ASSINATURAS DIGITAIS

NA ICP-BRASIL

DOC-ICP-15

Versão 1.0

Data: 20.02.2008

SUMÁRIO

1 INTRODUÇÃO

1.1. 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).

1.2 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

1.3 As diretrizes aqui constantes 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.

1.4 Aos titulares de certificados, terceiras partes confiáveis e desenvolvedores de aplicações que utilizem assinatura digital, recomenda-se fortemente que também utilizem os formatos e padrões aqui definidos, de forma a garantir a credibilidade do processo de assinatura digital e a interoperabilidade entre sistemas.

1.5 Este documento adota como referência, além das normas da ICP-Brasil, os padrões internacionais relacionados no item 6 – BIBLIOGRAFIA.

1.6 Os normativos sobre Assinatura Digital na ICP-Brasil são os seguintes:

a) ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15 (este documento) – traz uma visão geral do assunto, define os principais conceitos, estabelece os requisitos obrigatórios a serem observados na criação e verificação de assinaturas digitais na ICP-Brasil e lista os demais documentos que compõem as normas da ICP-Brasil sobre esse assunto;

b) PERFIL PARA ASSINATURAS CADES ICP-BRASIL – DOC-ICP-15.01 – delimita os atributos a serem usados na geração de assinaturas digitais no padrão CADES, no âmbito da ICP-Brasil;

c) PERFIL PARA ASSINATURAS XADES ICP-BRASIL – DOC-ICP-15.02 - delimita os atributos a serem usados na geração de assinaturas digitais no padrão XADES, no âmbito da ICP-Brasil;

d) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03 – define um formato de documento que deve ser adotado pelas entidades ao criar suas próprias políticas de assinatura digital;

e) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES – DOC-ICP-15.04 – define uma política oficial da AC-Raiz para criação e verificação de assinaturas digitais usando o padrão CADES.

f) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO XADES – DOC-ICP-15.05 – define uma política oficial da AC-Raiz para criação e verificação de assinaturas digitais usando o padrão XADES.

2 MOTIVAÇÕES

2.1 A ICP-Brasil instituiu uma infra-estrutura de chaves públicas confiável, em âmbito nacional, com regras e políticas que permitem a emissão e o gerenciamento de certificados digitais com segurança, para uso em aplicações e processos.

2.2 Assinaturas digitais e seus processos associados, como por exemplo, geração e verificação de assinaturas digitais, estão entre as principais aplicações da certificação digital, sobretudo no âmbito da ICP-Brasil, onde esse tipo de assinatura possui o mesmo valor de uma assinatura manuscrita.

2.3 Para propiciar a larga utilização de assinaturas digitais é necessário, porém, definir as diretrizes técnicas a serem adotadas para que os processos de geração e verificação de assinaturas digitais sejam realizados de forma padronizada e com requisitos de segurança suficientes para garantir, a médio e longo prazos, a recuperação das assinaturas e documentos eletrônicos, bem como a determinação de sua autoria e integridade.

2.4 Nesse contexto, portanto, a criação do conjunto de normativos sobre assinatura digital na ICP-Brasil apresenta as seguintes motivações:

a) auxiliar entidades na adoção de normas e condutas técnicas comuns que possam ser utilizadas em sistemas de assinatura digital;

b) consolidar e popularizar o uso seguro da assinatura digital;

c) desenvolver a interoperabilidade entre sistemas que utilizam a assinatura digital para agilizar seus processos e aplicações;

d) uniformizar os esforços na definição dos requisitos técnicos de segurança e interoperabilidade para assinaturas digitais, possibilitando maior pragmatismo e concentração de esforços na implementação dos sistemas de assinatura digital;

e) aprimorar a relação custo/benefício em processos e aplicações de TI; e

f) melhorar a competência técnica de entidades na utilização de assinaturas digitais.

3 DEFINIÇÕES

Para os propósitos desta Resolução, entende-se por:

3.1 documento eletrônico, uma seqüência de bits elaborada mediante processamento eletrônico de dados, destinada a reproduzir uma manifestação do pensamento ou um fato;

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 assinatura digital ICP-Brasil, 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;

3.4 chave de criação de assinatura, o conjunto único de dados eletrônicos, tal como chaves criptográficas privadas, utilizado para a criação de uma assinatura eletrônica;

3.5 chave de verificação de assinatura, o conjunto de dados eletrônicos,tal como chaves criptográficas públicas, utilizado para a verificação de uma assinatura eletrônica;

3.6 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 desta;
b) inviabilize a dedução desta 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;

3.7 carimbo de tempo, documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora;

3.8 componentes de aplicação de assinatura, os produtos físicos (hardware) e lógicos (software) que:

i. vinculem ao documento eletrônico processo de produção e verificação de assinaturas eletrônicas; ou
ii. verifiquem assinaturas eletrônicas e confiram certificados, disponibilizando os resultados;

3.9 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);

3.10 resultado hash de um documento**,** um valor calculado a partir de um documento eletrônico com a ajuda de uma função hash.

