



Infraestrutura de Chaves Públicas Brasileira

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

DOC-ICP-15.01

Versão 2.0

05 de abril de 2010



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

1. INTRODUÇÃO.....	3
2. REQUISITOS TÉCNICOS PARA ASSINATURAS DIGITAIS NA ICP-BRASIL.....	4
2.1 FORMATOS DE ASSINATURA DIGITAL ADMITIDOS NA ICP-BRASIL.....	4
2.2. REQUISITOS TÉCNICOS PARA GERAÇÃO E VALIDAÇÃO DE ASSINATURAS DIGITAIS ICP-BRASIL.....	7
2.2.1 Requisitos Gerais.....	7
2.2.2 Geração de uma assinatura digital ICP-Brasil.....	7
2.2.3 Validação de uma assinatura digital ICP-Brasil.....	9
2.2.4 Visualização e/ou extração do conteúdo digital.....	11
2.2.5 Assinaturas Digitais em Lote.....	11
2.3 POLÍTICAS DE ASSINATURA DIGITAL ICP-BRASIL.....	11
2.4 PERFIS DE ASSINATURAS DIGITAIS ICP-BRASIL.....	12
2.5 ALGORITMOS ADMITIDOS PARA ASSINATURAS DIGITAIS NA ICP-BRASIL.....	12
2.6 FORMATO DO DOCUMENTO ELETRÔNICO ASSINADO.....	12
BIBLIOGRAFIA.....	13



Infraestrutura de Chaves Públicas Brasileira

1. INTRODUÇÃO

1.1 A utilização de formatos padronizados de assinatura digital no âmbito da Infra-estrutura de Chaves Públicas Brasileira (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 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; e
- c) procedimentos para verificação e condições para validação de uma assinatura digital ICP-Brasil.

1.4 A seguir o capítulo 2 apresenta os requisitos técnicos para geração e validação de assinaturas digitais na ICP-Brasil, está organizado da seguinte forma: a seção 2.1 apresenta os formatos de assinatura digital admitidos na ICP-Brasil; a seção 2.2 descreve os requisitos técnicos para geração e validação dessas assinaturas; a seção 2.3 apresenta as políticas de assinatura digital e a seção 2.4 os perfis.

2. REQUISITOS TÉCNICOS PARA ASSINATURAS DIGITAIS NA ICP-BRASIL

2.1 FORMATOS DE ASSINATURA DIGITAL ADMITIDOS NA ICP-BRASIL

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

a) assinatura digital com Referência Básica (AD-RB), ilustrada na Figura 2.1;

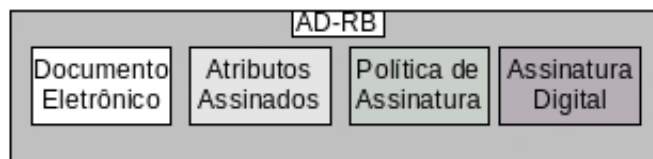


Figura 2.1: Assinatura digital com Referência Básica

b) assinatura digital com Referência de Tempo (AD-RT), ilustrada na Figura 2.2;

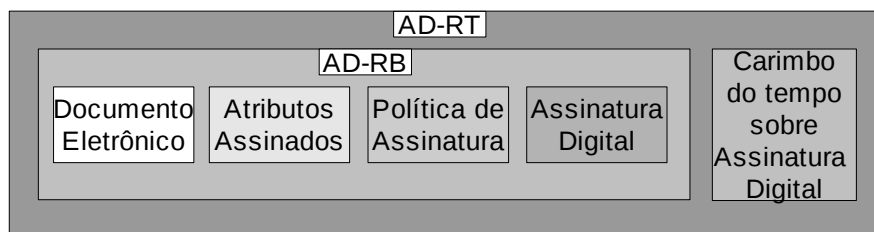


Figura 2.2: Assinatura digital com Referência de Tempo

c) assinatura digital com Referências para Validação (AD-RV), ilustrada na Figura 2.3;

