Infra-Estrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL

DOC-ICP-15.01
Versão 1.0

Sumário

1. INTRODUÇÃO

1.1 A utilização de formatos padronizados de assinatura digital no âmbito da ICP-Brasil é essencial para a confiabilidade e credibilidade do processo de criação e validação da assinatura, Sua não utilização compromete a interoperabilidade e pode acarretar a utilização de formatos de assinatura inadequados para o tipo de documento ou para o tipo de compromisso que está sendo selado com aquela assinatura

1.2 Este documento 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).

1.3 Ele regulamenta os requisitos a serem observados nos processos que tratam de assinaturas digitais na ICP-Brasil, quanto a:

a) algoritmos e parâmetros desses algoritmos para criação de uma assinatura digital ICP-Brasil;

b) o formato e a maneira de criar uma assinatura digital ICP-Brasil;

c) procedimentos para verificação e condições para validação de uma assinatura digital ICP-Brasil.

2. TERMINOLOGIA

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

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

2.1.2 **NÃO DEVE (ND)** - Esta expressão, ou o termo “PROIBIDO¨ significa que a definição é uma proibição absoluta na especificação.

2.1.3 **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.

2.1.4 **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.

2.1.5 **PODE (P)** - Esta palavra, ou o adjetivo "OPCIONAL", significa que é um item verdadei-

ramente 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.)

3. DEFINIÇÕES

Para os propósitos deste documento, aplicam-se as seguintes definições:

3.1 **Assinatura Digital ICP-Brasil** é a assinatura eletrônica que:

a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;

b) seja produzida por dispositivo seguro de criação de assinatura;

c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subseqüente neste seja plenamente detectável; e

d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.

3.2 **Assinatura eletrônica -** o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria

3.3 **BASE 64 –** é um método de codificação de dados. Permite transformar dados binários (seqüência de bytes) em dados ASCII imprimíveis (texto). Assim, possibilita que dados originalmente no formato binário, após a transformação, possam ser transmitidos através de meios que não permitem dados binários. Permite também que dados binários sejam armazenados na forma de seqüências ASCII. O conjunto de caracteres ASCII é constituído por 64 caracteres ([A-Za-z0-9], "/" e "+") que deram origem ao seu nome [26].

3.4 **Cadeia de certificação -** uma série hierárquica de certificados assinados por sucessivas autoridades certificadoras. A cadeia de certificação compreende o certificado da entidade final, assinado por uma AC, e zero ou mais certificados de ACs assinador por outras ACs, até o certificado de confiança, porém não incluindo este conforme descrito a RFC 5280 [27].

A figura 3.1 ilustra o conceito de cadeia de certificação.

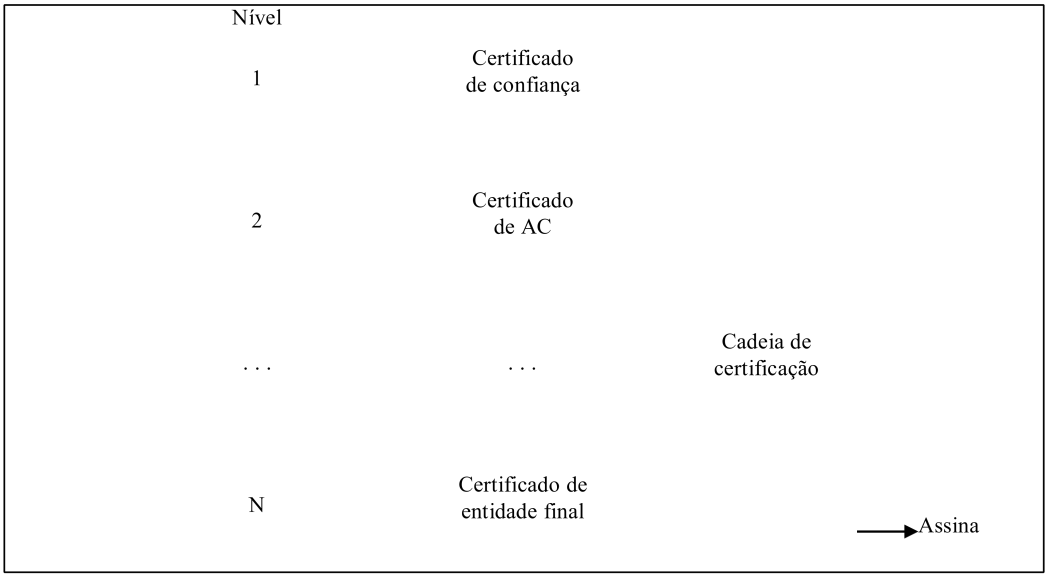

Figura 3.1 – Conceito de cadeia de certificação.

A figura 3.2 ilustra um exemplo de uma cadeia de certificação de um certificado ICP-Brasil de um signatário de um documento.