3.11 identificador da política de assinatura, dados que identificam de forma unívoca uma dada política de assinatura.

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

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

4 DOCUMENTOS SOBRE ASSINATURA DIGITAL NA ICP-BRASIL

4.1 A organização dos documentos que compõem o conjunto de normativos sobre assinatura digital na ICP-Brasil está retratada na figura 1.

4.2 Este conjunto de normas é voltado para assinaturas nos padrões CMS-CADES e XML-XADES, que são os mais usados atualmente para assinaturas digitais. É possível que, com a utilização intensiva das assinaturas, novos documentos, contemplando outros formatos de assinatura digital, venham a ser necessários e sejam incorporados a este conjunto.

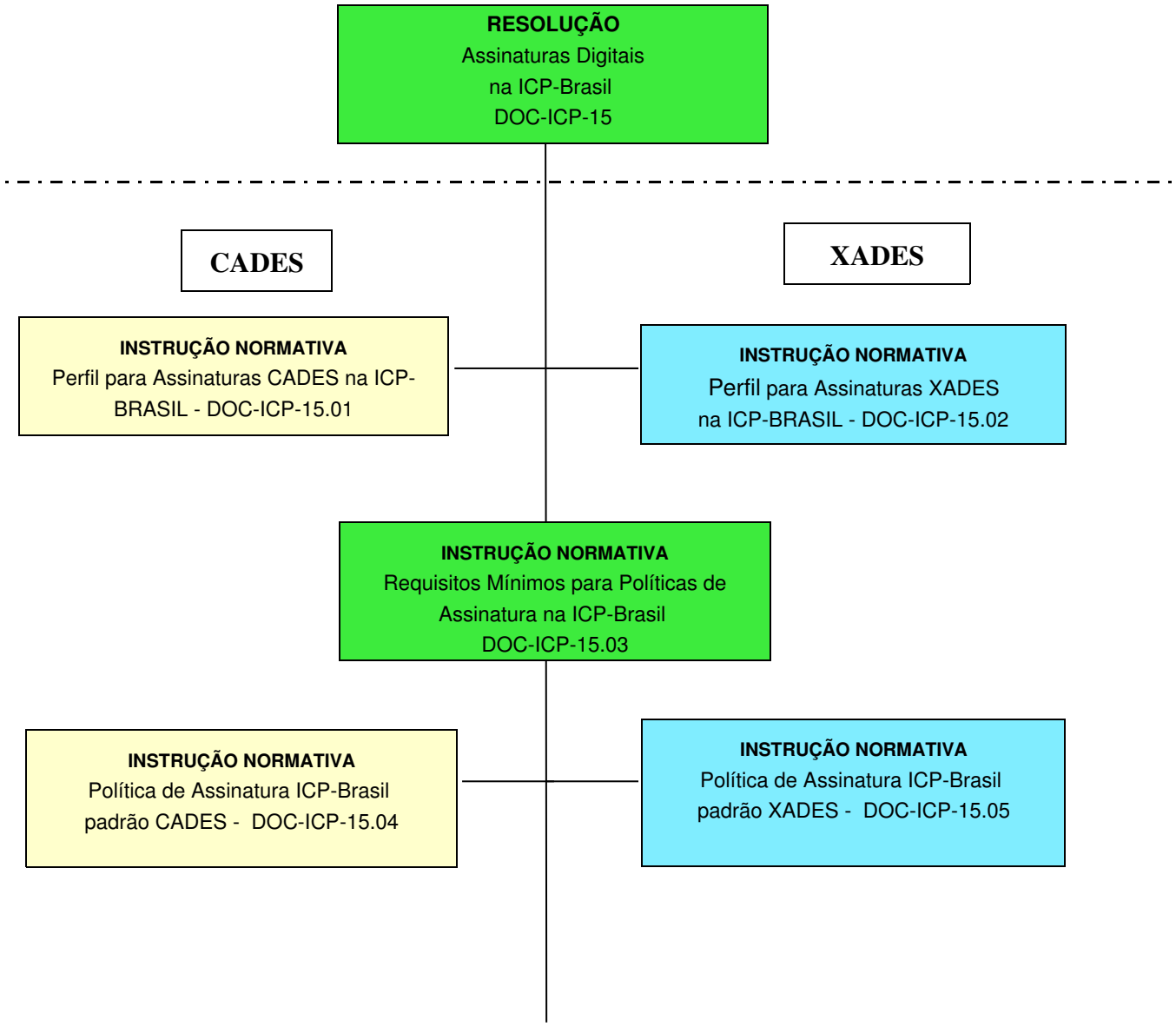

Figura 1 - Organização dos documentos sobre assinatura digital na ICP-Brasil

5 PRINCIPAIS CONCEITOS

5.1 Assinatura digital x Assinatura eletrônica

5.1.1 Uma assinatura eletrônica representa um conjunto de dados, no formato eletrônico, que é anexado ou logicamente associado a um outro conjunto de dados, também no formato eletrônico, para conferir-lhe autenticidade ou autoria.

5.1.2 A assinatura eletrônica, portanto, pode ser obtida por meio de diversos dispositivos ou sistemas, como login/senha, biometria, impostação de PIN etc.

5.1.3 Um dos tipos de assinatura eletrônica é a assinatura digital, que utiliza pares de chaves criptográficas associados a certificados digitais.

5.1.4 O conjunto de normativos ora criado trata, apenas, das assinaturas digitais geradas no âmbito da ICP-Brasil. Os demais tipos de assinaturas eletrônicas estão fora do seu escopo.

5.1.5 No contexto destes normativos estaremos sempre nos referindo a assinaturas digitais como sendo aquelas produzidas com a utilização de chaves criptográficas privadas associadas a certificados digitais ICP-Brasil.

5.2 Entidades envolvidas na assinatura digital

5.2.1 São as seguintes as entidades envolvidas no processo de assinatura digital:

a) Signatário ou assinante - é a entidade que cria a assinatura digital. Quando o assinante assina digitalmente sobre dados utilizando o formato indicado, isto representa um comprometimento da sua parte para com os dados que estão sendo assinados.

