Infra-Estrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL

DOC-ICP-15.03
Versão 1.0

Sumário

1. INFORMAÇÕES GERAIS

1.1 Este documento estabelece os requisitos mínimos 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 [6] e ETSI TR 102.038 [9].

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

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

b) REQUISITOS TÉCNICOS PARA GERAÇÃO E VERFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15.01;

c) PERFIL DE USO GERAL PARA ASSINATURAS ICP-BRASIL – DOC-ICP-15.02;

d) REQUISITOS MÍNIMOS PARA AS 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 Aprovadas ICP-Brasil 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 ASN.1 ou XML.

1.7 Antes de entrar em utilização, uma Política de Assinatura criada no âmbito da ICP-Brasil DEVE ser submetida à AC-Raiz para fins de obtenção de um identificador único (Object Identifier), que a diferencie de outras políticas e permita seu correto processamento pelos sistemas. Após esse procedimento, a política será reconhecida como Política de Assinatura Aprovada ICP-Brasil.

1.8 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).

1.9 Para facilitar a utilização de políticas de assinatura pelos usuários finais, o ITI criou 10 Políticas de Assinatura-padrão, que estão detalhadas no **Anexo 1** neste documento.

1.10 O processo de gerenciamento das Políticas de Assinatura pela AC Raiz da ICP-Brasil está descrito no **Anexo 2** deste documento.

1.1 TERMINOLOGIA

Os termos abaixo, quando encontrados ao longo deste documento grafados em maiúsculas, DEVEM ser interpretados conforme descrito neste item:

1.1.1 **DEVE (D)** - Esta palavra, ou os termos "EXIGIDO" ou "OBRIGATÓRIO, significa que a definição é um requisito absoluto da especificação.

1.1.2 **NÃO DEVE (ND)** - Esta expressão, ou o termo “PROIBIDO¨ significa que a definição é uma proibição absoluta na especificação.
1.1.3 **É RECOMENDADO (R)** - Esta expressão, ou o adjetivo "RECOMENDADO", significa que podem existir razões válidas, em circunstâncias particulares, para ignorar um ponto específico, mas as implicações completas precisam ser entendidas e ponderadas cuidadosamente antes de escolher um caminho diferente.
1.1.4 **NÃO É RECOMENDADO (NR)** - Esta expressão significa que podem existir razões válidas, em circunstâncias particulares, em que o comportamento possa ser aceitável ou mesmo útil, mas as implicações completas devem ser entendidas e ponderadas cuidadosamente, antes de se realizar qualquer comportamento descrito com este rótulo.
1.1.5 **PODE (P)** - Esta palavra, ou o adjetivo "OPCIONAL", significa que é um item verdadeiramente opcional. Um implementador pode optar por incluir o item, enquanto outro pode omitir o mesmo item. Uma aplicação que não inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que inclui aquela opção, embora talvez com funcionalidade reduzida. No mesmo espírito, uma aplicação que inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que não a inclui (exceto, é claro, para o recurso que a opção oferece.)

2. CONTEÚDO DA POLÍTICA DE ASSINATURA

Os itens a seguir relacionam os conteúdos que DEVEM, obrigatoriamente, fazer parte de uma Política de Assinatura Aprovada ICP-Brasil

2.1 Identificador da Política de Assinatura

2.1.1 Neste item DEVE ser identificada a Política de Assinatura e indicado o seu OID (*Object Identifier*).
2.1.2 No âmbito da ICP-Brasil, será atribuído um OID à Política de Assinatura na conclusão do processo de aprovação por parte ITI, o qual terá o formato 2.16.76.1.7.n.o.p, onde:
n: valor atribuído à entidade que solicita a aprovação da Política de Assinatura;
o: valor atribuído seqüencialmente às Políticas de Assinatura da entidade solicitante;
p: versão da Política de Assinatura Aprovada.
2.1.3 Toda Política de Assinatura Aprovada ICP-Brasil DEVE estar disponível publicamente a todos interessados. Neste item DEVE ser indicada a URL onde a Política de Assinatura PODE ser consultada.
2.1.4 Neste item DEVE ser mencionado que as Políticas de Assinatura Aprovadas estarão disponíveis para consulta também no repositório da AC-Raiz.

2.2 Data da Criação

Neste item DEVE ser informada a data de criação da Política de Assinatura.

2.3 Entidade Criadora da Política de Assinatura

Este item DEVE conter uma identificação da entidade responsável pela criação da Política de Assinatura e da comunidade que fará uso dela. No âmbito da ICP-Brasil, qualquer entidade (pessoa física ou jurídica, órgão de governo etc.) PODE criar Políticas de Assinatura, conforme sua

necessidade e conveniência.

2.4 Campo de Aplicação

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.

2.4.2 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

O campo Política de Validação estabelece as regras gerais e específicas aplicadas à Assinatura Digital e que DEVEM ser observadas pelo assinante e pelo verificador da assinatura.

2.5.1 Período para Assinatura

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

2.5.1.2 O período de validade máximo admitido para uma Política de Assinatura no âmbito da ICP-Brasil é de 05 (cinco) anos.

2.5.2 Regras Comuns

Este campo define as regras comuns e gerais, tanto para o processo de assinatura pelo signatário, quanto para o processo de verificação pelo verificador.

Se um campo estiver presente nas Regras Comuns então ele NÃO DEVERÁ estar presente em nenhum campo de Regras para Propósitos Específicos de Assinatura.

2.5.2.1 Regras do Signatário e do Verificador

2.5.2.1.1 Regras do Signatário

Este campo define as regras que DEVEM ser observadas e incluídas no pacote da assinatura pelo signatário, no momento da assinatura digital do documento eletrônico. Todas as assinaturas geradas segundo uma Política de Assinatura Aprovada ICP-Brasil DEVEM estar em conformidade com o disposto no DOC-ICP-15.01, capítulo 4.

OBS.: Permite-se, adicionalmente, o uso de qualquer dos atributos e propriedades previstos nos padrões CMS, CAdES, XMLDSIG e XAdES, definidos respectivamente na RFC 3852 [14], no documento ETSI TR 102733 [7], na RFC 3275 [15] e no documento ETSI TS 102903 [10].

2.5.2.1.1.1 Dados Externos ou Internos a Assinatura

Neste item DEVE ser descrito se existe ou não a obrigatoriedade de inclusão do conteúdo assinado (documento eletrônico) na assinatura digital.

No caso de o conteúdo não ser incluído, ou seja, se ele ficar externo ao pacote de assinatura digital, DEVE ser descrita a forma de obter o conteúdo para verificação da assinatura.

2.5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

2.5.2.1.1.2.1 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.

2.5.2.1.1.2.2 O documento DOC-ICP-15.01, capítulo 4, define os atributos ou propriedades obrigatórios, para todos os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

2.5.2.1.1.3.1 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.

2.5.2.1.1.3.2 O documento DOC-ICP-15.01, capítulo 4, define, os atributos ou propriedades obrigatórios, para todos os formatos de assinatura digital ICP-Brasil.

2.5.2.1.1.3.3 A inclusão desses atributos ou propriedades não assinados PODE, opcionalmente, ser realizada pelo verificador ao invés do signatário. Nestes casos DEVEM ser informados neste item apenas os atributos que DEVEM ser incluídos pelo signatário. Os que DEVEM ser incluídos pelo verificador DEVEM ser relacionados no item 2.5.2.1.2.1.

2.5.2.1.1.4 Referências à Cadeia de Certificação

2.5.2.1.1.4.1 Neste item DEVE ser descrito que todas as assinaturas digitais criadas com base nesta Política de Assinatura DEVEM conter obrigatoriamente a referência ao certificado do signatário, por meio do identificador Serial do Emissor.

2.5.2.1.1.5 Valores da Cadeia de Certificação

2.5.2.1.1.5.1 Neste item DEVE ser descrito se as assinaturas digitais criadas com base nesta Política de Assinatura devem ou não conter, obrigatoriamente, os certificados do signatário bem como todos os certificados da cadeia de certificação.

2.5.2.1.1.5.3 Caso o verificador possa encontrar um ou mais certificados da cadeia de certificação através de alguma outra forma, PODE ser incluído na assinatura digital apenas o certificado do signatário ou até mesmo nenhum dos certificados. Nestes casos, DEVE ser descrito de que forma os certificados estarão disponíveis e podem ser utilizados para a verificação da assinatura.

2.5.2.1.1.6 Regras Adicionais do Signatário

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

Este item descreve as regras de validação da Assinatura Digital, aplicáveis a atributos ou propriedades não incluídos pelo signatário no momento da assinatura, os quais DEVEM então ser incluídos pelo verificador.

2.5.2.1.2.1 Atributos Não-Assinados Obrigatórios

Este item DEVE conter obrigatoriamente os atributos descritos no item 2.5.2.1.1.3 que não são incluídos pelo signatário.

2.5.2.1.2.2 Regras Adicionais do Verificador

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

2.5.2.2.1 Validação da Cadeia de Certificação

Neste item DEVE constar que o processo de validação dos certificados da cadeia de certificação do signatário DEVE ser realizado em conformidade com a RFC 3280 e com o disposto nesta Política de Assinatura.