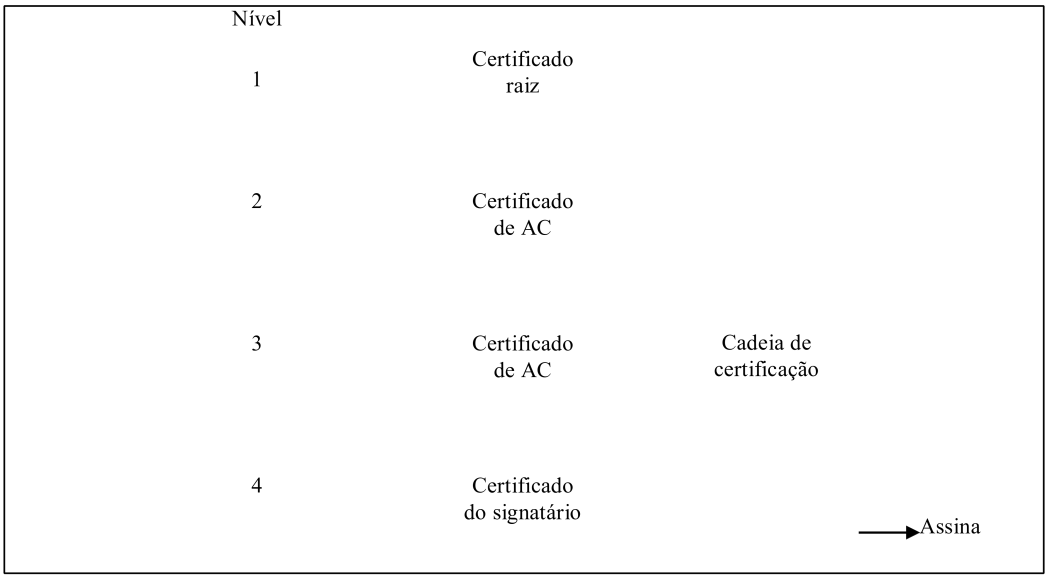

Figura 3.2 – Exemplo de uma cadeia de certificação da ICP-Brasil

3.5 **CAdES -** CMS Advanced Electronic Signature - uma extensão do padrão CMS (que é usado para descrever estrutura para armazenamento de conteúdos assinados digitalmente, em formato ASN-1), que incorpora elementos com vistas a prover as assinaturas digitais CMS de informações que permitam sua validação a mais longo prazo.

3.6 **Carimbo do tempo -** documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora.

3.7 **Chave de criação de assinatura -** o conjunto único de dados eletrônicos, tal como chaves criptográficas privadas, utilizado para a criação de uma assinatura eletrônica.

3.8 **Chave de verificação de assinatura -** o conjunto de dados eletrônicos, tal como chaves criptográficas públicas, utilizado para a verificação de uma assinatura eletrônica.

3.9 **Componentes de aplicação de assinatura -** os produtos físicos (hardware) e lógicos (software) que:

a) vinculem ao documento eletrônico processo de produção e verificação de assinaturas eletrônicas; ou

b) verifiquem assinaturas eletrônicas e confiram certificados, disponibilizando os resultados.

3.10 **Conteúdo digital -** um documento eletrônico sobre o qual se realiza uma assinatura digital.

3.11 **Dispositivo seguro de criação de assinaturas -** o dispositivo físico (hardware) e lógico (software) destinado a viabilizar o uso da chave de criação de assinatura que, na forma do regulamento:

a) assegure a confidencialidade da chave de criação de assinatura;

b) inviabilize a dedução dessa chave a partir de outros dados;

c) permita ao titular proteger a chave de criação de assinatura, de modo eficaz contra o seu uso por terceiros;

d) proteja a assinatura eletrônica contra falsificações; e

e) não modifique o documento eletrônico a ser assinado.

3.12 **Documento eletrônico -** uma seqüência de bits elaborada mediante processamento eletrônico de dados, destinada a reproduzir uma manifestação do pensamento ou um fato.

3.13 **Função hash -** uma transformação matemática que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor – conhecido como resultado *hash* ou resumo criptográfico – de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou).

3.14 **Identificador da política de assinatura -** dados que identificam de forma unívoca uma política de assinatura, compostos por um identificador (OID) e o resultado *hash* da política.

3.15 **Resultado hash** - um valor calculado a partir de um documento eletrônico com a ajuda de uma função hash.

3.16 **XAdES -** XML Advanced Electronic Signature - uma extensão do padrão XMLdSig (que é usado para descrever estrutura para armazenamento de conteúdos assinados digitalmente, em formato XML), que incorpora elementos com vistas a prover as assinaturas digitais XMLdSig de informações que permitam sua validação a mais longo prazo.

4. REQUISITOS TÉCNICOS PARA ASSINATURAS DIGITAIS NA ICP-BRASIL

As diretrizes constantes nesta seção DEVEM ser obrigatoriamente observadas pelas Autoridades Certificadoras, Autoridades de Registro, Prestadores de Serviço de Suporte, Empresas de Auditoria Independente, Laboratórios de Ensaio de Auditoria e outras entidades credenciadas ou cadastradas na ICP-Brasil, para geração e verificação de assinaturas digitais em documentos eletrônicos que tenham relação com os processos que tais entidades executam, no âmbito da ICP-Brasil, como: assinatura de logs, relatórios etc.

4.1 Formatos de assinatura digital admitidos na ICP-Brasil

4.1.1 Uma assinatura digital ICP-Brasil DEVE ter um dos seguintes formatos:

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 informações completas (AD-C);

e) assinatura digital com informações para arquivamento (AD-A); ou

f) uma combinação dos formatos citados nos subitens a) até e).

