Referências à revogação de atributo (<i>attribute revocation references</i>)	id-aa-ets-attrRevocationRefs	ND	ND
	AttributeRevocationRefs		
Carimbo do tempo das referências (<i>time-stamped certificate crls references</i>)	id-aa-ets-certCRLTimestamp	O	R
	TimestampedCertsCRLs		
Valores dos certificados (<i>certificate values</i>)	id-aa-ets-certValues	O	P
	CertificateValues		
Valores de revogação (<i>revocation values</i>)	id-aa-ets-revocationValues	O	P
	RevocationValues		
Carimbo do tempo de arquivamento (<i>archive time-stamp</i>)	id-aa-archiveTimeStampToken	ND	ND
	ArchiveTimeStampToken		

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



Infraestrutura de Chaves Públicas Brasileira

ANEXO 2

1 POLÍTICA-PADRÃO AD-RB BASEADA EM CADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIA BÁSICA NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.1.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns

5.2.1 Regras de Signatário e Verificador

5.2.1.1 Regras do Signatário



Infraestrutura de Chaves Públicas Brasileira

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) **id-aa-signingCertificate**;
- d) **id-aa-ets-sigPolicyId**.

5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

Não se aplica.

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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Não se aplica.

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

5.2.2.1 Requisitos de Certificados

5.2.2.1.1 Raiz Confiável



Infraestrutura de Chaves Públicas Brasileira

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

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

5.2.3 Condições de Confiabilidade de Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatários

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

2 POLÍTICA-PADRÃO AD-RT BASEADA EM CADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIA DO TEMPO NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.2.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns

5.2.1 Regras de Signatário e Verificador

5.2.1.1 Regras do Signatário



Infraestrutura de Chaves Públicas Brasileira

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) **id-aa-signingCertificate**;
- 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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

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.

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

5.2.2.1 Requisitos de Certificados



Infraestrutura de Chaves Públicas Brasileira

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e

<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e

<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras adicionais de Revogação para Certificados



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

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.

5.2.3.2.2.2 Regras adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatários

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

3 POLÍTICA-PADRÃO AD-RV BASEADA EM CADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS PARA VALIDAÇÃO NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.3.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns

5.2.1 Regras de Signatário e Verificador



Infraestrutura de Chaves Públicas Brasileira

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) **id-aa-signingCertificate**;
- 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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

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:



Infraestrutura de Chaves Públicas Brasileira

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

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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 :

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

5.2.2.2 Requisitos de Revogação

5.2.2.2.1 Requisitos de Revogação para Certificados Finais



Infraestrutura de Chaves Públicas Brasileira

5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

5.2.2.2.1.2 Regras adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos



Infraestrutura de Chaves Públicas Brasileira

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

4 POLÍTICA-PADRÃO AD-RC BASEADA EM CADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS COMPLETAS NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.4.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns

5.2.1 Regras de Signatário e Verificador



Infraestrutura de Chaves Públicas Brasileira

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) **id-aa-signingCertificate**;
- 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

Os certificados do caminho de certificação completo 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**;



Infraestrutura de Chaves Públicas Brasileira

- 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.**

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

5.2.2.2 Requisitos de Revogação

5.2.2.2.1 Requisitos de Revogação para Certificados Finais



Infraestrutura de Chaves Públicas Brasileira

5.2.2.2.1.1 Mecanismos de Revogação para Certificados

LCR ou OCSP.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário



Infraestrutura de Chaves Públicas Brasileira

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 1135491 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA e de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5 POLÍTICA-PADRÃO AD-RA BASEADA EM CADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS PARA ARQUIVAMENTO NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.5.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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).

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

5 Política de Validação da Assinatura

5.1 Período para Assinatura

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns



Infraestrutura de Chaves Públicas Brasileira

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) **id-aa-signingCertificate**;
- 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-certValues**;
- e) **id-aa-ets-revocationValues**;
- f) **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

Os certificados do caminho de certificação completo do signatário.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios



Infraestrutura de Chaves Públicas Brasileira

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-certValues;**
- e) **id-aa-ets-revocationValues;**
- f) **id-aa-ets-archiveTimestampV2.**

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e

<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos



Infraestrutura de Chaves Públicas Brasileira

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA e de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

6 POLÍTICA-PADRÃO AD-RB BASEADA EM XADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIA BÁSICA NO FORMATO XML-DSig versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.6.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

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.



Infraestrutura de Chaves Públicas Brasileira

5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

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

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

5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

Não se aplica.

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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Não se aplica.

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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 :

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e



Infraestrutura de Chaves Públicas Brasileira

<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3 Condições de Confiabilidade do Carimbo do Tempo



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

7 POLÍTICA-PADRÃO AD-RT BASEADA EM XADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIA do tempo NO FORMATO XML-DSig versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.7.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns

5.2.1 Regras de Signatário e Verificador



Infraestrutura de Chaves Públicas Brasileira

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:

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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

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**.