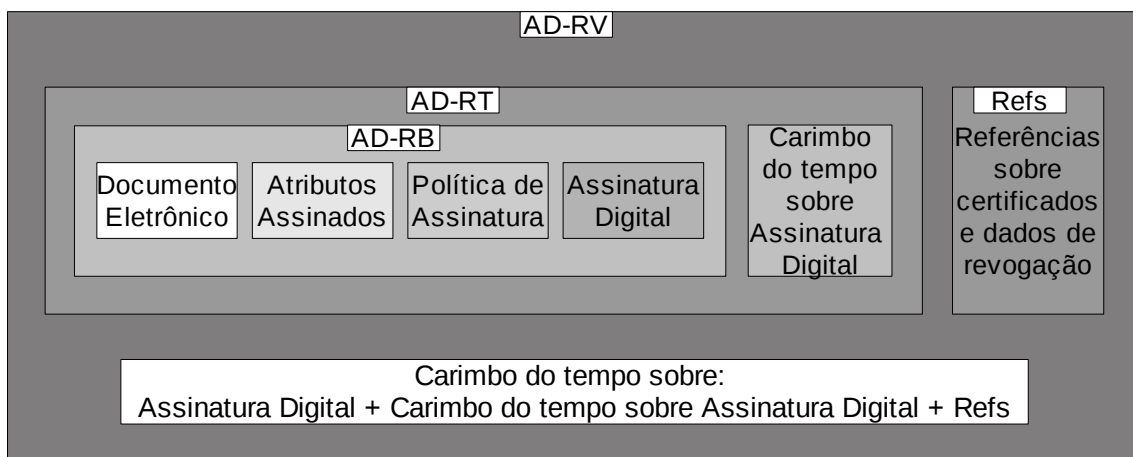


Figura 2.3: Assinatura digital com Referências para Validação

d) assinatura digital com Referências Completas (AD-RC), ilustrada na Figura 2.4; ou

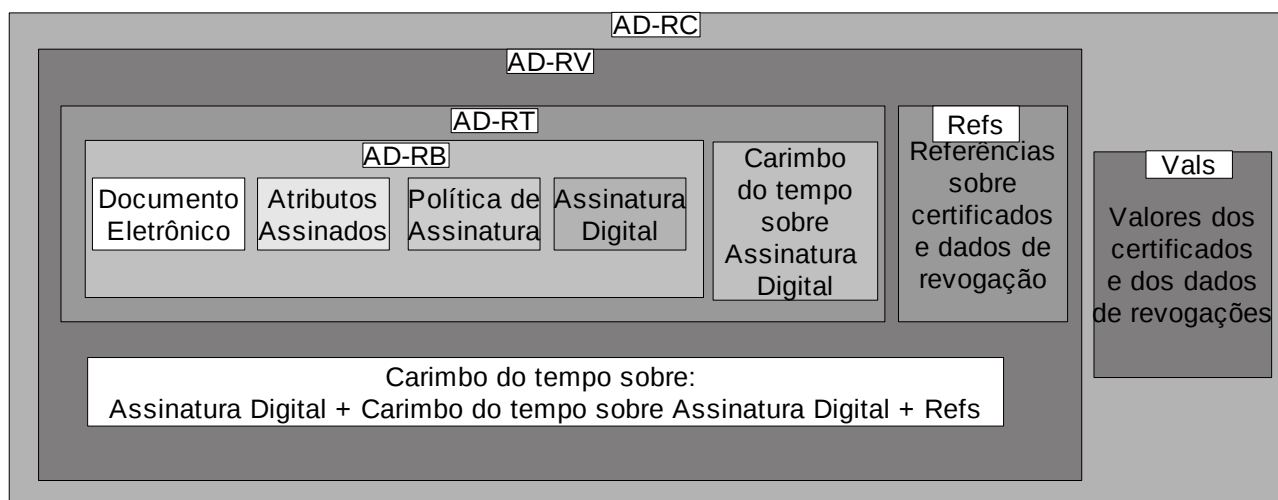


Figura 2.4: Assinatura digital com Referências Completas

e) assinatura digital com Referências para Arquivamento (AD-RA), ilustrada na Figura 2.5.