4.1.2 As figuras a seguir ilustram os formatos de assinatura acima descritos:

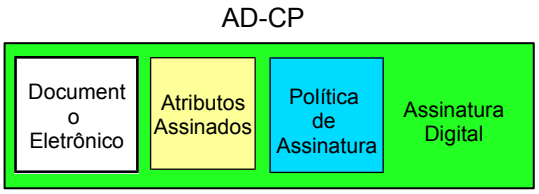

Figura 4.1 – Assinatura digital de curto prazo (AD-CP)

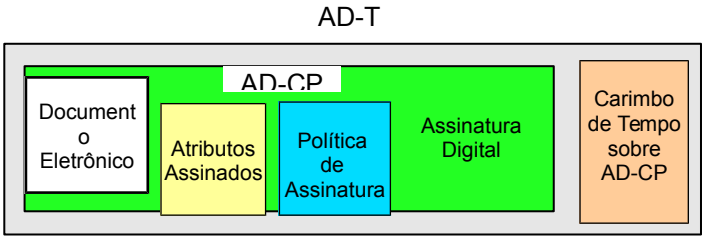

Figura 4.2 – Assinatura digital com carimbo do tempo (AD-T)

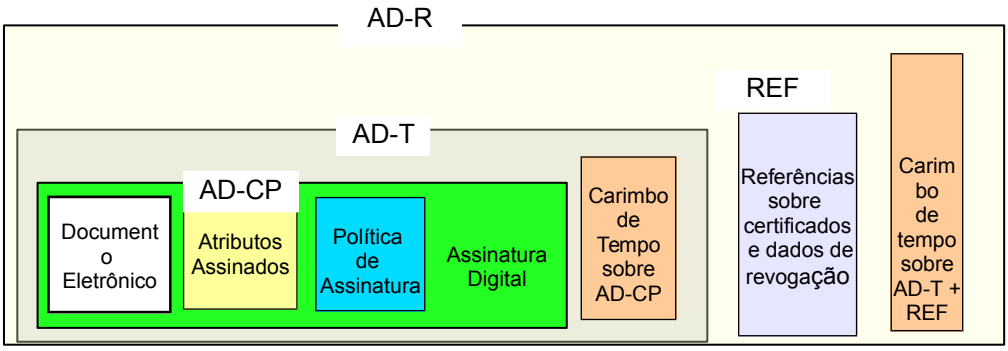

Figura 4.3 – Assinatura digital com referências para validação (AD-R)

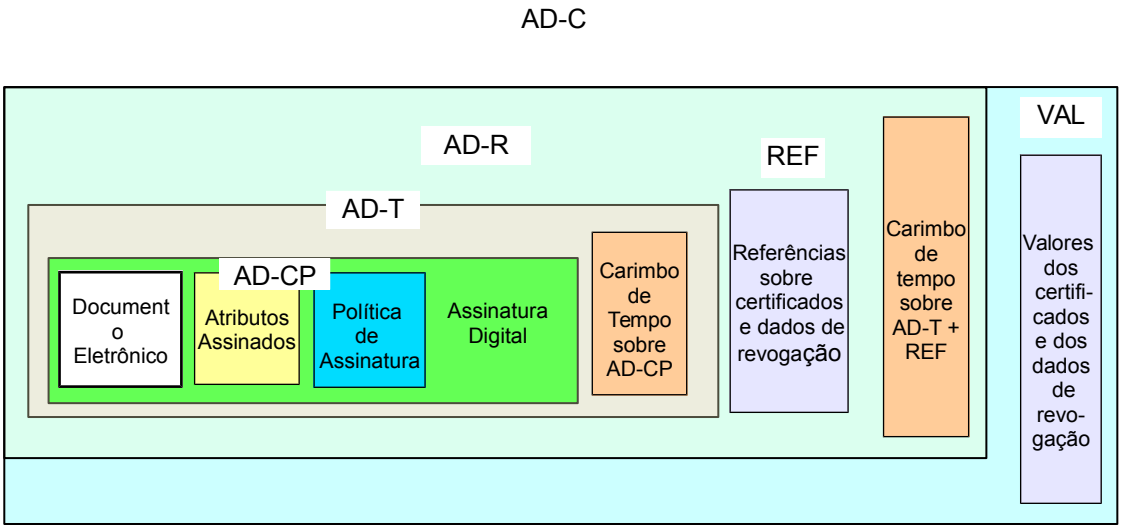

Figura 4.4 – Assinatura digital com informações completas (AD-C)