b) Terceira parte ou verificador – uma ou mais entidades que validam a assinatura digital.

c) Mediador ou árbitro - Pessoa ou entidade que pode ser chamada para arbitrar a disputa entre o signatário e o verificador (terceira parte) quando há disputas sobre a validade da assinatura digital.

d) Provedores de Serviços de Confiança (PSC) - são uma ou mais entidades que ajudam a construir uma relação de confiança entre o assinante e o verificador. Eles apóiam o signatário e o verificador por meios de serviços de suporte, como emissão de certificados digitais, emissão e LCR ou de respostas OCSP, emissão de carimbos de tempo etc.

5.3 Ciclo de vida de uma assinatura digital

5.3.1 O ciclo de vida de uma assinatura digital compreende os processos de:

a) Criação - processo de criação de um código logicamente associado a um conteúdo digital e a chave criptográfica do signatário;

b) Verificação ou validação - processo de verificação quanto a validade de uma ou mais assinaturas digitais logicamente associado a um conteúdo digital;

c) Armazenamento – processo que trata da guarda da assinatura digital. Deve compreender, pelo menos, cuidados para conversão dos dados para mídias mais atuais, sempre que necessário;

d) Revalidação – processo que estende a validade do documento assinado, por meio da re-assinatura dos documentos ou da aposição de carimbos de tempo, quando da expiração ou revogação dos certificados utilizados para gerar ou revalidar as assinaturas, ou ainda quando do enfraquecimento dos algoritmos ou tamanhos de chave utilizados.

5.3.2 As assinaturas digitais devem ser criadas com características apropriadas à finalidade e longevidade esperada. Adiante veremos que, sobre uma assinatura digital básica, podem-se incorporar elementos que permitam uma validação mais confiável a longo prazo, o que, em contrapartida, aumenta o tamanho do arquivo e o tempo gasto na geração da assinatura.

5.3.3 As Figuras 2 e 3 apresentam, de forma simplificada os processos de criação e de verificação de uma assinatura digital, respectivamente.