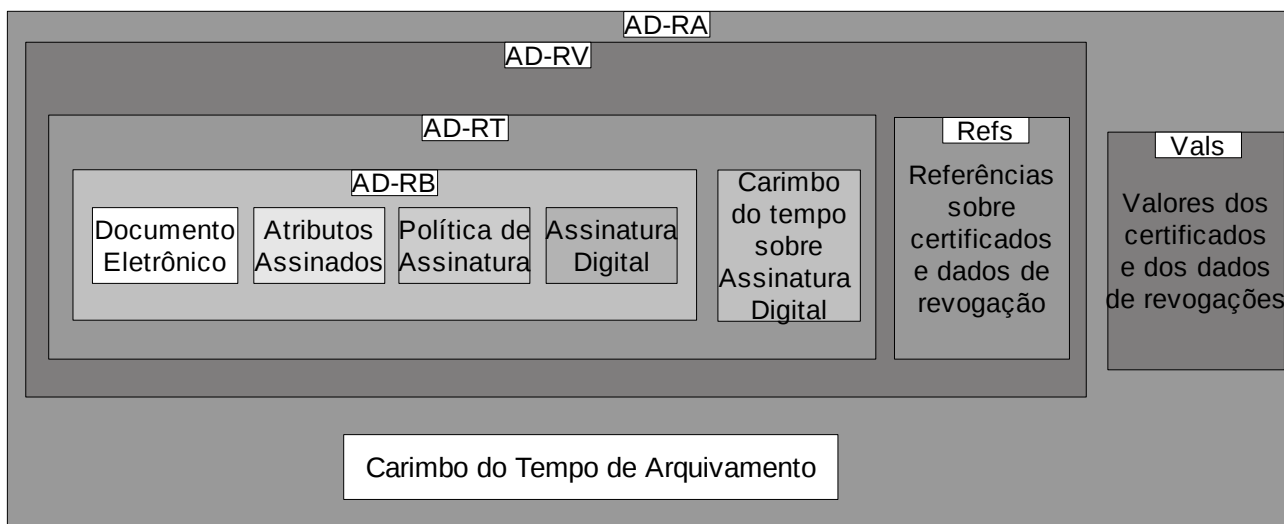


Figura 2.5: Assinatura digital com Referências para Arquivamento

2.1.2 Uma assinatura digital ICP-Brasil com Referência Básica é formada por:

- identificador da política de assinatura usada para criação e verificação de uma dada assinatura digital ICP-Brasil;
- dados da assinatura, os quais o signatário incluiu na assinatura digital ICP-Brasil (por exemplo:

instante de criação da assinatura);
c) a seqüência de códigos da assinatura propriamente dita.

2.1.3 Uma assinatura digital ICP-Brasil com Referência de Tempo é formada por uma assinatura digital ICP-Brasil com Referência Básica (AD-RB) na qual foi acrescentado ou logicamente conectado, por algum meio, um carimbo do tempo emitido por uma Autoridade de Carimbo do Tempo (ACT) credenciada na ICP-Brasil, criado com base nos procedimentos aprovados pelo documento DOC-ICP-12 [1].

2.1.4 Uma assinatura digital ICP-Brasil com Referências para Validação é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) na qual foram acrescentadas referências sobre todos os certificados de chave pública e sobre todas as Listas de Certificados Revogados (LCR) ou respostas de *Online Certificate Status Protocol* (OCSP) que são necessários para a validação daquela assinatura. Sobre esses dados é acrescentado ou logicamente conectado outro carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil.

2.1.5 Uma assinatura digital ICP-Brasil com Referências Completas é formada por uma assinatura digital ICP-Brasil com Referências para Validação (AD-RC) à qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento.

2.1.6 Uma assinatura digital ICP-Brasil com Referências para Arquivamento é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) à qual foram acrescentadas referências de validação e todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento. Um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil é criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

2.2. REQUISITOS TÉCNICOS PARA GERAÇÃO E VALIDAÇÃO DE ASSINATURAS DIGITAIS ICP-BRASIL

2.2.1 Requisitos Gerais

2.2.1.1 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”.

2.2.1.2 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.

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

- a) Assinaturas com base no padrão CMS *Advanced Electronic Signature* (CADES)
 - i. id-contentType
 - ii. id-messageDigest
 - iii. id-aa-signingCertificate
 - iv. id-aa-ets-sigPolicyId
- b) Assinaturas com base no padrão XML-DSig *Advanced Electronic Signature* (XADES)
 - i. DataObjectFormat (para assinaturas do tipo *detached*)
 - ii. SigningCertificate
 - iii. SignaturePolicyIdentifier

2.2.2 Geração de uma assinatura digital ICP-Brasil

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 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.

2.2.2.4 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.

2.2.2.5 Os componentes de aplicação de assinatura DEVEM conter 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.

2.2.2.6 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.

2.2.2.7 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.

2.2.2.8 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.