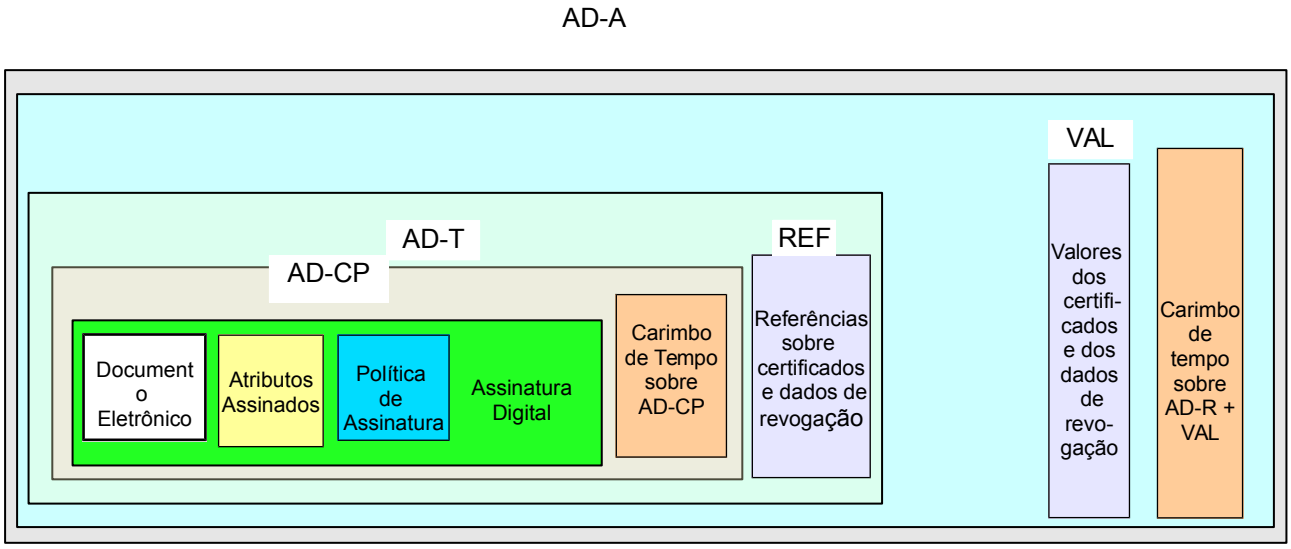

Figura 4.5 – Assinatura digital com informações para arquivamento (AD-A)

4.1.3 Uma **assinatura digital ICP-Brasil de curto prazo (AD-CP)** contém:

a) o identificador da política de assinatura usada para criação e verificação de uma dada assinatura digital ICP-Brasil;

b) dados da assinatura, os quais o signatário incluiu na assinatura digital ICP-Brasil (por exemplo: instante de criação da assinatura);

c) assinatura digital, que foi criada com base em:
   i. um resultado *hash* do documento assinado;
   ii. um identificador de política de assinatura;
   iii. dados incluídos pelo signatário na assinatura digital.

4.1.4 No mínimo os seguintes campos assinados DEVEM constar das assinaturas digitais ICP-Brasil:

a) Assinaturas com base no padrão CAdES

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

b) Assinaturas com base no padrão XAdES
i. DataObjectFormat (para assinaturas do tipo *detached*)
ii. SigningCertificate
iii. SignaturePolicyIdentifier

4.1.5 Uma **assinatura digital ICP-Brasil com carimbo do tempo (AD-T)** tem a forma de uma assinatura digital ICP-Brasil de curto prazo (AD-CP) na qual foi acrescentado ou logicamente conectado, por algum meio, um carimbo do tempo emitido por uma Autoridade de Carimbo do Tempo credenciada na ICP-Brasil, criado com base nos procedimentos aprovados pelo documento DOC-ICP-12 [20].

4.1.6 Uma **assinatura digital ICP-Brasil com referências para validação (AD-R)** tem a forma de uma assinatura digital ICP-Brasil com carimbo do tempo (AD-T) na qual foram acrescentadas referências sobre todos os certificados de chave pública e sobre todas as LCR ou respostas OCSP que são necessários para a validação daquela assinatura. Sobre esses dados é acrescentado ou logicamente conectado outro carimbo do tempo, emitido por uma Autoridade de Carimbo do Tempo credenciada na ICP-Brasil.

4.1.7 Uma **assinatura digital ICP-Brasil com informações completas (AD-C)** tem a forma de uma assinatura digital ICP-Brasil com referências para validação (AD-R) à qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com os itens 4.2.3.1 e 4.2.3.2 deste documento.

4.1.8 Uma **assinatura digital ICP-Brasil com informações para arquivamento (AD-A)** tem a forma de uma assinatura digital ICP-Brasil com carimbo do tempo (AD-T) à qual foram acrescentadas referências de validação e todos os dados necessários para validação da assinatura, de acordo com os itens 4.2.3.1 e 4.2.3.2 deste documento. Um carimbo do tempo, emitido por uma Autoridade de Carimbo do Tempo credenciada na ICP-Brasil, é criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

4.2 Requisitos técnicos para geração e validação de assinaturas digitais ICP-Brasil

4.2.1 Requisitos Gerais

4.2.1.1 Os processos relacionados ao ciclo de vida de uma assinatura digital DEVEM ser capazes de identificar e manipular certificados digitais emitidos no âmbito da ICP-Brasil, bem como suas extensões, campos e "campos específicos ICP-Brasil".

4.2.1.2 Nos processos relacionados ao ciclo de vida da assinatura digital, por meios técnicos e procedimentais, os seguintes requisitos DEVEM ser atendidos:

a) a assinatura digital DEVE estar protegida contra falsificação;

b) os conteúdos digitais assinados DEVEM ser protegidos contra alterações;

c) qualquer componente de software ou hardware utilizado não DEVE provocar alterações no conteúdo digital;

d) qualquer componente de *software* ou *hardware* utilizado NÃO DEVE impedir que o conteúdo digital seja apresentado e visualizado antes e depois de cada um dos processos relacionados ao ciclo de vida da assinatura digital.