2.5.2.2.1.1 Raiz Confiável

Neste item DEVE constar que a validação DEVE ser feita tomando como ponto de confiança o certificado da AC-Raiz da ICP-Brasil, que se encontra disponível em http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt.

2.5.2.2.1.2 Restrição do Caminho de Certificação

Neste item DEVE constar que o número máximo de certificados de AC, no caminho de certificação entre o certificado do signatário e o da AC-Raiz é 2 (dois).

2.5.2.2.1.3 Conjunto de Políticas de Certificação Aceitáveis

Neste item DEVEM constar os tipos de certificados ICP-Brasil, cujas chaves privadas associadas PODEM gerar assinaturas digitais segundo a Política de Assinatura. Entre os tipos aceitáveis, tem-se:

Tipo de Certificado	OID
A1	2.16.76.1.2.1.*n*
A2	2.16.76.1.2.2.*n*
A3	2.16.76.1.2.3.*n*
A4	2.16.76.1.2.4.*n*

2.5.2.2.1.4 Restrições de Nome

Neste item, caso existam, DEVEM constar os nomes (Subject Distinguished Name e/ou Subject Alternative Name) para os quais os certificados DEVEM ser rejeitados.

2.5.2.2.1.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

2.5.2.2.1.5.1 Neste item PODEM constar os indicadores relativos às Políticas de Certificado permitidas para garantir a aceitação dos certificados da cadeia de certificação. Opcionalmente PODEM ser definidos os certificados da cadeia que DEVEM ter suas Políticas verificadas.

2.5.2.2.1.5.2 Caso existam, também PODEM constar os indicadores relativos às Políticas de Certificado correspondentes aos certificados que DEVEM ser rejeitados. Opcionalmente PODEM ser definidos os certificados da cadeia que DEVEM ter suas Políticas verificadas.

2.5.2.2.2 Forma de Verificação do Estado da Cadeia de Certificação

2.5.2.2.2.1 Neste item DEVE constar que é obrigatória a verificação do estado do certificado do signatário. Deve ser especificado o método a ser utilizado para essa verificação.

2.5.2.2.2.2 Também DEVE constar que é obrigatória a verificação do estado dos certificados das Autoridades Certificadoras da cadeia de certificação do signatário. Deve ser especificado o método a ser utilizado para essa verificação.

2.5.2.2.2.3 Entre os métodos de verificação de estado estão a consulta a LCR (Lista de Certificados Revogados) em conformidade com a RFC 3280, a consulta OCSP (Online Certificate Status Protocol) em conformidade com a RFC 2560 ou algum outro método aprovado pela ICP-Brasil.

2.5.2.3 Condições de Confiabilidade do Carimbo de Tempo

NOTA: Este item não se aplica a assinaturas formato EPES

2.5.2.3.1 Validação da Cadeia de Certificação

Neste item DEVE constar que o processo de validação dos certificados da cadeia de certificação da Autoridade de Carimbo de Tempo DEVE ser realizado em conformidade com a RFC 3280 e com o disposto nesta Política de Assinatura.

2.5.2.3.1.1 Raiz Confiável

Neste item DEVE constar que a validação DEVE ser feita tomando como ponto de confiança o certificado da AC-Raiz da ICP-Brasil, que se encontra disponível em http://acraiz.icpbrasil.gov.br/CertificadoACRaiz.crt

2.5.2.3.1.2 Restrição do Caminho de Certificação

Neste item DEVE constar o tamanho máximo do caminho de certificação, ou seja, número de Autoridades Certificadoras entre a Raiz confiável e o certificado da Autoridade de Carimbo de Tempo. No caso da ICP-Brasil, o máximo é 2 (dois).

2.5.2.3.1.3 Conjunto de Políticas de Certificação Aceitáveis

Neste item DEVEM constar os tipos de certificados ICP-Brasil, cujas chaves privadas associadas PODEM gerar carimbos de tempo, aceitos segundo esta Política de Assinatura. Entre os tipos aceitáveis tem-se:

Tipo de Certificado	OID
T3	2.16.76.1.2.303.n
T4	2.16.76.1.2.304.n

2.5.2.3.1.4 Restrições de Nome

Neste item, caso existam, DEVEM constar os nomes (Subject Distinguished Name e/ou Subject Alternative Name) para os quais os certificados DEVEM ser rejeitados.

2.5.2.3.1.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

2.5.2.2.3.1.5.1 Neste item PODEM constar os indicadores relativos as Políticas de Certificado permitidos para garantir a aceitação dos certificados da cadeia de certificação da Autoridade de Carimbo de Tempo. Opcionalmente PODEM ser definidos os certificados dessa cadeia de certificação que DEVEM ter suas Políticas verificadas.

2.5.2.2.3.1.5.2 Caso existam, também PODEM constar os indicadores relativos as Políticas de Certificado correspondentes aos certificados que DEVEM ser rejeitados. Opcionalmente PODEM ser definidos os certificados da cadeia que DEVEM ter suas Políticas verificadas.

2.5.2.3.2 Forma de Verificação do Estado da Cadeia de Certificação

2.5.2.3.2.1 Neste item DEVE constar que é obrigatória a verificação do estado do certificado da Autoridade de Carimbo de Tempo. Deve ser especificado o método a ser utilizado para essa verificação.

2.5.2.3.2.2 Também DEVE constar que é obrigatória a verificação do estado dos certificados das Autoridades Certificadoras da cadeia de certificação da Autoridade de Carimbo de Tempo. Deve ser especificado o método a ser utilizado para essa verificação

2.5.2.3.2.3 Entre os métodos de verificação de estado estão a consulta a LCR (Lista de Certificados Revogados) em conformidade com a RFC 3280, a consulta OCSP (Online Certificate Status Protocol) em conformidade com a RFC 2560 ou algum outro método aprovado pela ICP-Brasil.

2.5.2.3.3 Restrições de Nome

Neste item, caso existam, DEVEM constar as restrições dos nomes (Subject Distinguished Name e/ ou Subject Alternative Name) aceitos para as Autoridades de Carimbo de Tempo que PODEM atuar como tal no âmbito desta Política de Assinatura.

2.5.2.3.4 Período de Cautela

Opcionalmente, PODE ser informado neste item o período de tempo necessário após a data e hora do atributo assinado “Signing Time” para que seja realizada a validação da assinatura digital.

2.5.2.3.5 Atraso do Carimbo de Tempo

Nos casos de assinaturas digitais que incluem o atributo assinado “Signing Time”, opcionalmente PODE ser definido um período de tempo máximo permitido entre a data e hora do atributo assinado e a data e hora do carimbo de tempo. Este item determina o período de latência de data e hora entre a data e hora da máquina onde foi realizada a assinatura e a data e hora oficial dada pela ACT.

2.5.2.4 Condições de Confiabilidade dos Atributos

2.5.2.4.1 Atributos Obrigatórios

Item não aplicável.

2.5.2.4.2 Atributos Exigidos

Item não aplicável.

2.5.2.4.3 Validação da Cadeia de Certificação

2.5.2.4.3.1 Raiz Confiável

Item não aplicável.

2.5.2.4.3.2 Restrição do Caminho de Certificação

Item não aplicável.

2.5.2.4.3.3 Conjunto de Políticas de Certificação Aceitáveis

Item não aplicável.

2.5.2.4.3.4 Restrições de Nome

Item não aplicável.

2.5.2.4.3.5 Restrições de Políticas (Aceitável e Não-Aceitáveis)

Item não aplicável.

2.5.2.4.4 Forma de Verificação do Estado da Cadeia de Certificação

Item não aplicável.

2.5.2.4.5 Restrições de Atributos

Item não aplicável.

2.5.2.5 Conjunto de Restrições de Algoritmos

2.5.2.5.1 Caso existam restrições quanto aos algoritmos e tamanhos de chaves, associados a assinatura digital e às entidades que têm algum tipo de participação na assinatura digital, aceitos no âmbito desta Política de Assinatura, essas DEVEM ser descritas neste item.

2.5.2.5.2 Podem ser incluídas restrições de aceitação do algoritmo utilizado pelo signatário para a realização da assinatura digital, do algoritmo do usado para assinar o certificado do signatário, dos certificados das Autoridades Certificadoras que compõe a cadeia de certificação do signatário, da Autoridade de Atributo e da Autoridade de Carimbo de Tempo, indicando para cada um desses tipos quais são as restrições quanto aos algoritmos (hash, chave pública, combinação do hash com chave pública) e quanto ao tamanho de chave mínimo exigido para esses algoritmos de assinatura.

2.5.2.5.3 Opcionalmente, PODEM também ser descritas quaisquer outras restrições de aceitação relacionadas a algoritmos.

2.5.2.5.4 Os algoritmos DEVEM ser escolhidos entre os listados no documento Padrões e Algoritmos Criptográficos da ICP-Brasil – DOC-ICP-01.01.