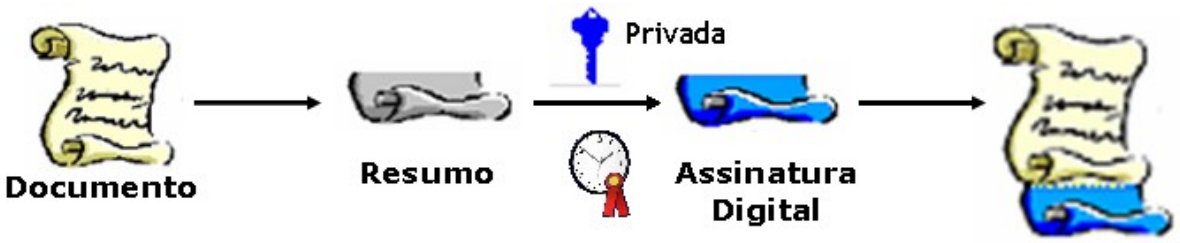

Figura 2 – Diagrama simplificado de criação de assinatura digital

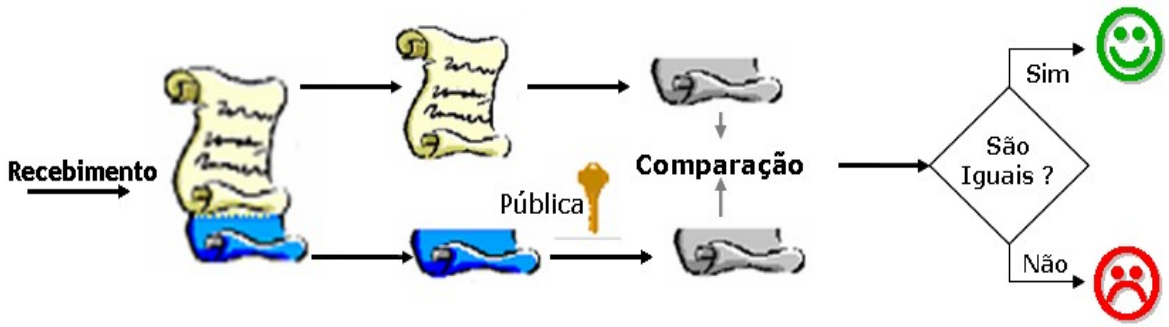

Figura 3 – Diagrama simplificado de verificação de assinatura

5.4 Padrões internacionais para assinatura digital

5.4.1 CMS-CADES

5.4.1.1 O padrão CMS é uma evolução do padrão PKCS#7. A versão CMS utilizada como referência neste documento é a descrita na RFC 3852 [14]. O padrão CMS descreve uma

estrutura para armazenamento de conteúdos (dados) assinados digitalmente, conteúdos cifrados, conteúdos autenticados e conteúdos com resultados hash . Este documento trata especificamente do tipo de conteúdo *Signed-data*, relevante para o contexto de assinatura digital.

5.4.1.2 O padrão CMS dispõe de ampla documentação e de variada gama de bibliotecas de *software* disponíveis. É o padrão mais utilizado, atualmente, nas aplicações em nível mundial.

5.4.1.3 Em assinaturas digitais no padrão CMS, o armazenamento do conteúdo digital propriamente dito é opcional e, por este motivo, permite a existência de duas representações diferentes:

a) Estrutura assinada com conteúdo digital incluído (*attached*): neste caso, o conteúdo digital está incluído na estrutura CMS;

b) Estrutura assinada sem conteúdo incluído (*detached*): neste caso, o conteúdo digital não está incluído na estrutura CMS.

5.4.1.4 Além dos atributos assinados (ou seja, que fazem parte do cálculo do resultado hash , sobre o qual a assinatura será gerada), o CMS permite adicionar atributos não assinados, bem como gerar assinaturas em paralelo e assinaturas em série (ver item 5.9). O CMS não permite, todavia, assinar partes de um documento, somente o documento como um todo.

5.4.1.5 O padrão CADES (CMS Advanced Electronic Signature) é uma extensão do padrão CMS, descrita no documento ETSI TR 102733 [7]. Foi criado com vistas a prover as assinaturas digitais de informações que permitam sua validação a mais longo prazo.

5.4.1.6 A validação de uma assinatura digital de acordo com o padrão CADES exige que se incorporem dados adicionais, necessários para validar a assinatura. Esses dados adicionais incluem:

a) certificados de chave pública;

b) LCR ou respostas OCSP sobre o estado de revogação para cada certificado;

c) carimbos de tempo confiáveis aplicados sobre a assinatura digital;

d) quando apropriado, os detalhes sobre a política de assinatura usada para gerar e verificar a assinatura.

5.4.1.7 A incorporação desses dados de validação às assinaturas digitais leva à criação de diferentes formatos de assinaturas. Para cada formato, existe um conjunto de atributos de caráter obrigatório, sendo permitida a incorporação de atributos não obrigatórios à assinatura, conforme a necessidade de cada signatário, organização, aplicação ou negócio.

5.4.2 XML-XADES

5.4.2.1 Outro padrão utilizado para representação de assinaturas digitais é o XMLSignature, derivado da linguagem Extensible Markup Language (XML), cuja especificação é mantida pela organização World Wide Web Consortium (W3C) e Internet Engineering Task Force (IETF).