4.2.2 Geração de uma assinatura digital ICP-Brasil

4.2.2.1 A aposição de uma assinatura digital ICP-Brasil DEVE referir-se inequivocamente a uma pessoa física ou jurídica e ao documento eletrônico ao qual é aposta.

4.2.2.2 A assinatura digital ICP-Brasil será reconhecida quando aposta durante o prazo de validade do certificado em que está baseada e respeitadas as restrições indicadas neste.

4.2.2.3 A assinatura digital ICP-Brasil aposta após a expiração ou revogação do certificado em que está baseada ou que não respeite as restrições indicadas neste equivale à ausência de assinatura.

4.2.2.4 A assinatura de documentos eletrônicos com certificados ICP-Brasil exige o uso de componentes de aplicação de assinatura que indiquem a produção de uma assinatura digital ICP-Brasil e permitam a identificação do documento a que a assinatura se refere.

4.2.2.5 Os componentes de aplicação de assinatura conterão mecanismos que demonstrem:

a) a que documento a assinatura se refere;

b) se o documento não foi modificado;

c) a que titular de certificado está vinculado o documento; e

d) o conteúdo do certificado em que está baseada a assinatura.

4.2.2.6 A menos que explicitamente mencionado, as regras definidas nesta seção referentes ao

processo de geração de assinatura digital aplicam-se à geração de assinaturas digitais simples, co-assinaturas digitais e contra-assinaturas digitais.

4.2.2.7 Quando aplicável, os requisitos para considerar um certificado digital válido PODEM ser verificados antes da geração da assinatura digital. Entretanto, caso haja algum problema ou não conformidade com o certificado digital do signatário que foi verificado, exceto no caso de expiração, cabe ao contexto, aplicação ou negócio decidir se o processo de geração da assinatura digital vai ser executado ou não.

4.2.2.8 Caso seja o desejo do signatário, o processo de geração de assinatura digital DEVE permitir que o conteúdo digital seja visualizado antes e depois da realização da(s) assinatura(s) digital(is). Além disso, o conteúdo digital visualizado DEVE corresponder ao conteúdo digital assinado, ou seja, o conteúdo digital que foi visualizado pelo signatário DEVE ser o conteúdo submetido ao processo de geração de assinatura digital.

4.2.2.9 Um documento eletrônico a ser assinado DEVE conter apenas objetos estáticos e todos os componentes necessários devem estar contidos no documento eletrônico, isto é, ele NÃO DEVE conter referências a recursos internos ou externos que possam alterar a visualização do conteúdo assinado ao longo do tempo. Quando for necessário realizar a assinatura digital sobre um documento eletrônico cuja visualização possa se alterar ao longo do tempo, é OBRIGATÓRIO realizar sua conversão para um formato estático.

4.2.2.10 Os processos de geração de assinatura digital DEVEM ser capazes de incluir e manipular atributos assinados e não assinados definidos conforme a política de assinatura adotada.

4.2.2.11 Uma **assinatura digital ICP-Brasil de curo prazo (AD-CP)** é criada pelo signatário com a ajuda de um dispositivo seguro de criação de assinaturas, com base no documento eletrônico a ser assinado e na chave privada do signatário, utilizando algoritmos aprovados no documento DOC-ICP-01.01 [21].

4.2.2.11 Uma **assinatura digital ICP-Brasil com carimbo do tempo (AD-T)** é criada com base numa assinatura digital ICP-Brasil de curto prazo para a qual foi emitido um carimbo do tempo por uma Autoridade de carimbo do Tempo credenciada na ICP-Brasil, de forma que esse carimbo fique anexado ou logicamente conectado à assinatura digital para a qual foi criado. O processo de solicitação do carimbo do tempo DEVE ser realizado pelo próprio signatário **ou** pelo verificador.

4.2.2.12 Uma **assinatura digital ICP-Brasil com referências para validação (AD-R)** é criada com base numa assinatura digital ICP-Brasil com carimbo do tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com os itens 4.2.3.1 e 4.2.3.2 deste documento, bem como um carimbo do tempo sobre o conjunto de dados, emitido por uma Autoridade de carimbo do Tempo credenciada na ICP-Brasil. As referências e o segundo carimbo do tempo DEVE ser incorporados pelo signatário ou pelo verificador da assinatura.

4.2.2.13 Uma **assinatura digital ICP-Brasil com informações completas (AD-C)** é criada com base numa assinatura digital ICP-Brasil com carimbo do tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com os itens 4.2.3.1 e 4.2.3.2 deste documento, bem como todos os dados necessários para a verificação dessa assinatura digital ICP-Brasil.. As referências e os dados de validação DEVE ser incorporados pelo signatário ou pelo verificador da assinatura.

4.2.2.14 Uma **assinatura digital ICP-Brasil com informações para arquivamento (AD-A)** é criada com base numa assinatura digital ICP-Brasil com carimbo do tempo ou numa assinatura digital com referências para validação, à qual são anexados todos os dados necessários para a verificação dessa assinatura digital ICP-Brasil. Sobre esses dados é emitido um novo carimbo do tempo, gerado por uma Autoridade de Carimbo do Tempo credenciada na ICP-Brasil, se possível utilizando algoritmos mais fortes (ou comprimentos de chaves maiores) do que no carimbo do tempo original. Essa operação, que DEVE ser realizada pelo signatário ou pelo verificador, PODE ser repetida cada vez que a proteção estiver em vias de se tornar fraca. Assim, uma assinatura digital ICP-Brasil com informações para arquivamento suporta múltiplos carimbos do tempo embutidos.