2.5.2.6 Regras Adicionais

Caso haja a necessidade de incluir regras adicionais para geração ou verificação de assinaturas digitais, como por exemplo o ambiente mínimo exigido para assinatura digital, elas DEVEM ser incluídas neste item.

2.5.3 Regras para Propósitos Específicos de Assinatura

Caso existam regras para propósitos específicos de assinatura, diferentes das regras definidas no item 2.5.2., essas DEVEM ser detalhadas nos próximos itens.

2.5.3.1 Tipos de Propósitos Selecionados

Deve ser identificado o tipo de propósito para o qual a assinatura se destina, dentre aqueles definidos nos padrões ETSI TR 102 733 [7] e ETSI TS 101 903 [9].

2.5.3.2 Regras de Signatário e Verificador

Caso existam regras específicas para determinados tipos de compromisso, elas DEVEM ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.1.

2.5.3.3 Condições de Confiabilidade dos Certificados dos Signatários

Caso existam regras específicas para determinados tipos de compromisso, elas DEVEM ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.2.

2.5.3.4 Condições de Confiabilidade do Carimbo de Tempo

Caso existam regras específicas para determinados tipos de compromisso, elas DEVEM ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.3.

2.5.3.5 Condições de Confiabilidade dos Atributos

Caso existam regras específicas para determinados tipos de compromisso, elas DEVEM ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.4.

2.5.3.6 Conjunto de Restrições de Algoritmos

Caso existam regras específicas para determinados tipos de compromisso, elas DEVEM ser detalhadas neste item, usando a mesma estrutura definida em 2.5.2.5.

2.5.3.7 Regras Adicionais

Caso haja a necessidade de regras adicionais para geração ou verificação de assinaturas digitais para determinado propósito específico, elas DEVEM ser incluídas neste item.

2.5.4 Informações Adicionais sobre a Validação das Assinaturas

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

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

3. BIBLIOGRAFIA

[1] ITI. Glossário ICP-Brasil. Instituto Nacional de Tecnologia da Informação. Versão 1.2; Brasília:

ICP-Brasil, 2007.
[2] SCHNEIER, Bruce. Applied Cryptografy, Second Edition: protocols, algorithms, and source code in C. USA: Wiley, 1996.
[3] DOURNAEE, Blake. XML Security. Berkely: McGraw-Hill/Osborne, 2002.
[4] ETSI. Signature Policies Report. ETSI TR 102 041 (2002-02); European Telecomunications Standards Institute, 2002.
[5] ETSI. Eletronic Signature and Infraestructures (ESI); Signature policy for extended business model. ETSI TR 102 045 (2005-03); European Telecomunications Standards Institute, 2005.
[6] ETSI. Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies. ETSI TR 102 272 (2003-12); European Telecomunications Standards Institute, 2003.
[7] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), Technical Specification, 2008.
[8] ETSI. Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES); ETSI TS 102 734 (2007-02); European Telecomunications Standards Institute, 2007.
[9] ETSI. TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies; ETSI TR 102 038 (2002-04); European Telecomunications Standards Institute, 2002.
[10] ETSI. XML Advanced Electronic Signatures (XAdES); ETSI TS 101 903 (2006-03); European Telecomunications Standards Institute, 2006.
[11] ETSI. Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES); ETSI TS 102 904 (2007-02); European Telecomunications Standards Institute, 2007.
[12] ETSI. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; ETSI TR 102 176 A (2005-07); European Telecomunications Standards Institute, 2005.
[13] ETSI.Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices; ETSI TR 102 176 B (2005-07); European Telecomunications Standards Institute, 2005.
[14] HOUSLEY, R. RFC 3852: Cryptographic message syntax (CMS). Internet Engineering Task Force (IETF), July 2004. (disponível em http://www.ietf.org/rfc/rfc3852.txt).
[15] RFC 3275 (Extensible Markup Language) XML - Signature Syntax and Processing (2002-03);
[16] RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (1999-06);
[17] RFC 3126 Electronic Signature Formats for long term electronic signatures (2001-09);
[18] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2002-04);
[19] W3-IET-XML SIG XML- Signature Syntax and Processing W3C Recommendation (2002-02).
[20] REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL DOC-ICP-12 - V 1.0
[21] ITI. PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL. DOC-ICP-01.01 Instituto Nacional de Tecnologia da Informação. Versão 1.0; Brasília: ICP-Brasil, 2006.
[22] RIVAU Fernandes, Murilo SIPEX: Uma proposta de modelo de política de assinatura / M.

Rivau Fernandes. -- ed.rev. -- São Paulo, 2006. 105 p. Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.
[23] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. ETSI TS 101 861 V1.2.1 (2002-03): Time stamping profile, technical specification, 2002.
[24] ADAMS, C.; CAIN, P.; PINKAS, D.; ZUCCHERATO, R. RFC 3161 – Internet X.509 public key infrastructure: Time-Stamp Protocol (TSP) Internet Engineering Task Force (IETF), August 2001. (disponível em http://www.ietf.org/rfc/rfc3161.txt).

4. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Código	Nome do documento
DOC-ICP-12	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL
DOC-ICP-01.01	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL

ANEXO 1 - POLÍTICAS DE ASSINATURA-PADRÃO ICP-BRASIL

1. Para facilitar a utilização de Políticas de Assinatura pelos usuários finais, o ITI criou 10 Políticas de Assinatura-padrão, que estão detalhadas a seguir.

2. Essas Políticas de Assinatura-padrão 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 CAdES e XAdES, citados no documento DOC-ICP-15.01, a saber:

a) assinatura digital de curto prazo (AD-CP);
b) assinatura digital com carimbo do tempo (AD-T);
c) assinatura digital com referências para validação (AD-R);
d) assinatura digital com referências completas (AD-C);
e) assinatura digital com informações para arquivamento (AD-A); ou
f) uma combinação dos formatos citados nos subitens a) até e).

3. Nas tabelas 1 a 12, nas páginas seguintes, temos a combinação dos elementos citados no parágrafo acima, aplicada aos diferentes contextos de assinatura.

4. Nos documentos “A” até “J” temos as 10 Políticas de Assinatura-padrão.

Tabela 1 – Presença de atributos assinados no SignerInfo do signatário

Nome do atributo	Identificação do atributo	Origem do requisito de inclusão do atributo	Perfil AD				
	Tipo do conteúdo		CP	T	R	C	A
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3852 [14] ETSI CAdES [7] seção 5.6	O	O	O	O	O
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3852 [14] ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate	RFC 2634 [14] e ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	id-aa-signingCertificatev2 SigningCertificateV2	FC5035 [14] e ETSI CAdES [7] seção 5.6					
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier	Requisito do perfil ICP-Brasil	O	O	O	O	O
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication	ETSI CAdES [7]	R	R	R	R	R
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute	ETSI CAdES [7]	P	P	P	P	P
Instante da assinatura **(*signing time*)**	id-signingTime SigningTime	RFC 3852 [14]	P	P	P	P	P
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation	ETSI CAdES [7]	P	P	P	P	P
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp	ETSI CAdES [7]	P	P	P	P	P
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 2 – Presença de atributos não assinados no SignerInfo do signatário

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD CP	T	R	C	A
Contra assinatura (*countersignature*)	id-countersignature CounterSignature	RFC 3852 [14]	P	P	P	P	P
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken	ETSI CAdES [7], ETSI TS 101 861 [23] e RFC 3161 [24]	P	O	O	O	O
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7]	P	P	O	O	O
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7]	P	P	O	O	O
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs	ETSI CAdES [7]	P	P	O	O	O
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs	ETSI CAdES [7]	P	P	O	O	O
Carimbo de tempo das referências (*time-stamped certificate crls references*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES[7]	P	P	O	O	P
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7]	P	P	P	O	O
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7]	P	P	P	O	O
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken	ETSI CAdES [7], ETSI TS 101 861 [23] e RFC 3161 [24]	ND	ND	ND	ND	O
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 3 – Presença de atributos assinados no SignerInfo de “contra assinatura”

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD				
			CP	T	R	C	A
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3852 [14] seção 11.4	ND	ND	ND	ND	ND
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3852 [14] seção 11.4 e ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate	ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	id-aa-signingCertificatev2 SigningCertificateV2						
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier	Requisito do perfil ICP-Brasil	O	O	O	O	O
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication	Requisito do perfil ICP-Brasil	R	R	R	R	R
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute		P	P	P	P	P
Instante da assinatura (*signing time*)	id-signingTime SigningTime		P	P	P	P	P
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation		P	P	P	P	P
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 4 – Presença de atributos não assinados no SignerInfo de "contra assinatura"

Nome do atributo	Identificação do atributo	Origem do requisito de inclusão do atributo	Perfil AD				
	Tipo do conteúdo		CP	T	R	C	A
Contra assinatura (*countersignature*)	id-countersignature CounterSignature	RFC 3852 [14] seção 11.4	P	P	P	P	P
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken	ETSI CAdES [7], ETSI TS 101 861 [23] e RFC 3161 [24]	P	O	O	O	O
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7]	P	P	O	O	O
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7]	P	P	O	O	O
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs	ETSI CAdES [7]	P	P	O	O	O
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs	ETSI CAdES [7]	P	P	O	O	O
Carimbo de tempo das referências (*time-stamped certificate crls references*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES [7]	P	P	O	O	O
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7]	P	P	P	O	O
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7]	P	P	P	O	O
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken	ETSI CAdES [7]	ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 5 – Presença de atributos assinados no TimeStampToken de "carimbo de tempo de conteúdo"