5.4.2.2 Sua última especificação é dada pela RFC-3275 [15]. Em comparação ao CMS, o XMLSignature apresenta as vantagens da própria linguagem XML, que é extensível, possibilitando a criação de *tags* de um modo arbitrário, desde que as regras de aninhamento sejam respeitadas.

É bastante útil como meio de integração de diversas fontes de informação e apresentação de interface uniforme para esses dados.

5.4.2.3 O padrão XMLSignature contempla assinatura de diversos tipos de conteúdo como dados codificados em ASCII em diversos tipos de formatos, dados em código binário ou ainda dados formatados em XML.

5.4.2.4 O padrão XMLSignature permite gerar uma assinatura digital sobre apenas uma parte de um documento eletrônico.

5.4.2.5 Outra característica do padrão XMLSignature é que, em relação ao armazenamento do conteúdo digital, são possíveis três representações diferentes:

a) Estrutura assinada sem conteúdo incluído (*detached*): neste caso, o conteúdo digital não está incluído na estrutura XMLSignature;

b) Estrutura assinada com conteúdo digital incluído (*enveloping*): neste caso, o conteúdo digital está incluído na estrutura XMLSignature;

c) Estrutura assinada incluída no conteúdo digital (*enveloped*): neste caso, a assinatura digital está incluída no conteúdo digital que está sendo assinado.

5.4.2.6 Da mesma forma que o CMS, o padrão XMLSignature recebeu uma extensão com vistas a prover as assinaturas digitais de informações que permitam sua validação a mais longo prazo. Trata-se do padrão XADES (XMLSignature Advanced Electronic Signature), descrito no documento ETSI TS 101903 [10].

5.4.2.7 O XADES também exige que se incorporem à assinatura dados adicionais, similares aos do CADES, que levam à criação de diferentes formatos de assinaturas. Para cada formato, existe um conjunto de atributos de caráter obrigatório, sendo permitida a incorporação de atributos não obrigatórios à assinatura, conforme a necessidade de cada signatário, organização, aplicação ou negócio.

5.5 Perfis de assinatura digital

5.5.1 Os padrões CADES e XADES disponibilizam uma diversificada gama de atributos ou propriedades, que permitem às entidades envolvidas incorporar às assinaturas digitais informações com os mais diferentes objetivos.

5.5.2 Essa abundância de opções, se por um lado traz flexibilidade, por outro leva à criação de sistemas que exigem grande capacidade de processamento dos equipamentos, para conseguir gerar e validar todos os atributos num tempo hábil. Isso faz com que os desenvolvedores escolham apenas alguns atributos para implementar no seu sistema, que podem ser diferentes dos escolhidos por outros desenvolvedores, o que acaba comprometendo a interoperabilidade entre diferentes sistemas.

5.5.3 Para maximizar a interoperabilidade nas comunidades que utilizam os padrões CADES e XADES para geração de assinaturas, é necessário identificar um conjunto comum de opções que sejam apropriadas para aquela comunidade. Tal seleção é chamada de perfil. Exemplos de perfil estão nos documento ETSI TS 102 734 [8] e ETSI TS 102 904 [11].

5.6 Políticas de assinatura

5.6.1 Uma política de assinatura é um conjunto de regras que formaliza os processos de criação e verificação de uma assinatura digital e define a base para que a assinatura digital possa ser considerada válida. O formato e a estrutura usados para criação de políticas de assinatura nos padrões CADES e XADES estão descritos nos documentos ETSI TR 102 272 [6] e ETSI TR 102 038 [9], respectivamente.

5.6.2 Uma assinatura digital deve ser criada pelo signatário de acordo com a política de assinatura nela definida. A validade de uma assinatura digital é avaliada pelo verificador utilizando a mesma política de assinatura usada na criação dessa assinatura digital.

5.6.3 A parte que recebe os documentos assinados com uma assinatura digital determina quais políticas de assinatura podem ser aceitas no seu processo de negócios.

5.6.4 A utilização de políticas de assinatura torna claro e dá pleno conhecimento às partes envolvidas sobre os requisitos para geração e verificação das assinaturas e formaliza as condições de validade de um documento assinado digitalmente.

5.6.5 A utilização de políticas de assinatura também facilita a criação de sistemas de processamento adaptáveis aos diferentes modelos de negócios de cada empresa, com controle do processo de geração e verificação de assinatura digital.