4.2.3 Validação de uma assinatura digital ICP-Brasil

4.2.3.1 Toda assinatura digital ICP-Brasil DEVE ser passível de validação. Para verificar a validade de uma assinatura digital ICP-Brasil o verificador DEVE utilizar:

a) o documento eletrônico para o qual a assinatura digital ICP-Brasil foi criada;

b) a assinatura digital ICP-Brasil do documento eletrônico;

c) o certificado digital do signatário e sua correspondente cadeia de certificação;

d) elementos utilizados para verificação do estado de revogação dos certificados da cadeia de certificação;

e) a política de assinatura, cujo identificador encontra-se na assinatura digital ICP-Brasil;

f) um dos algoritmos definidos no DOC-ICP-01.01 [21].

4.2.3.2 Para validar uma assinatura digital ICP-Brasil, realizada sobre um documento eletrônico com base nos dados mencionados no parágrafo 4.2.3.1, é necessário assegurar-se que:

a) o estado criptográfico da assinatura digital seja válido, o que envolve:
   i. autenticação e/ou autoria: pela decifração da assinatura digital gerada sobre o conteúdo digital utilizando a chave criptográfica assimétrica pública contida no certificado digital do signatário;
   ii. integridade: por comparação de resultados hash , mostrando que o conteúdo digital não foi alterado desde que sua assinatura digital foi criada pelo signatário.

b) o certificado digital correspondente à chave privada utilizada para geração da assinatura seja válido, o que envolve a verificação de:
   i. observância aos requisitos definidos nos itens 4.2.2.2 e 4.2.2.3;
   ii. validade da assinatura digital da entidade que emitiu o certificado do signatário.

4.2.3.3 A validade de uma assinatura digital ICP-Brasil NÃO DEVE ser verificada se o verificador não dispuser dos dados listados no item 4.2.3.1, acima.

4.2.3.4 A validação de uma **assinatura digital ICP-Brasil com carimbo do tempo** consiste na verificação de:

a) a validade da assinatura digital ICP-Brasil conforme itens 4.2.3.1 e 4.2.3.2, acima;

b) a validade do carimbo do tempo, conforme disposto no documento DOC-ICP-12 [20];

4.2.3.5 A validação de uma **assinatura digital ICP-Brasil com referências para validação** compreende a verificação de:

a) a disponibilidade e completude das informações para validação da assinatura digital ICP-Brasil;

b) a validade da assinatura digital ICP-Brasil com carimbo do tempo, conforme item 4.2.3.4.

4.2.3.6 A validação de uma **assinatura digital ICP-Brasil com informações completas** compreende a verificação de:

c) a completude das informações para validação da assinatura digital ICP-Brasil;

d) a validade da assinatura digital ICP-Brasil com carimbo do tempo, conforme item 4.2.3.4.

4.2.3.7 A validação de uma **assinatura digital ICP-Brasil com informações para arquivamento** compreende a verificação de:

a) a validade do carimbo do tempo de arquivamento, conforme disposto no DOC-ICP-12 [20];

b) a completude das informações para validação da assinatura digital ICP-Brasil;

c) a validade da assinatura com carimbo do tempo, emitida conforme item 4.2.3.4.

4.2.3.8 Os processo de validação de assinatura digital e seus requisitos aplicam-se para os três contextos de geração: assinatura digital simples, co-assinaturas digitais e contra-assinaturas. Cada assinatura gerada DEVE ser verificada e DEVE atender aos requisitos do processo de verificação.

4.2.3.9 Caso uma entidade específica (por exemplo, uma aplicação de assinatura digital para

contratos eletrônicos de câmbio) necessite gerar a última co-assinatura digital do processo de negócio ou aplicação, então tal entidade DEVE realizar o processo de verificação sobre sua assinatura digital gerada e também sobre as assinaturas anteriores. Neste caso, a verificação de revogação do certificado digital pelo primeiro signatário e pelos signatários intermediários PODE ser opcional.

4.2.3.10 Um conteúdo digital PODE estar armazenado de forma particionada em um repositório interno de um ambiente computacional. Por exemplo, um conteúdo digital PODERIA ser composto de várias partes que estejam armazenadas em tabelas diferentes de um mesmo servidor de banco de dados. Neste caso específico, o processo de geração DEVE primeiro juntar as partes para formar o conteúdo digital e depois gerar a assinatura digital propriamente dita. Como conseqüência, o processo de verificação de assinatura digital DEVE requerer, quando necessário, a reconstrução, de forma confiável, de um conteúdo digital já assinado anteriormente para a verificação das assinaturas.

4.2.3.11 O término do processo de validação de assinatura digital DEVE mostrar como resultado o estado de cada assinatura avaliada em termos de válido, inválido e indeterminado, identificando também os signatários. Além disso, caso algum certificado digital de assinatura apresente qualquer não conformidade, o sistema DEVE gerar um alerta ao verificador, ressaltando quais são os problemas encontrados.