Nome do atributo	Identificação do atributo	Origem do requisito de inclusão do atributo	Perfil AD				
	Tipo do conteúdo		CP	T	R	C	A
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate id-aa-signingCertificatev2	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	 SigningCertificateV2						
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier		ND	ND	ND	ND	ND
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication		ND	ND	ND	ND	ND
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute		ND	ND	ND	ND	ND
Instante da assinatura (*signing time*)	id-signingTime SigningTime		ND	ND	ND	ND	ND
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation		ND	ND	ND	ND	ND
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 6 – Presença de atributos não assinados no TimeStampToken de "carimbo de tempo de conteúdo"

Nome do atributo	Identificação do atributo	Origem do requisito de inclusão do atributo	Perfil AD				
	Tipo do conteúdo		CP	T	R	C	A
Contra assinatura (*countersignature*)	id-countersignature CounterSignature		ND	ND	ND	ND	ND
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken		ND	ND	ND	ND	ND
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7] seção 6.2.1	R (*)	R (*)	O (*)	O (*)	O (*)
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7] seção 6.2.2	R (*)	R (*)	O (*)	O (*)	O (*)
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs		ND	ND	ND	ND	ND
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs		ND	ND	ND	ND	ND
Carimbo de tempo das referências (*time-stamped certificate crls references*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES [7] seção 6.3.6	R (*)	R (*)	O (*)	O (*)	O (*)
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7] seção 6.3.3	R (*)	R (*)	R (*)	O (*)	O (*)
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7] seção 6.3.4	R (*)	R (*)	R (*)	O (*)	O (*)
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							
(*) Como o atributo "carimbo de 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.							

Tabela 7 – Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo de tempo de assinatura."

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD				
			CP	T	R	C	A
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	id-aa-signingCertificatev2 SigningCertificateV2						
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier		ND	ND	ND	ND	ND
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication		ND	ND	ND	ND	ND
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute		ND	ND	ND	ND	ND
Instante da assinatura (*signing time*)	id-signingTime SigningTime		ND	ND	ND	ND	ND
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation		ND	ND	ND	ND	ND
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 8 – Presença de atributos não assinados no SignerInfo do TimeStampToken de "carimbo de tempo de assinatura."

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD				
			CP	T	R	C	A
Contra assinatura (*countersignature*)	id-countersignature CounterSignature		ND	ND	ND	ND	ND
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken		ND	ND	ND	ND	ND
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7] seção 6.2.1	P	P	O	O	O
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7] seção 6.2.2	P	P	O	O	O
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs		ND	ND	ND	ND	ND
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs		ND	ND	ND	ND	ND
Carimbo de tempo das referências (*time-stamped certificate crls references*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES [7] seção 6.3.6	P	P	O	O	O
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7] seção 6.3.3	P	P	P	O	O
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7] seção 6.3.4	P	P	P	O	O
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 9 – Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo de tempo das referências"

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD CP	T	R	C	A
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute) ETSI CAdES [7] seção 5.6	O	O	O	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	id-aa-signingCertificatev2 SigningCertificateV2						
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier		ND	ND	ND	ND	ND
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication		ND	ND	ND	ND	ND
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute		ND	ND	ND	ND	ND
Instante da assinatura (*signing time*)	id-signingTime SigningTime		ND	ND	ND	ND	ND
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation		ND	ND	ND	ND	ND
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 10 – Presença de atributos não assinados no SignerInfo do TimeStampToken de "carimbo de tempo das referências"

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Perfil AD				
			CP	T	R	C	A
Contra assinatura (*countersignature*)	id-countersignature CounterSignature		ND	ND	ND	ND	ND
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken		ND	ND	ND	ND	ND
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7] seção 6.2.1	P	P	O	O	O
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7] seção 6.2.2	P	P	O	O	O
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs		ND	ND	ND	ND	ND
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs		ND	ND	ND	ND	ND
Carimbo de tempo das referências (*time-stamped certificate crls references*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES [7] seção 6.3.6	P	P	O	O	O
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7] seção 6.3.3	P	P	P	O	O
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7] seção 6.3.4	P	P	P	O	O
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken		ND	ND	ND	ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)							

Tabela 11 – Presença de atributos assinados no SignerInfo do TimeStampToken de "carimbo de tempo de arquivamento"

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Carimbo de Arquivamento	
			Anterior	Corrente
Tipo de conteúdo (*content type*)	id-contentType ContentType	RFC 3852 [14] seção 5.3 e RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute)	O	O
hash da mensagem (*message digest*)	id-messageDigest MessageDigest	RFC 3852 [14] seção 5.3 e RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute)	O	O
Certificado do signatário v1 (*ESS signing certificate*)	id-aa-signingCertificate SigningCertificate	RFC 3161 [24] seção 2.4.2 (ref. SigningCertificate attribute)	O	O
Certificado do signatário v2 (*ESS signing certificate v2*)	id-aa-signingCertificatev2 SigningCertificateV2			
Identificador da política de assinatura (*signature policy identifier*)	id-aa-ets-sigPolicyId SignaturePolicyIdentifier		ND	ND
Indicação de tipo de compromisso (*commitment type indication*)	id-aa-ets-commitmentType CommitmentTypeIndication		ND	ND
Atributos do signatário (*signer attributes*)	id-aa-ets-signerAttr SignerAttribute		ND	ND
Instante da assinatura (*signing time*)	id-signingTime SigningTime		ND	ND
Localização do signatário (*signer location*)	id-aa-ets-signerLocation SignerLocation		ND	ND
Carimbo de tempo de conteúdo (*content time stamp*)	id-aa-ets-contentTimeStamp ContentTimeStamp		ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)				

Tabela 12 – Presença de atributos não assinados no SignerInfo do TimeStampToken de "carimbo de tempo de arquivamento"

Nome do atributo	Identificação do atributo Tipo do conteúdo	Origem do requisito de inclusão do atributo	Carimdo de Arquivamento	
			Anterior	Corrente
Contra assinatura (*countersignature*)	id-countersignature CounterSignature		ND	ND
Carimbo de tempo de assinatura (*signature time stamp*)	id-aa-signatureTimeStampToken SignatureTimeStampToken		ND	ND
Referências completas aos certificados (*complete certificate references*)	id-aa-ets-certificateRefs CompleteCertificateRefs	ETSI CAdES [7] seção 6.2.1	O	O
Referências completas à revogação (*complete revogation references*)	id-aa-ets-revocationRefs CompleteRevocationRefs	ETSI CAdES [7] seção 6.2.2	O	O
Referências aos certificados de atributo (*attribute certificate references*)	id-aa-ets-attrCertificateRefs AttributeCertificateRefs		ND	ND
Referências à revogação de atributo (*attribute revogation references*)	id-aa-ets-attrRevocationRefs AttributeRevocationRefs		ND	ND
Carimbo de tempo das referências (*time-stamped certificate and crls*)	id-aa-ets-certCRLTimestamp TimestampedCertsCRLs	ETSI CAdES [7] seção 6.3.6	O	R
Valores dos certificados (*certificate values*)	id-aa-ets-certValues CertificateValues	ETSI CAdES [7] seção 6.3.3	O	P
Valores de revogação (*revocation values*)	id-aa-ets-revocationValues RevocationValues	ETSI CAdES [7] seção 6.3.4	O	P
Carimbo de tempo de arquivamento (*archive time-stamp)*	id-aa-archiveTimeStampToken ArchiveTimeStampToken		ND	ND
Legenda: O-obrigatório, P-permitido, R-recomendado, ND-não deve (proibido)				

A - POLÍTICA-PADRÃO ICP-BRASIL AD-CP PARA ASSINATURAS BASEADAS EM CMS / CADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL DE CURTO PRAZO NO FORMATO CMS, versão 1.0.

O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.1.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.1.n+1.

Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2 .Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

4. Campo de Aplicação

Neste tipo de assinatura não são armazenados os dados fundamentais para sua validação futura e nem é colocado carimbo de tempo de assinatura. Como não existem condições de garantir a irretratabilidade da assinatura digital, este tipo de assinatura não pode ser usado para arbitragem, em caso de disputa entre signatário e verificador.

Por esse motivo, assinaturas do tipo AD-CP **somente devem ser utilizadas em situações especiais, por exemplo, para serviços transacionais que exigem autenticação de entidades e/ou verificação de integridade.**

Caso seja necessário verficar a assinatura posteriormente devem existam ferramentas adicionais para isso. As informações de validação deverão poder ser obtidas por outras fontes, como o sistema operacional da parte verificadora, por exemplo. Nessas situações, é recomendável que exista um acordo prévio, assinado por ambas as partes, signatário e verificador, concordando com a guarda unilateral desses dados complementares.