2.2.2.9 Em qualquer tempo no futuro, o conteúdo digital visualizado deve ser o mesmo daquele visualizado quando foi assinado, ou seja, a assinatura só deve ser válida para o conteúdo visualizado durante o momento de geração da assinatura.

2.2.2.10 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.

2.2.2.11 Uma assinatura digital ICP-Brasil com referência de tempo é criada com base numa assinatura digital ICP-Brasil com referência básica para a qual foi emitido um carimbo do tempo por uma ACT 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.

2.2.2.12 Uma assinatura digital ICP-Brasil com referências para validação é criada com base numa assinatura digital ICP-Brasil com referência de tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com o item 2.2.3.1 deste documento,

bem como um carimbo do tempo sobre o conjunto de dados, emitido por uma ACT credenciada na ICP-Brasil. As referências e o segundo carimbo do tempo DEVEM ser incorporados pelo signatário ou pelo verificador da assinatura.

2.2.2.13 Uma assinatura digital ICP-Brasil com referências completas é criada com base numa assinatura digital ICP-Brasil com referência de tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com o item 2.2.3.1 deste documento, bem como todos os dados necessários para a verificação dessa assinatura digital ICP-Brasil. As referências e os dados de validação DEVEM ser incorporados pelo signatário ou pelo verificador da assinatura.

2.2.2.14 Uma assinatura digital ICP-Brasil com referências para arquivamento é criada com base numa assinatura digital ICP-Brasil com referência de 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 ACT 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 referências para arquivamento suporta múltiplos carimbos do tempo embutidos.

2.2.3 Validação de uma assinatura digital ICP-Brasil

2.2.3.1 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) os status de revogação referentes aos certificados dos caminhos de certificação do usuário e, quando houver carimbo do tempo, da ACT;
- e) a política de assinatura, cujo identificador encontra-se na assinatura digital ICP-Brasil;
- f) um dos algoritmos definidos no DOC-ICP-01.01 [2].

2.2.3.2 Para validar uma assinatura digital ICP-Brasil, realizada sobre um documento eletrônico com base nos dados mencionados no parágrafo 2.2.3.1, 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 resumos criptográficos, mostrando que o conteúdo digital não foi alterado desde que sua assinatura digital foi criada pelo signatário.
- b) o caminho de certificação do signatário seja válido na referência temporal adotada para a

verificação da assinatura, o que envolve

c) a observância aos requisitos definidos nos itens 2.2.2.2 e 2.2.2.3;

2.2.3.3 A validade de uma assinatura digital ICP-Brasil NÃO DEVE ser verificada se o verificador não dispuser dos dados listados no item 2.2.3.1, acima.

2.2.3.4 A validação de uma assinatura digital ICP-Brasil com referência de tempo consiste na verificação de:

- a) a validade do carimbo do tempo, conforme disposto no documento DOC-ICP-12;
- b) a validade da assinatura digital ICP-Brasil conforme itens 2.2.3.1 e 2.2.3.2, adotando-se como referência temporal a data e hora informada pelo carimbo do tempo.

2.2.3.5 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 2.2.3.4.

2.2.3.6 A validação de uma assinatura digital ICP-Brasil com referências completas compreende a verificação de:

- a) a completude das informações para validação da assinatura digital ICP-Brasil;
- b) a validade da assinatura digital ICP-Brasil com carimbo do tempo, conforme item 2.2.3.4.

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

- a) a validade do carimbo do tempo de arquivamento, conforme disposto no DOC-ICP-12;
- b) a completude das informações para validação da assinatura digital ICP-Brasil;
- c) a validade da assinatura com carimbo do tempo, emitida conforme item 2.2.3.4.

2.2.3.8 Os processo de validação de assinatura digital e seus requisitos aplicam-se para os três contextos de geração:

- a) assinatura digital simples;
- b) co-assinaturas digitais e
- c) contra-assinaturas digitais.

Cada assinatura gerada DEVE ser verificada e DEVE atender aos requisitos do processo de validação.

2.2.3.9 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 consequência, 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.

2.2.3.10 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.

2.2.3.11 Com relação aos instantes de tempo envolvidos numa assinatura digital, e considerando o disposto no item 6.12 do DOC-ICP-15, as seguintes restrições temporais DEVEM ser satisfeitas no processo de validação de uma assinatura digital:

- a) $T_{dec} \leq T_{ref}$;
- b) $T_{dec} \leq T_{ref}$;
- c) $T_{dec} < T_{ref}$;
- d) Outras restrições temporais declaradas na política de assinatura digital.