5.2.1.2.2 Regras Adicionais do Verificador



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

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 :

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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



Infraestrutura de Chaves Públicas Brasileira

LCR ou OCSP.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave



Infraestrutura de Chaves Públicas Brasileira

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

8 POLÍTICA-PADRÃO AD-RV BASEADA EM XADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS PARA VALIDAÇÃO NO FORMATO XML-DSig versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.8.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns



Infraestrutura de Chaves Públicas Brasileira

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:

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

Nenhum certificado.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

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:



Infraestrutura de Chaves Públicas Brasileira

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

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

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



Infraestrutura de Chaves Públicas Brasileira

LCR ou OCSP.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo



Infraestrutura de Chaves Públicas Brasileira

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

9 POLÍTICA-PADRÃO AD-RC BASEADA EM XADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS COMPLETAS NO FORMATO XML-DSig versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.9.1

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.

5.2 Regras Comuns



Infraestrutura de Chaves Públicas Brasileira

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:

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

Os certificados do caminho de certificação completo do signatário.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

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:



Infraestrutura de Chaves Públicas Brasileira

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

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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 :

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado

Não se aplica.

5.2.2.2 Requisitos de Revogação



Infraestrutura de Chaves Públicas Brasileira

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e

<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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.

5.2.3.1.4 Restrições de Nome

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos



Infraestrutura de Chaves Públicas Brasileira

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chave para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.



Infraestrutura de Chaves Públicas Brasileira

10 POLÍTICA-PADRÃO AD-RA BASEADA EM XADES

1 Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM REFERÊNCIAS PARA ARQUIVAMENTO NO FORMATO XML-DSig versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.10.1.

2 Data de Emissão

A data de emissão desta PA é 31.10.2008.

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).

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

O período para assinatura desta PA é de 31/10/2008 a 31/12/2014.



Infraestrutura de Chaves Públicas Brasileira

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:

- a) **DataObjectFormat** (em assinaturas do tipo *detached*);
- b) **SigningCertificate**;
- c) **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) **CertificateValues**;
- e) **RevocationValues**;
- f) **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

Os certificados do caminho de certificação completo do signatário.

5.2.1.1.6 Regras Adicionais do Signatário

Não se aplica.

5.2.1.2 Regras do Verificador



Infraestrutura de Chaves Públicas Brasileira

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) **CertificateValues;**
- e) **RevocationValues;**
- f) **ArchiveTimeStamp.**

5.2.1.2.2 Regras Adicionais do Verificador

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.2.1.2 Restrição do Caminho de Certificação

não se aplica.

5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável

Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada 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.

5.2.2.1.4 Restrições de Nome

Não se aplica.

5.2.2.1.5 Restrições de Políticas de Certificado



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

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.

5.2.2.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.2.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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:

<http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt> e
<http://acraiz.icpbrasil.gov.br/ICP-Brasil.crt>

5.2.3.1.2 Restrição do Caminho de Certificação

Não se aplica.

5.2.3.1.3 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



Infraestrutura de Chaves Públicas Brasileira

2.16.76.1.2.304.1 ao OID 2.16.76.1.2.304.100), conforme definido no DOC-ICP-04.

5.2.3.1.4 Restrições de Nome

Não se aplica.

5.2.3.1.5 Restrições de Políticas de Certificado

Não se aplica.

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.

5.2.3.2.1.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

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.

5.2.3.2.2.2 Regras Adicionais de Revogação para Certificados

Não se aplica.

5.2.3.3 Restrições de Nome

Não se aplica.

5.2.3.4 Período de Cautela

Não se aplica.

5.2.3.5 Atraso do Carimbo do Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos



Infraestrutura de Chaves Públicas Brasileira

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

5.2.5.1 Restrições de Algoritmos para Signatário

5.2.5.1.1 Restrições de Algoritmos

5.2.5.1.1.1 Identificador de Algoritmo

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar o algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

5.2.5.1.1.2 Tamanho Mínimo de Chave

O tamanho mínimo de chaves para criação de assinaturas segundo esta PA é de 1024 bits.

5.2.5.1.1.3 Regras Adicionais de Restrições

Não se aplica.

5.2.5.2 Restrições de Algoritmos para AC Final

Não se aplica.

5.2.5.3 Restrições de Algoritmos para AC Intermediária

Não se aplica.

5.2.5.4 Restrições de Algoritmos para Autoridade de Atributo

Não se aplica.

5.2.6 Regras Adicionais

Não se aplica.

5.3 Regras para Propósitos Específicos de Assinatura

Não se aplica.

5.4 Informações Adicionais sobre a Validação das Assinaturas

Não se aplica.

6 Informações Adicionais sobre a Política de Assinatura

Não se aplica.

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.



ICP Brasil Infraestrutura de Chaves Públicas Brasileira

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 A LPA é assinada e publicada pela AC Raiz da ICP-Brasil, de forma segura, no seu repositório no endereço web www.acraiz.icpbrasil.gov.br/LPA.

4.3 A LPA é atualizada pela AC Raiz **a cada 90 dias** e contém em seu corpo a data da sua próxima atualização.

4.4 A LPA é assinada com uma Assinatura Digital ICP-Brasil, **por funcionário da AC Raiz** nomeado e autorizado, a quem foi emitido um certificado por uma das autoridades certificadoras credenciadas na ICP-Brasil.

4.5 A LPA é codificada em linguagem de máquina (ASN.1 e XML) e traz, 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).

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.

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.