5.6.6 Um exemplo seria a criação de um sistema de gerenciamento eletrônico de fluxo de documentos onde cada signatário tenha um tipo de compromisso diferenciado no processo, ou onde a aposição das assinaturas tenha de ser realizada em determinada ordem. O resultado final – um documento com diversas assinaturas – poderia ser obtido mesmo sem o uso de uma política. Entretanto, a utilização de uma política de assinatura, disponível publicamente a todos os interessados, assegura que cada signatário conheça os requisitos do processo e concorde com eles. Para tanto, é necessário que o sistema informe ao signatário, antes da aposição da assinatura, qual política está sendo usada naquela transação e onde ela se encontra publicada, para que ele possa decidir se a assina ou não.

5.6.7 O uso de políticas de assinatura também permite ao verificador, no futuro, validar as assinaturas apostas no documento mesmo que não disponha mais do sistema onde foram geradas.

5.6.8 As políticas podem ser criadas pelo signatário, pelo verificador ou por qualquer outra entidade que julgue apropriado fazê-lo.

5.7 Relação entre padrões internacionais e os documentos ICP-Brasil

5.7.1 A figura seguinte ilustra a relação existente entre os padrões internacionais que tratam de assinatura digital, os perfis e políticas de assinatura e demais documentos ICP-Brasil

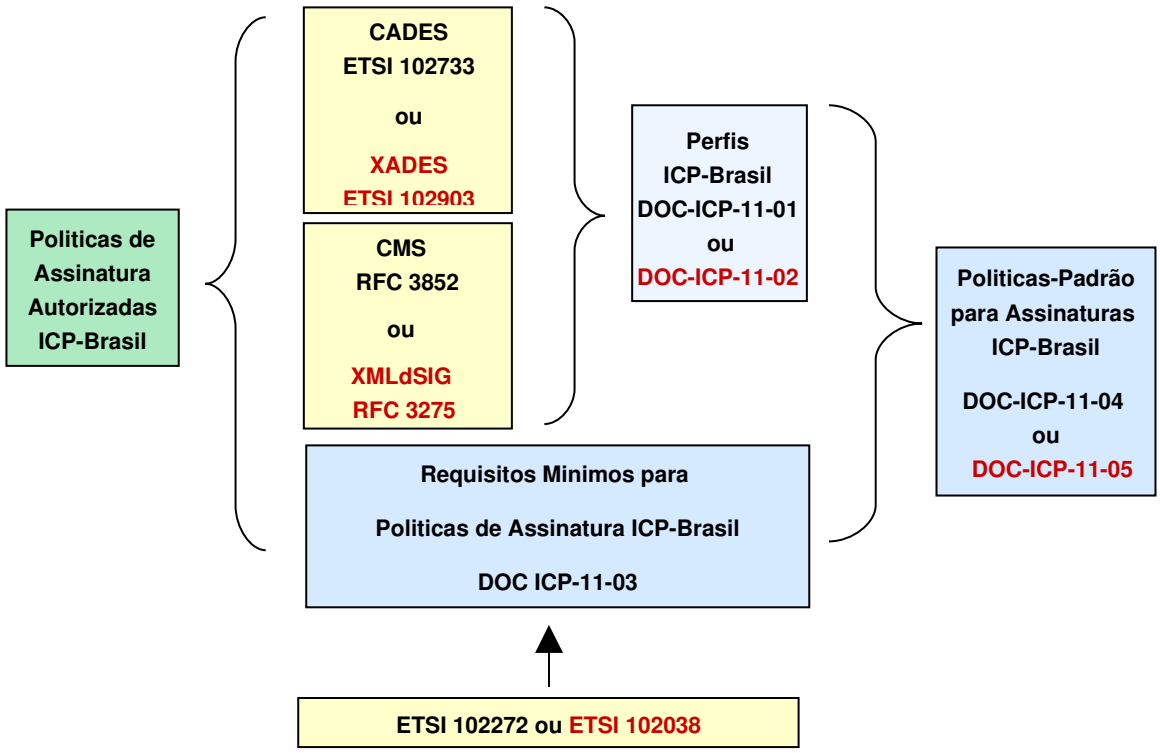

Figura 4 – Relação entre padrões internacionais sobre assinatura digital e os documentos ICP-Brasil

5.8 Documentos eletrônicos com mais de uma assinatura digital

5.8.1 Com relação ao processo de geração de assinatura digital, podemos ter três contextos diferentes: assinaturas simples, co-assinaturas e contra-assinaturas.

5.8.2 A geração de assinatura digital simples ocorre quando uma única assinatura digital é gerada sobre um conteúdo digital disponível.

5.8.3 A geração de co-assinaturas digitais ocorre quando duas ou mais assinaturas digitais podem ser geradas de forma paralela e independente pelos signatários, utilizando conteúdos digitais idênticos. Cada co-assinatura gerada pode conter atributos assinados próprios.