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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas realizadas segundo esta PA **podem ou não** incluir o conteúdo assinado na assinatura digital (*attached, ou detached*).

5.2.1.1.2 Atributos 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 ou Id-aa-signingCertificateV2
d) Id-aa-ets-sigPolicyId

5.2.1.1.3 Atributos Não-Assinados Obrigatórios

Não se aplica.

5.2.1.1.4 Referências à Cadeia de Certificação

O atributo signingCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas estruturas *SignerInfo*.

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

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

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

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

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos Não-Assinados Obrigatórios
Não se aplica.
5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável
Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificados ICP-Brasil tipo A3 (cujo OID é 2.16.76.1.2.3.n) ou A4 (cujo OID é 2.16.76.1.2.4.n), conforme definido no 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
Não se aplica

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

B - POLÍTICA-PADRÃO ICP-BRASIL AD-T PARA PARA ASSINATURAS BASEADAS EM CMS / CADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM CARIMBO DE 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. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.2.n+1.

Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de sua geração, pois o carimbo de tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura.

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. Mesmo assim, uma assinatura desse tipo pode ser contestada se houver, por exemplo, o 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas realizadas segundo esta PA **podem ou não** incluir o conteúdo assinado na assinatura digital (*attached, ou detached*).

5.2.1.1.2 Atributos 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 ou Id-aa-signingCertificateV2
d) Id-aa-ets-sigPolicyId

5.2.1.1.3 Atributos Não-Assinados Obrigatórios

a) id-aa-signatureTimeStampToken

5.2.1.1.4 Referências à Cadeia de Certificação

O atributo signingCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas estruturas *SignerInfo*.

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

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

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

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

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos Não-Assinados Obrigatórios

Caso não tenha sido incluído pelo signatário, o seguinte atributo DEVE ser incluído pelo verificador:

a) id-aa-signatureTimeStampToken.

5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável
Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificados ICP-Brasil tipo A3 (cujo OID é 2.16.76.1.2.3.n) ou A4 (cujo OID é 2.16.76.1.2.4.n), conforme definido no 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação
5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável

Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

C - POLÍTICA-PADRÃO ICP-BRASIL AD-R PARA PARA ASSINATURAS BASEADAS EM CMS / 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. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.3.n+1.

Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de 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 de 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

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

5.1 Período para Assinatura

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas realizadas segundo esta PA **podem ou não** incluir o conteúdo assinado na assinatura digital (*attached, ou detached*).

5.2.1.1.2 Atributos Assinados Obrigatórios

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

i. Id-contentType
ii. Id-messageDigest
    e) id-aa-signingCertificate ou Id-aa-signingCertificateV2
iii. Id-aa-ets-sigPolicyId

5.2.1.1.3 Atributos Não-Assinados Obrigatórios

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

5.2.1.1.4 Referências à Cadeia de Certificação

O atributo signingCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas estruturas *SignerInfo*.

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

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

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

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

5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos Não-Assinados Obrigatórios

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

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

5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável
Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificados ICP-Brasil tipo A3 (cujo OID é 2.16.76.1.2.3.n) ou A4 (cujo OID é 2.16.76.1.2.4.n), conforme definido no 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação
5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do

equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

D-POLÍTICA-PADRÃO ICP-BRASIL AD-C PARA PARA ASSINATURAS BASEADAS EM CMS / CADES

1. Identificador da Política de Assinatura
O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM INFORMAÇÕES 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. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.4.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação
A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura
A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas realizadas segundo esta PA **podem ou não** incluir o conteúdo assinado na assinatura digital (*attached, ou detached*).

5.2.1.1.2 Atributos Assinados Obrigatórios

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

i. Id-contentType
ii. Id-messageDigest
a) id-aa-signingCertificate ou Id-aa-signingCertificateV2
iii. Id-aa-ets-sigPolicyId

5.2.1.1.3 Atributos Não-Assinados Obrigatórios

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 Referências à Cadeia de Certificação

O atributo signingCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas estruturas *SignerInfo*.

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

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no

Anexo 1 do DOC-ICP-15.01.
Deve-se utilizar a codificação MIME para o valor do campo *eContent* da estrutura *EncapsulatedContentInfo*, e o MIME *type* para identificação do formato de apresentação dos dados.
O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.
5.2.1.2 Regras do Verificador

5.2.1.2.1 Atributos Não-Assinados Obrigatórios
Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

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

5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável
Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificados ICP-Brasil tipo A3 (cujo OID é 2.16.76.1.2.3.n) ou A4 (cujo OID é 2.16.76.1.2.4.n), conforme definido no 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento

DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação
5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)

c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

E - POLÍTICA-PADRÃO ICP-BRASIL AD-A PARA PARA ASSINATURAS BASEADAS EM CMS / CADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM INFORMAÇÕES 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. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.5.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituto Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

4. Campo de Aplicação

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 de 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 de 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas realizadas segundo esta PA **podem ou não** incluir o conteúdo assinado na assinatura digital (*attached, ou detached*).

5.2.1.1.2 Atributos Assinados Obrigatórios

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

a) Id-contentType
b) Id-messageDigest
   f) id-aa-signingCertificate ou Id-aa-signingCertificateV2
c) Id-aa-ets-sigPolicyId

5.2.1.1.3 Atributos Não-Assinados Obrigatórios

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-archiveTimestamp

5.2.1.1.4 Referências à Cadeia de Certificação

O atributo signingCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas estruturas *SignerInfo*.

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

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

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

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

5.2.1.2 Regras do Verificador
5.2.1.2.1 Atributos Não-Assinados Obrigatórios
Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

a) id-aa-signatureTimeStampToken
b) id-aa-ets-certificateRefs
c) id-aa-ets-revocationRefs
d) id-aa-ets-certValues
e) id-aa-ets-revocationValues
f) id-aa-ets-archiveTimestamp

5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
5.2.2.1.3 Conjunto de Políticas de Certificado Aceitável
Assinaturas digitais geradas segundo esta Política de Assinatura deverão ser criadas com chave privada associada a certificados ICP-Brasil tipo A3 (cujo OID é 2.16.76.1.2.3.n) ou A4 (cujo OID é 2.16.76.1.2.4.n), conforme definido no 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação

5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

F - POLÍTICA-PADRÃO ICP-BRASIL AD-CP PARA ASSINATURAS BASEADAS EM XMLDSIG / XADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL DE CURTO PRAZO NO FORMATO XMLdSIG versão 1.0.
O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.6.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.6.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituo Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

4. Campo de Aplicação

Neste tipo de assinatura não são armazenados os dados fundamentais para sua validação futura e nem é colocado carimbo de tempo de assinatura. Como não existem condições de garantir a irretratabilidade da assinatura digital, este tipo de assinatura não pode ser usado para arbitragem, em caso de disputa entre signatário e verificador.
Por esse motivo, assinaturas do tipo AD-CP **somente devem ser utilizadas em situações especiais, por exemplo, para serviços transacionais que exigem autenticação de entidades e/ou verificação de integridade.**
Caso seja necessário verficar a assinatura posteriormente devem existam ferramentas adicionais para isso. As informações de validação deverão poder ser obtidas por outras fontes, como o sistema operacional da parte verificadora, por exemplo. Nessas situações, é recomendável que exista um acordo prévio, assinado por ambas as partes, signatário e verificador, concordando com a guarda unilateral desses dados complementares.
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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas regulamentadas por esta PA podem ser realizadas usando uma das seguintes representações:

a) Estrutura assinada com conteúdo digital separado (*detached*);
b) Estrutura assinada com conteúdo digital anexado (*enveloping*);
c) Estrutura assinada incluída no conteúdo digital *(enveloped).*

5.2.1.1.2 Propriedades Assinadas Obrigatórias

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 Propriedades Não-Assinadas Obrigatórias

Não se aplica.

5.2.1.1.4 Referências à Cadeia de Certificação

A propriedade SigningCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas assinaturas XMLDSIG referenciado o mesmo documento por meio do elemento *ds:Reference*.

Para contra-assinaturas, deverão ser empregadas propriedades *xades:CounterSignature*.

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

A identificação do formato de apresentação dos dados deve ser realizada por meio da propriedade *MimeType* da propriedade *DataObjectFormat*.