4.2.3.12 Com relação aos instantes de tempo envolvidos numa assinatura digital, e considerando o disposto no item 5.12 do DOC-ICP-15, as seguintes restrições temporais DEVEM ser satisfeitas no processo de validação de uma assinatura digital:

a) T_{dec} ϵ Ivu ;
b) Tref ϵ Ivu ;
c) T_{dec} < Tref ;
d) Trc < Ttvc → Ivu < Ivc
e) Outras restrições temporais declaradas na política de assinatura digital.

4.2.4 Visualização e/ou extração do conteúdo digital

Os processos de assinatura digital DEVEM permitir, quando for do desejo dos signatários ou de alguma parte interessada envolvida nos processos, a visualização e/ou extração do conteúdo digital assinado.

4.2.5 Assinaturas Digitais em Lote

4.3.5.1 Para assinaturas digitais em lote DEVEM ser aplicados os mesmos requisitos definidos para

os processos relacionados ao ciclo de vida da assinatura individual.

4.3.5.2 Quando for necessário realizar assinaturas digitais em lote DEVEM ser estabelecidos métodos ou procedimentos seguros de acesso à chave privada do signatário de tal forma que permitam o uso contínuo e seguro dessa chave durante a realização da assinatura digital em cada conteúdo digital pertencente a um lote.

4.3.5.3 No caso das assinaturas digitais em lote, por questões de pragmatismo, a chave assimétrica privada do signatário PODE ser habilitada somente uma vez (por exemplo, com a inserção do PIN) para a geração das assinaturas digitais em todos os conteúdos do lote.

4.3 Políticas de assinatura digital ICP-Brasil

4.3.1 Todas as assinaturas digitais ICP-Brasil DEVEM conter um indicador da Política de Assinatura usada para criação e verificação da assinatura.

4.3.2 As entidades que desejarem criar suas próprias políticas de assinatura DEVEM utilizar o padrão definido no DOC-ICP-15.03 e submeter sua Política à AC-Raiz da ICP-Brasil, onde será avaliada e, se aprovada, receberá um identificador único (OID).

4.3.3 Com vistas a facilitar a adoção de políticas de assinaturas digitais e a estabelecer um patamar mínimo de segurança, foram criadas Políticas de Assinatura Padrão ICP-Brasil, codificadas em linguagem humana, ASN-1 e XML, que trazem os requisitos mínimos que DEVEM ser observados na geração e validação de uma assinatura digital.

4.3.4 As políticas-padrão de assinatura ICP-Brasil estão definidas no DOC-ICP-15.03 e encontram-se também publicadas no site www.iti.gov.br.

4.4 Perfis de assinaturas digitais ICP-Brasil

4.4.1 Com o objetivo de orientar os desenvolvedores de aplicações, foram definidos perfis de assinatura que incorporam as principais informações julgadas relevantes para o contexto brasileiro. Tais perfis encontram-se detalhados no documento DOC-ICP-15.02 para ADAC e ADAX.

4.4.2 A adoção desses perfis é OBRIGATÓRIA, com vistas a permitir a interoperabilidade entre diferentes aplicações.

4.4.3 Quando julgado necessário, PODEM ser implementados outros atributos ou propriedades, dentre os constantes nos documentos RFC 3852 [14], ETSI TR 102733 [7], RFC 3275 [15] e ETSI TR 102903 [10], desde que os campos e subestruturas utilizadas sejam submetidas à AC Raiz para publicação e obtenção de OID específicos e derivados de números com limitação de domínio, quando for o caso.

4.5 Algoritmos admitidos para assinaturas digitais na ICP-Brasil

A lista dos algoritmos aprovados e parâmetros para algoritmos para criação de assinatura digital ICP-Brasil é dada no documento DOC-ICP-01.01 [21]

4.6 Formato do documento eletrônico assinado

4.6.1 Cabe ao signatário escolher o formato a ser utilizado no documento eletrônico e ao verificador decidir se aceita ou não aquele formato.

4.6.2 As entidades credenciadas ou cadastradas junto à ICP-Brasil DEVEM adotar os formatos relacionados no Documento de Referência E-Ping [23] para geração e verificação de assinaturas digitais em documentos eletrônicos que tenham relação com os processos que executam, no âmbito da ICP-Brasil.

5. 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] ETSI. Eletronic Signature and Infraestructures (ESI); CMS Advanced Eletronica Signatures (CAdES). ETSI TR 102 733 (2007-01); European Telecomunications Standards Institute, 2007.

[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] RFC 3852 Cryptographic Message Syntax (CMS) (2004-07);

[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 2.0

[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] E-Ping – Documento de Referência - http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/versoes-do-documento-da-e-ping.

[24] RFC 2311 - S/MIME Version 2 Message Specification (1998-03).

[25] UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL). Model Law on Electronic Signatures with Guide to Enactment. United Nations, 2001. (obtido de http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf)

6. 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

TIPOS DE COMPROMISSO PARA USO EM ASSINATURAS DIGITAIS ICP-BRASIL

1. INTRODUÇÃO

1.1 Durante a geração e verificação de uma Assinatura Digital ICP-Brasil, PODE haver situações onde um signatário deseja indicar explicitamente para um verificador que, assinando os dados, ele expressa um tipo de compromisso como signatário. O atributo *commitment-type-indication* expressa tal informação. O atributo *commitment-type-indication* DEVE ser um atributo assinado.

1.2 O tipo de compromisso pode ser definido de duas formas: como parte da política de assinatura ou como um tipo registrado.