5.8.4 A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre a seqüência de bytes (bloco) que representa uma assinatura digital já previamente existente. O conteúdo digital a ser assinado em uma contra-assinatura corresponde a

um bloco de assinatura digital já previamente gerado (assinatura digital em série a partir de uma outra já previamente existente). Uma contra-assinatura pode conter outros atributos assinados próprios.

5.9 Assinaturas Digitais em Lote

5.9.1 O termo “assinaturas digitais em lote” representa um caso particular da assinatura digital, no qual é necessário realizar diversas assinaturas digitais em um lote de conteúdos digitais (uma assinatura digital para cada conteúdo do lote), resultando assim em diversas operações criptográficas seqüenciais utilizando a mesma chave assimétrica privada do signatário.

5.10 Formato do documento eletrônico assinado

5.10.1 O documento eletrônico a ser assinado pode ser criado em formatos públicos (ex.: TXT, XML ou PDF) ou em formatos para os quais a especificação não está publicada (ex. DOC). O risco, nesse segundo caso, é de que tais formatos sejam descontinuados, e a falta de informação sobre os formato poderia dificultar ou inviabilizar a recuperação do conteúdo do documento eletrônico.

5.10.2 Cabe ao signatário escolher o formato a ser utilizado no documento eletrônico e ao verificador decidir se aceita ou não aquele formato, que está indicado no corpo da assinatura digital.

6 REQUISITOS TÉCNICOS PARA ASSINATURAS DIGITAIS NA ICP-BRASIL

Esta seção regulamenta os requisitos que devem ser obrigatoriamente 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) detalhes das condições de validade de uma assinatura digital ICP-Brasil, os procedimentos para verificação de uma assinatura digital ICP-Brasil e as condições de validação de uma assinatura digital ICP-Brasil.

6.1 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]

6.2 Formatos de assinatura digitais admitidos na ICP-Brasil

6.2.1 Uma assinatura digital ICP-Brasil pode ter os seguintes formatos:

a) sem carimbo de tempo;

b) com carimbo de tempo;

c) com informação completa para validação;

d) com informações para arquivamento; ou

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

6.2.2 Uma **assinatura digital ICP-Brasil sem carimbo de tempo (EPES)** 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.

6.2.3 No mínimo os seguintes campos assinados devem constar das assinaturas digitais ICP-Brasil:

a) Assinaturas no padrão CADES
   i. Message Digest

ii. Id-contentType
iii. Id-messageDigest
iv. id-aa-signingCertificate ou Id-aa-signingCertificateV2
v. id-aa-sigPolicyId
vi. id-signingTime

b) Assinaturas no padrão XADES

i. Message Digest
ii. DataObjectFormat
iii. SigningCertificate
iv. SignaturePolicyIdentifier
v. SigningTime

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

6.2.5 Uma **assinatura digital ICP-Brasil com informação completa para validação (EPES-C-X)** tem a forma de uma assinatura digital ICP-Brasil com carimbo de tempo (EPES-T) na qual foram acrescentadas referências sobre todos os certificados de chave pública necessários para validar aquela assinatura digital, assim como referências sobre as LCR ou respostas OCSP que são necessárias para a validação daquela assinatura digital ICP-Brasil. Sobre esses dados é acrescentado ou logicamente conectado outro carimbo de tempo, emitido por uma Autoridade de Carimbo de Tempo credenciada na ICP-Brasil.

6.2.6 Uma **assinatura digital ICP-Brasil com informações para arquivamento (EPES-A)** tem a forma de uma assinatura digital ICP-Brasil com carimbo de tempo (EPES-T) ou com informação completa de validação (EPES-C-X) na qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com o item 6.3.3.1e 6.3.3.2 deste documento. Um carimbo de tempo, emitido por uma Autoridade de Carimbo de Tempo credenciada na ICP-Brasil, é criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