O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.
5.2.1.2 Regras do Verificador
5.2.1.2.1 Atributos Não-Assinados Obrigatórios
Não se aplica.
5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
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 A3, com OID 2.16.76.1.2.3.n, ou A4, com OID 2.16.76.1.2.4.n, 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
Não se aplica

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os

algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

Infra-Estrutura de Chaves Públicas Brasileira

G - POLÍTICA-PADRÃO ICP-BRASIL AD-T PARA ASSINATURAS BASEADAS EM XMLDSIG / XADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM CARIMBO DE TEMPO NO FORMATO XMLdSIG versão 1.0.
O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.7.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.7.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituo Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de sua geração, pois o carimbo de tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura.
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. Mesmo assim, uma assinatura desse tipo pode ser contestada se houver, por exemplo, o 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas regulamentadas por esta PA podem ser realizadas usando uma das seguintes representações:

a) Estrutura assinada com conteúdo digital separado (*detached*);
b) Estrutura assinada com conteúdo digital anexado (*enveloping*);
c) Estrutura assinada incluída no conteúdo digital *(enveloped).*

5.2.1.1.2 Propriedades Assinadas Obrigatórias

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 Propriedades Não-Assinadas Obrigatórias

a) SignatureTimeStamp

5.2.1.1.4 Referências à Cadeia de Certificação

A propriedade SigningCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

Paralelas: quando a ordem de inserção das assinaturas não é importante; ou

Contra-assinaturas: quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento com a primeira assinatura já presente.

No caso de assinaturas paralelas haverá múltiplas assinaturas XMLDSIG referenciado o mesmo documento por meio do elemento *ds:Reference*.

Para contra-assinaturas, deverão ser empregadas propriedades *xades:CounterSignature*.

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

A identificação do formato de apresentação dos dados deve ser realizada por meio da propriedade *MimeType* da propriedade *DataObjectFormat*.

O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.
5.2.1.2 Regras do Verificador
5.2.1.2.1 Propriedades Não-Assinadas Obrigatórias
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
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
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 A3, com OID 2.16.76.1.2.3.n, ou A4, com OID 2.16.76.1.2.4.n, 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação
5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

H - POLÍTICA-PADRÃO ICP-BRASIL AD-R PARA ASSINATURAS BASEADAS EM XMLDSIG / 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 XMLdSIG versão 1.0.
O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.8.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.8.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituo Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de 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 de 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

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

5.1 Período para Assinatura

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas regulamentadas por esta PA podem ser realizadas usando uma das seguintes representações:

a) Estrutura assinada com conteúdo digital separado (*detached*);
b) Estrutura assinada com conteúdo digital anexado (*enveloping*);
c) Estrutura assinada incluída no conteúdo digital *(enveloped).*

5.2.1.1.2 Propriedades Assinadas Obrigatórias

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

i. DataObjectFormat (em assinaturas do tipo *detached*);
ii. SigningCertificate;
iii. SignaturePolicyIdentifier.

5.2.1.1.3 Propriedades Não-Assinadas Obrigatórias

a) SignatureTimeStamp
b) CompleteCertificateRefs
c) CompleteRevocationRefs
d) SigAndRefsTimeStamp

5.2.1.1.4 Referências à Cadeia de Certificação

A propriedade SigningCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas assinaturas XMLDSIG referenciado o mesmo documento por meio do elemento *ds:Reference*.

Para contra-assinaturas, deverão ser empregadas propriedades *xades:CounterSignature*.

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

A identificação do formato de apresentação dos dados deve ser realizada por meio da propriedade *MimeType* da propriedade *DataObjectFormat*.

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

5.2.1.2 Regras do Verificador

5.2.1.2.1 Propriedades Não-Assinadas Obrigatórias

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

a) SignatureTimeStamp
b) CompleteCertificateRefs
c) CompleteRevocationRefs
d) SigAndRefsTimeStamp

5.2.1.2.2 Regras Adicionais do Verificador

Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários

5.2.2.1 Validação da Cadeia de Certificação

5.2.2.1.1 Raiz Confiável

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

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

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 A3, com OID 2.16.76.1.2.3.n, ou A4, com OID 2.16.76.1.2.4.n, 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.

5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)

Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.

O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo

5.2.3.1 Validação da Cadeia de Certificação

5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

I - POLÍTICA-PADRÃO ICP-BRASIL AD-C PARA ASSINATURAS BASEADAS EM XMLDSIG / XADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM INFORMAÇÕES COMPLETAS NO FORMATO XMLdSIG versão 1.0.
O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.9.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.9.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituo Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas regulamentadas por esta PA podem ser realizadas usando uma das seguintes representações:

a) Estrutura assinada com conteúdo digital separado (*detached*);
b) Estrutura assinada com conteúdo digital anexado (*enveloping*);
c) Estrutura assinada incluída no conteúdo digital *(enveloped).*

5.2.1.1.2 Propriedades Assinadas Obrigatórias

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

1. DataObjectFormat (em assinaturas do tipo *detached*);
2. SigningCertificate;
3. SignaturePolicyIdentifier.

5.2.1.1.3 Propriedades Não-Assinadas Obrigatórias

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

5.2.1.1.4 Referências à Cadeia de Certificação

A propriedade SigningCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas assinaturas XMLDSIG referenciado o mesmo documento por meio do elemento *ds:Reference*.

Para contra-assinaturas, deverão ser empregadas propriedades *xades:CounterSignature*.

Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.

A identificação do formato de apresentação dos dados deve ser realizada por meio da propriedade *MimeType* da propriedade *DataObjectFormat*.
O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.
5.2.1.2 Regras do Verificador
5.2.1.2.1 Propriedades Não-Assinadas Obrigatórias
Caso não tenham sido incluídas pelo signatário, as seguintes propriedades DEVEM ser incluídas pelo verificador:

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

5.2.1.2.2 Regras Adicionais do Verificador
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
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 A3, com OID 2.16.76.1.2.3.n, ou A4, com OID 2.16.76.1.2.4.n, 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.

O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo

5.2.3.1 Validação da Cadeia de Certificação

5.2.3.1.1 Raiz Confiável

A validação da assinatura constante no carimbo de 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

O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).

5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável

Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.

5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)

Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.

O método mínimo aplicável deve ser a verificação por LCR.

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 de Tempo

Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos

Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos

Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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.

J - POLÍTICA-PADRÃO ICP-BRASIL AD-A PARA ASSINATURAS BASEADAS EM XMLDSIG / XADES

1. Identificador da Política de Assinatura

O nome desta Política de Assinatura é POLÍTICA ICP-BRASIL PARA ASSINATURA DIGITAL COM INFORMAÇÕES DE ARQUIVAMENTO NO FORMATO XMLdSIG versão 1.0.
O *Object Identifier* (OID) desta PA, atribuído pelo ITI é: 2.16.76.1.7.1.10.1. Novas versões desta política, se criadas, receberão OID diferenciado, do tipo 2.16.76.1.7.1.10.n+1.
Esta PA está protegida contra alterações indevidas por meio da publicação, no repositório da AC Raiz da ICP-Brasil (http://www.iti.gov.br/twiki/bin/view/Certificacao/RepositoriodaACRaiz), do seu conteúdo assinado digitalmente por chave privada associada a certificado digital do Instituto Nacional de Tecnologia da Informação, utilizando algoritmo Sha1withRSAEncryption(1 2 840 113549 1 1 5).

2. Data da Criação

A data de criação desta PA é 31.10.2008.

3. Entidade Criadora da Política de Assinatura

A entidade criadora desta PA é o Instituo Nacional de Tecnologia da Informação (ITI). Ela pode ser utilizada por qualquer pessoa física ou jurídica, órgão de governo ou outro tipo de entidade, sem restrições.

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 de 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 de 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

Esta PA terá validade desde a data de publicação até 31.12.2010.

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

As assinaturas regulamentadas por esta PA podem ser realizadas usando uma das seguintes representações:

a) Estrutura assinada com conteúdo digital separado (*detached*);
b) Estrutura assinada com conteúdo digital anexado (*enveloping*);
c) Estrutura assinada incluída no conteúdo digital *(enveloped).*

5.2.1.1.2 Propriedades Assinadas Obrigatórias

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 Propriedades Não-Assinadas Obrigatórias

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

5.2.1.1.4 Referências à Cadeia de Certificação

A propriedade SigningCertificate deve conter apenas referência ao certificado do signatário, por meio do Identificador Serial do Emissor e do *hash* do certificado.

5.2.1.1.5 Valores da Cadeia de Certificação

Não se aplica.

5.2.1.1.6 Regras Adicionais do Signatário

Na utilização de múltiplas assinaturas, todas elas devem empregar os mesmos algoritmos definidos no item 5.2.5. As formas possíveis de múltiplas assinaturas são:

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

No caso de assinaturas paralelas haverá múltiplas assinaturas XMLDSIG referenciado o mesmo documento por meio do elemento *ds:Reference*.

Para contra-assinaturas, deverão ser empregadas propriedades *xades:CounterSignature*.
Para a indicação do tipo de comprometimento devem ser empregados aqueles tipos definidos no Anexo 1 do DOC-ICP-15.01.
A identificação do formato de apresentação dos dados deve ser realizada por meio da propriedade *MimeType* da propriedade *DataObjectFormat*.
O signatário é responsável por se certificar que o documento assinado não contém qualquer conteúdo dinâmico capaz de modificar o resultado do documento visualizado ao longo do tempo, como, por exemplo, quantias ou sentenças que se alteram após certa data.
5.2.1.2 Regras do Verificador
5.2.1.2.1 Propriedades Não-Assinadas Obrigatórias
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
Caso esteja presente mais de uma assinatura, aposta ao mesmo documento assinado, deve-se validar cada assinatura encontrada independentemente, segundo o item 5.2.1.1

5.2.2 Condições de Confiabilidade dos Certificados dos Signatários
5.2.2.1 Validação da Cadeia de Certificação
5.2.2.1.1 Raiz Confiável
A validação deve ser feita tomando como ponto de confiança os certificados da AC-Raiz da ICP-Brasil, disponíveis em 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do signatário e a AC-Raiz é 2 (dois).
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 A3, com OID 2.16.76.1.2.3.n, ou A4, com OID 2.16.76.1.2.4.n, 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.
5.2.2.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do signatário quanto para os certificados das Autoridades Certificadoras da cadeia de certificação a verificação do status dos certificados deve ser realizada através de LCRs

(Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.