2.2.4 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.

2.2.5 Assinaturas Digitais em Lote

2.2.5.1 Para assinaturas digitais em lote DEVEM ser aplicados os mesmos requisitos definidos para os processos relacionados ao ciclo de vida da assinatura individual.

2.2.5.2 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.

2.2.5.3 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 *Personal Identification Number* (PIN) - para a geração das assinaturas digitais em todos os conteúdos do lote.

2.3 POLÍTICAS DE ASSINATURA DIGITAL ICP-BRASIL

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

2.3.2 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, *Abstract Syntax Notation One* (ASN.1) e *Extensible Markup Language* (XML), que trazem os requisitos mínimos que DEVEM ser observados na geração e validação de uma assinatura digital.

2.3.3 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.

2.4 PERFIS DE ASSINATURAS DIGITAIS ICP-BRASIL

2.4.1 Com o objetivo de orientar os desenvolvedores de aplicações, foi definido um perfil de uso geral para assinaturas digitais que incorpora as principais informações julgadas relevantes para o contexto brasileiro. Tal perfil encontra-se detalhado no documento “Perfil de uso Geral para Assinaturas Digitais na ICP-Brasil” (DOC-ICP-15.02) [4] para CADES e XAdES.

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

2.4.3 Quando julgado necessário, PODEM ser implementados outros atributos ou propriedades, dentre os constantes nos documentos RFC 3852 [5], ETSI TR 102 733 [6], RFC 3275 [7] e ETSI TR 102 903 [8], desde que os campos e subestruturas utilizadas sejam submetidas à AC Raiz para publicação e obtenção de OIDs específicos e derivados de números com limitação de domínio, quando for o caso.

2.5 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 “Padrões e Algoritmos Criptográfico da ICP-Brasil” (DOC-ICP-01.01).

2.6 FORMATO DO DOCUMENTO ELETRÔNICO ASSINADO

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

2.6.2 As entidades credenciadas ou cadastradas junto à ICP-Brasil DEVEM adotar os formatos relacionados no Documento de Referência e-PING [9] para geração e verificação de assinaturas digitais em documentos eletrônicos que tenham relação com os processos que executam, no âmbito da ICP-Brasil.



Infra-Estrutura de Chaves Públicas Brasileira

BIBLIOGRAFIA

- [1] ITI. *Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil*. v.1.0. Brasília, Dezembro 2008. DOC-ICP-12.
- [2] ITI. *Padrões e Algoritmos Criptográficos da ICP-Brasil*. v.2.0. Brasília, Junho 2009. DOC-ICP-01.01.
- [3] ITI. *Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil*. v.1.0. Brasília. DOC-ICP-15.03.
- [4] ITI. *Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil*. v.1.0. Brasília. DOC-ICP-15.02.
- [5] HOUSLEY, R. *Cryptographic Message Syntax (CMS)*. IETF, jul. 2004. RFC 3852 (Proposed Standard). (Request for Comments, 3852). Updated by RFCs 4853, 5083. Disponível em: <<http://www.ietf.org/rfc/rfc3852.txt>>.
- [6] ETSI. *Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAAdES)*. 2008. Acesso em: 23/02/2009.
- [7] Eastlake 3rd, D.; REAGLE, J.; SOLO, D. *(Extensible Markup Language) XML-Signature Syntax and Processing*. IETF, mar. 2002. RFC 3275 (Draft Standard). (Request for Comments, 3275). Disponível em: <<http://www.ietf.org/rfc/rfc3275.txt>>.
- [8] ETSI. *XML Advanced Electronic Signatures (XAdES)*. 1.3.2. ed. [S.l.], 2006. Acesso em: 23/02/2009.
- [9] ELETRÔNICO, C. E. de G. *e-PING: Padrões de Interoperabilidade de Governo Eletrônico*. Disponível em: <<https://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>>. Acesso em: 24 jun. 2007.
- [10] PINKAS, D.; POPE, N.; ROSS, J. *CMS Advanced Electronic Signatures (CAAdES)*. IETF, mar. 2008. RFC 5126 (Informational). (Request for Comments, 5126). Disponível em: <<http://www.ietf.org/rfc/rfc5126.txt>>.