1.2.1 No primeiro caso, o tipo de compromisso possui semântica específica, que é definida dentro da política de assinatura. A política de assinatura especifica um conjunto de atributos que ela "reconhece". Este conjunto "reconhecido" inclui todos os tipos de compromisso definidos como parte da política de assinatura, assim como qualquer tipo de compromisso externamente definido, que a política PODE escolher reconhecer.

1.2.2 No segundo caso, o tipo de compromisso registrado possui semântica definida por uma autoridade. No caso da ICP- Brasil, a AC-Raiz brasileira é a autoridade competente para criar tipos de compromisso que PODEM ser utilizados por qualquer signatário, em diferentes contextos.

1.3 Se a assinatura digital incluir uma indicação de tipo de compromisso diferente dos que foram reconhecidos sob a política de assinatura, ou dos que foram definidos pela AC-Raiz, a assinatura DEVE ser tratada como inválida.

1.4 Este documento padroniza os tipos de compromisso a serem utilizados na ICP-Brasil. 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).

2. TIPOS DE COMPROMISSO NA ICP-BRASIL

2.1 Para evitar redundâncias, procurou-se aproveitar os tipos de compromisso já padronizados por organismos internacionais, que todavia mostraram-se insuficientes para atender aos diferentes propósitos de assinatura no País.

2.2 Por esse motivo, foram criados tipos de compromisso próprios da ICP-Brasil, utilizando a árvore de OID brasileira, de acordo com a seguinte regra:

2.16.76.1.7.n – Políticas de Assinatura Digital

2.16.76.1.8.n – Tipos de Compromisso em Assinatura Digital

2.3 Para atender necessidades específicas de segmentos da sociedade e da economia, podem ser necessários outros tipos de compromisso além dos aqui listados. Nesse caso, seu registro pode ser solicitado à Diretoria de Auditoria, Fiscalização e Normalização da AC-Raiz da ICP-Brasil, por email endereçado a normalizacao@iti.gov.br

2.4 A tabela a seguir relaciona os tipos de compromisso para Assinaturas Digitais definidos pelo IETF na RFC 3126 e pelo ETSI no documento ETSI TS 101 733:

Nome	OID	Descrição
Prova de origem (proof of origin)	id-cti-ets-proofOfOrigin (1.2.840.113549.1.9.16.6.1)	Indica que o signatário reconhece a criação, aprovação e o envio de uma mensagem.
Prova de recebimento (proof of receipt)	id-cti-ets-proofOfReceipt (1.2.840.113549.1.9.16.6.2)	Indica que o signatário reconhece o recebimento do conteúdo de uma mensagem.
Prova de envio (proof of delivery)	id-cti-ets-proofOfDelivery (1.2.840.113549.1.9.16.6.3)	Indica que o "fornecedor de serviço confiável" (TSP – Trusted Service Provider) emissor da indicação disponibilizou uma mensagem em uma área de armazenamento local acessível ao destinatário da mensagem.

Prova de envio (proof of sender)	id-cti-ets-proofOfSender (1.2.840.113549.1.9.16.6.4)	Indica que a entidade emissora da indicação enviou a mensagem (mas não necessariamente a criou).
Prova de aprovação (proof of aproval)	id-cti-ets-proofOfApproval (1.2.840.113549.1.9.16.6.5)	Indica que o signatário aprovou o conteúdo da mensagem.
Prova de criação (proof of creation)	id-cti-ets-proofOfCreation (1.2.840.113549.1.9.16.6.6)	Indica que o signatário criou a mensagem (mas não necessariamente a aprovou ou a enviou).

2.5 A tabela a seguir relaciona os tipos de compromisso para Assinaturas Digitais criados pela AC-Raiz para uso no âmbito da ICP-Brasil.

Nome	OID	Descrição do compromisso
Concordância	2.16.76.1.8.1	A assinatura aposta indica que o signatário concorda com o conteúdo assinado.
Autorização	2.16.76.1.8.2	A assinatura aposta indica que o signatário autoriza o constante no conteúdo assinado.
Testemunho	2.16.76.1.8.3	A assinatura aposta indica o compromisso de testemunho do signatário. Não necessariamente indica concordância do signatário com o conteúdo.
Autoria	2.16.76.1.8.4	A assinatura aposta indica que o signatário foi autor do conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo.
Conferência	2.16.76.1.8.5	A assinatura aposta indica que o signatário realizou a conferência do conteúdo.
Revisão	2.16.76.1.8.6	A assinatura aposta indica que o signatário revisou o conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo.
Ciência	2.16.76.1.8.7	A assinatura aposta indica que o signatário tomou ciência do conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo.
Publicação	2.16.76.1.8.8	A assinatura tem o propósito de indicar que o signatário publicou o documento em algum meio de comunicação externo à entidade que o originou.

Protocolo	2.16.76.1.8.9	A assinatura aposta indica a intenção do signatário em protocolar o conteúdo.
Integridade	2.16.76.1.8.10	A assinatura aposta indica a intenção do signatário em garantir somente a integridade da mensagem.
Autenticação de usuário	2.16.76.1.8.11	A assinatura aposta é utilizada somente como prova de autenticação do signatário.
Teste	2.16.76.1.8.12	A assinatura aposta indica a intenção do signatário em realizar um teste.