5.2.3 Condições de Confiabilidade do Carimbo de Tempo
5.2.3.1 Validação da Cadeia de Certificação
5.2.3.1.1 Raiz Confiável
A validação da assinatura constante no carimbo de 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
O número máximo de certificados de ACs, no caminho de certificação, entre o certificado do equipamento emissor do carimbo de tempo (SCT) e a AC-Raiz é 2 (dois).
5.2.3.1.3 Conjunto de Políticas de Certificado Aceitável
Os carimbos de tempo deverão ser criados com chave privada associada a certificados ICP-Brasil tipo T3 (cujo OID é 2.16.76.1.2.303.n) ou T4 (cujo OID é 2.16.76.1.2.304.n), 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.
5.2.3.1.6 Forma de Verificação do Status da Cadeia de Certificação (Revogação)
Tanto para o certificado do SCT quanto para os certificados das Autoridades Certificadoras da cadeia de certificação, a verificação do status deve ser realizada através de LCRs (Lista de Certificados Revogados) em conformidade com o perfil de LCR definido no documento DOC-ICP-04 ou através de consultas OCSP (*Online Certificate Status Protocol*) em conformidade com a RFC 2560 ou algum outro método presente em DOC-ICP-04.
O método mínimo aplicável deve ser a verificação por LCR.
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 de Tempo
Não se aplica.

5.2.4 Condições de Confiabilidade dos Atributos
Não se aplica.

5.2.5 Conjunto de Restrições de Algoritmos
Os processos para criação e verificação de assinaturas segundo esta PA devem utilizar os algoritmos:

a) Sha1(1 3 14 3 2 26)
b) Sha1withRSAEncryption(1 2 840 113549 1 1 5)
c) RsaEncryption(1 2 840 113549 1 1 1) com minKeyLength=1024

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 2

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 PA aprovadas e definir processos de aprovação, 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 PA aprovadas, o que inclui: a forma de aprovação e de publicação de uma PA e os procedimentos a serem adotados em caso de término da validade, prorrogação da validade e revogação de PA aprovadas.

2. Administração e ciclo de vida de uma PA

2.1 PA 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. Comunicação entre as partes

3.1 Políticas de assinatura são aprovadas pela AC Raiz da ICP-Brasil em nome de uma pessoa

física ou jurídica, doravante designada Entidade Criadora de Política de Assinatura (ECP).

3.2 Toda e qualquer comunicação entre a ECP e a AC Raiz da ICP-Brasil, no que tange aos processos regulamentados por este normativo, DEVE ser formalizada mediante o envio de mensagem de correio eletrônico, que DEVE conter assinatura digital baseada em certificado digital emitido no âmbito da ICP-Brasil.

3.3 No caso das mensagens eletrônicas enviadas da ECP para a AC Raiz, o certificado digital referido no parágrafo 3.2 DEVE ser da pessoa física interessada na aprovação da PA ou, em se tratando de solicitação formulada por pessoa jurídica, DEVE ter como titular a própria pessoa jurídica interessada e como responsável uma pessoa física que será indicada, conforme definido no parágrafo 4.1.1.a

3.4 No caso das mensagens eletrônicas enviadas da AC Raiz à ECP, o certificado digital referido no parágrafo 3.2 DEVE ser de pessoa jurídica, tendo como seu titular a AC Raiz.

3.5 Todas mensagens eletrônicas enviadas pela ECP à AC Raiz DEVEM ser destinadas ao endereço eletrônico normalizacao@iti.gov.br.

3.6 Todas mensagens eletrônicas enviadas pela AC Raiz à ECP serão destinadas aos endereços eletrônicos do responsável definido no parágrafo 4.1.1.a.

4. Aprovação de uma PA

Os procedimentos administrativos a serem empreendidos em todos os processos de aprovação de Políticas de Assinatura no âmbito da ICP-Brasil DEVEM observar a forma definida neste documento.

4.1 Formalização do pedido

4.1.1 Um pedido para aprovação de uma PA e para sua integração na LPA DEVE conter:

a) Dados de identificação básicos do requerente e do responsável, em se tratando de solicitação formulada por pessoa jurídica;
b) Política de Assinatura codificada em linguagem humana, em conformidade com o documento DOC-ICP-15.03;
c) Resumo criptográfico da política de assinatura, para os dois formatos citados acima;
d) Razão pela qual a PA deve ser aprovada;
e) Propósito de uso da Política de Assinatura;
f) Restrições Básicas;
g) Início e fim de validade esperados da PA.

4.2 Organização dos processos

4.2.1 Para cada solicitação de aprovação de uma PA corresponderá, individualmente, um processo administrativo com numeração própria e independente.
4.2.2 Para efeito de deferimento ou indeferimento das solicitações, os processos administrativos são independentes entre si, não implicando os resultados de uns nos dos outros.
4.2.3 Todas as mensagens eletrônicas trocadas entre a ECP e a AC Raiz serão impressas, autenticadas por servidor público e integradas aos autos dos respectivos processos administrativos.

4.3 Avaliação dos pedidos

4.3.1 Depois de analisar o pedido, sua validade e conformidade com os padrões e a legislação aplicável, a AC Raiz irá emitir uma decisão sobre a aprovação ou desaprovação de uma PA, juntamente com a justificativa da sua decisão.
4.3.2 É possível aplicar um recurso contra essa decisão, conforme procedimentos descritos na seção 8.
4.3.3 Uma PA, após a aprovação, será publicada no repositório da AC Raiz da ICP-Brasil e incluída na nova LPA, que será assinada por um certificado digital emitido especificamente para a assinatura de LPA.

5. Publicação da PA e da LPA

5.1 Os arquivos com as PAs aprovadas são publicados no repositório da AC Raiz da ICP-Brasil e são utilizados para a criação da LPA.

5.2 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.

5.3 A LPA é atualizada pela AC Raiz **mensalmente**, no primeiro dia útil de cada mês, e contém em seu corpo a data da sua próxima atualização.

5.4 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.

5.5 A LPA é escrita com base em um XML Schema e traz, para cada PA aprovada, os seguintes dados:

iv. uma breve descrição da política: os aplicativos assinadores poderão exibir essa informação para que o usuário decida qual PA empregar;
v. período de validade da Política;
vi. URLs da PA em formato textual e processável por máquina (XML/DER);
vii. resultados *hash* dos arquivos da PA, no formato textual e processável por máquina (XML/DER).

5.6 Uma PA aprovada é válida pelo período indicado no campo validade, se ela não tiver sido revogada. Nesse caso, seu prazo de validade será reduzido na próxima LPA a ser publicada e assinada pela AC Raiz.

6. Prorrogação da validade de uma PA aprovada

6.1 A política de assinatura PODE ser publicada por um período ilimitado, caso o campo *Validade* esteja setado como NULO.

6.2 Se a validade de uma PA aprovada estiver limitada a um certo período, ela poderá ser prorrogada antes da expiração, a pedido da ECP**,** usando os mesmos procedimentos para aprovação descritos na seção anterior.

6.3 Para que a prorrogação da validade seja aprovada, é preciso que não tenham sido encontradas fraquezas na PA, as quais não sejam mais aceitáveis para o período de validade seguinte.

6.4 A prorrogação é 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.

7. Revogação de uma PA

7.1 PAs aprovadas PODEM ser revogadas pela AC Raiz da ICP-Brasil a qualquer tempo, a pedido da ECP. A AC Raiz também PODE revogar uma PA aprovada a pedido de outra pessoa física ou jurídica, nos casos em que determinada PA não deveria ter sido aprovada ou por motivos de segurança ou ainda em razão de outros conflitos e problemas legais.

7.2 Um pedido de revogação de uma PA aprovada DEVE conter:

a) Dados de identificação básicos do requerente;
b) Dados de identificação da política de assinatura a ser revogada;
c) Razão pela qual a política de assinatura deve ser revogada.

7.3 Depois de analisar o pedido e sua conformidade com as normas e padrões da ICP-Brasil, a AC Raiz irá emitir uma decisão sobre a rejeição do pedido ou sobre a revogação da Política de Assinatura, juntamente com a justificativa para sua decisão.

7.4 É possível aplicar um recurso contra essa decisão, conforme procedimentos descritos na seção 8.

7.5 Em caso de revogação de uma PA aprovada, ela será publicada no site da AC Raiz da ICP-Brasil como revogada e sua validade, constante na LPA, será encurtada até o momento da sua revogação. Uma nova LPA será publicada e assinada pelo certificado emitido para assinatura de

LPA.

7.6 A nova LPA irá conter o momento de revogação da validade de uma PA aprovada, o qual será o instante imediatamente após o momento da assinatura e publicação da nova LPA.

8. Recursos

8.1 Caberá recurso quanto ao indeferimento de pedido de aprovação ou revogação de PA, em até 20 (vinte) dias úteis após a data da notificação da decisão da AC Raiz.

8.2 O recurso será dirigido ao Diretor de Auditoria, Fiscalização e Normalização do ITI e DEVE incluir:

a) dados de identificação básicos do requerente;
b) resumo criptográfico da política de assinatura;
c) o número do processo administrativo correspondente à solicitação;
d) a justificativa para o recurso;
e) discriminação da correspondente documentação e material apresentados comprobatórios dos fatos justificados.

8.3 O recurso será analisado pela Diretoria de Auditoria, Fiscalização e Normalização do ITI (DAFN/ITI), que PODE, se necessário, formular outras exigências ao solicitante, que DEVEM ser cumpridas no prazo estabelecido.

8.4 Caso a DAFN/ITI decida pelo indeferimento do recurso, o processo será submetido ao Diretor-Presidente do ITI, em segunda instância, que PODE:

a) acatar as justificativas apresentadas no recurso, o que implicará a observância do disposto nos parágrafos 11.6 e 11.7, conforme o caso; ou
b) ratificar o indeferimento do recurso, mediante notificação ao solicitante.

8.5 A decisão do recurso, em segunda instância, é final e irrecorrível na esfera administrativa.

8.6 Antes de sua decisão, o Diretor-Presidente do ITI PODE encaminhar o processo à Procuradoria Federal Especializada do ITI para elaboração de manifestação jurídica, que subsidie sua decisão.

9. Procedimentos para criação e verificação da LPA

9.1 A estrutura do arquivo LPA é a seguinte:

a) campo **NOME**: contém o nome da PA, conforme consta no campo *IDENTIFICADOR DA POLÍTICA DE ASSINATURA*, existente no corpo da PA;
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 **VALIDADE**: contém a data de fim de validade da PA, em Generlized Time;
d) campo **URL TEXTUAL**: contém a URL do repositório da AC Raiz da ICP-Brasil onde está publicada a PA aprovada, em formato textual;
e) campo **URL MAQUINA**: contém a URL do repositório da AC Raiz da ICP-Brasil onde está publicada a PA aprovada, em formato DER ou XML;
f) campo **HASH TEXTUAL**: contém o *hash* da PA em formato textual;
g) campo **HASH MAQUINA**: contém o hash da PA codificada em DER ou XML.

9.2 A data da revogação da política de assinatura indicada no campo VALIDADE, para as PA aprovadas que não tenham sido revogadas, DEVE corresponder à data indicada no campo Validade no arquivo da PA aprovada. Em caso de revogação de qualquer PA aprovada, o campo VALIDADE DEVE conter a data de revogação da PA, ao invés da data indicada no campo Validade constante do arquivo da PA aprovada.

9.3 A LPA DEVE ser verificada em relação ao momento atual e DEVE conter sempre todas as PAs aprovadas. Isso significa que também aquelas que tenham expirado ou tenham sido revogadas DEVEM ter a data da sua expiração ou revogação indicada no campo AVISO.

9.4 Esta propriedade da LPA é muito importante especialmente para verificação de Assinaturas Digitais ICP-Brasil criadas no passado por meio de PA aprovadas que tenham sido válidas por um período, mas posteriormente tenham sido revogadas.

9.5 Os campos com resumos *hash* DEVEM conter um algoritmo seguro, compatível com o documento “PADRÕES E ALGORTIMOS CRIPTOGRÁFICOS DA ICP-BRASIL – DOC-ICP-01.01”.

9.7 Na verificação da LPA em relação ao momento atual, a aplicação que realiza a verificação tenta obter a LCR atual (OCSP) a ser utilizada para verificação da validade do certificado do signatário da LPA.

9.8 Os dados contidos na LPA PODEM ser declarados como válidos apenas para o momento da emissão da LCR atual (OCSP) para verificação da validade do certificado do signatário da LPA.

9.8 Assim, uma plena verificação da validade da Assinatura Digital ICP-Brasil DEVE ser feita apenas no que diz respeito a períodos de tempo mais antigos ou iguais ao momento da emissão da LCR atual (OCSP), que foi utilizada para verificar a validade do certificado do signatário da LPA.

9.9 Uma descrição mais detalhada dos campos da PA e do processo de controle dos campos individuais na verificação das Assinaturas Digitais ICP-Brasil está no documento "REQUISITOS MÍNIMOS PARA POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL - DOC-ICP-15.03”

10. A validade da Assinatura Digital ICP-Brasil de um documento eletrônico

10.1 A validade da Assinatura Digital ICP-Brasil de um documento é sempre determinada no que

diz respeito ao momento da assinatura do documento.

10.2 O momento da assinatura do documento é um dentre:

1. o tempo constante de um carimbo de tempo emitido sobre a assinatura do documento;
2. o tempo a partir de um registro seguro de auditoria contendo o *hash* da assinatura;
3. um tempo próximo ao momento de verificação da LCR (OCSP) que permite validar o certificado do signatário do documento. É necessário também obter as LCRs (OCSP) para verificação de todo o caminho de certificação até o certificado confiável, sendo que todas elas devem ter sido emitidas ao mesmo tempo ou após a LCR (OCSP) relativa ao certificado do signatário.

10.3 Se a PA aprovada utilizada é válida com relação ao momento da assinatura e se os outros requisitos legais em relação à validade das Assinaturas Digitais ICP-Brasil também são atendidos, é possível declarar que a Assinatura Digital ICP-Brasil do documento é válida.

10.4 No caso de a PA aprovada ser inválida com relação ao momento da assinatura do documento, é necessário declarar a Assinatura Digital ICP-Brasil do documento como inválida.

11 - Exemplos de LPA

A tabela 1 demonstra uma lista de PA aprovadas

Tabela 1 - Lista de PA aprovadas (PA01, PA02 e PA03)

	Nome	Aplicacao	Validade	URL textual	URL máquina	hash textual	hash máquina
1.	Política de assinatura-padrão ICP-Brasil de uso restrito	Aplicação X	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA01.txt	www.acraiz.icpbrasil.gov.br/LPA/PA01.der	Hash T1	Hash M1
2.	Política de assinatura-padrão ICP-Brasil com carimbo de tempo	Aplicação Y	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA02.txt	www.acraiz.icpbrasil.gov.br/LPA/PA02.der	Hash T2	Hash M2
3.	Política de assinatura padrão ICP-Brasil com referências para validação	Aplicação Z	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA02.txt	www.acraiz.icpbrasil.gov.br/LPA/PA02.der	Hash T3	Hash M3

A tabela 2 demonstra a revogação de uma PA aprovada na terceira linha e o momento da revogação na coluna “Validade”.

Tabela 2 - Lista de PA aprovadas com uma PA revogada (PA03)

	Descrição	**Aplicacao**	**Validade**	**URL textual**	**URL máquina**	**hash textual**	**hash máquina**
1.	Política de assinatura-padrão ICP-Brasil de uso restrito	Aplicação X	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA01.txt	www.acraiz.icpbrasil.gov.br/LPA/PA01.der	Hash T1	Hash M1
2.	Política de assinatura-padrão ICP-Brasil com carimbo de tempo	Aplicação Y	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA02.txt	www.acraiz.icpbrasil.gov.br/LPA/PA02.der	Hash T2	Hash M2
3.	Política de assinatura padrão ICP-Brasil com referências para validação	Aplicação Z	**20081013**000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA03.txt	www.acraiz.icpbrasil.gov.br/LPA/PA03.der	Hash T3	Hash M3

Uma nova PA aprovada é adicionada na LPA

Tabela 3 - Lista de PA aprovadas com adição de uma nova PA (PA04)

	Descrição	Aplicacao	Validade	URL textual	URL máquina	hash textual	hash máquina
1.	Política de assinatura-padrão ICP-Brasil de uso restrito	Aplicação X	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA01.txt	www.acraiz.icpbrasil.gov.br/LPA/PA01.der	Hash T1	Hash M1
2.	Política de assinatura-padrão ICP-Brasil com carimbo de tempo	Aplicação Y	20150520000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA02.txt	www.acraiz.icpbrasil.gov.br/LPA/PA02.der	Hash T2	Hash M2
3.	Política de assinatura padrão ICP-Brasil com referências para validação	Aplicação Z	20081013000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA03.txt	www.acraiz.icpbrasil.gov.br/LPA/PA03.der	Hash T3	Hash M3
4.	Política de assinatura-padrão ICP-Brasil com referências completas	Aplicação W	20151020000000Z	www.acraiz.icpbrasil.gov.br/LPA/PA04.txt	www.acraiz.icpbrasil.gov.br/LPA/PA04.der	Hash T4	Hash M4