6.2.7 A figura a seguir ilustra os formatos de assinatura acima:

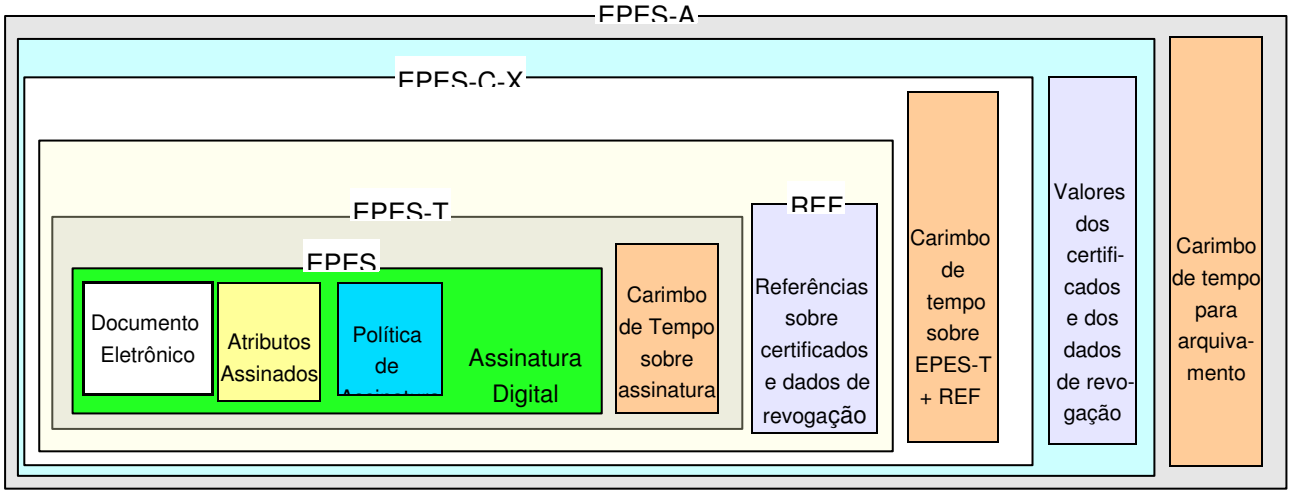

Figura 5 – Formatos de assinatura ICP-Brasil

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

6.3.1 Requisitos Gerais

6.3.1.1 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".

6.3.1.2 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.

6.3.2 Geração de uma assinatura digital ICP-Brasil

6.3.2.1 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.

6.3.2.2 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.

6.3.2.3 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.

6.3.2.4 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.

6.3.2.5 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.

6.3.2.6 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.

6.3.2.7 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.

6.3.2.8 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.

6.3.2.9 Quando o conteúdo digital for de natureza dinâmica, por exemplo, uma página web, os signatários devem manter cópias do conteúdo digital que foi assinado no período de execução do processo de geração da assinatura digital. Para isso, os signatários podem, utilizando procedimentos técnicos e operacionais, manter cópias do conteúdo digital dinâmico em seu ambiente computacional (por exemplo, em um servidor de banco de dados ou de arquivos), ou então, utilizar uma estrutura assinada com conteúdo digital incluído.

6.3.2.10 Quando um conteúdo digital apresentar referências a objetos externos, por exemplo, uma página web, o processo de geração de assinatura digital deve alertar aos signatários sobre tal situação e, além disso, caso seja do interesse dos signatários gerar a assinatura digital, o processo deve remover todas as referências a objetos externos contidas. Portanto, o conteúdo digital a ser assinado deve ser compatível apenas com o texto visualizado pelo signatário, e não devem ser geradas assinaturas digitais sobre referências a objetos externos.

6.3.2.11 Assinaturas digitais podem ser retiradas ou copiadas entre estruturas CMS e XML desde que se preserve o mesmo conteúdo digital. Além disso, assinaturas digitais geradas de forma paralela e independente sobre o mesmo conteúdo digital também podem ser juntadas em estruturas CMS ou XML únicas.

6.3.2.12 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.

6.3.2.13 Uma **assinatura digital ICP-Brasil sem carimbo de tempo (EPES)** 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].

6.3.2.14 Uma **assinatura digital ICP-Brasil com carimbo de tempo (EPES-T)** é criada com base numa assinatura digital ICP-Brasil para a qual foi emitido um carimbo de tempo por uma Autoridade de Carimbo de 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 de tempo pode ser realizado pelo próprio signatário ou pelo verificador.

6.3.2.15 Uma **assinatura digital ICP-Brasil com informação completa para validação (EPES-C-X)** é criada com base numa assinatura digital ICP-Brasil com carimbo de tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com os itens 6.3.3.1 e 6.3.3.2 deste documento, bem como um carimbo de tempo sobre o conjunto de dados, emitido por uma Autoridade de Carimbo de Tempo credenciada na ICP-Brasil. As

referências e o segundo carimbo de tempo podem ser incorporados pelo signatário ou pelo verificador da assinatura.

6.3.2.16 Uma **assinatura digital ICP-Brasil com informações para arquivamento (EPES-A)** é criada com base numa assinatura digital ICP-Brasil com carimbo de tempo ou numa assinatura digital com informação completa 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 de tempo, gerado por uma Autoridade de Carimbo de Tempo credenciada na ICP-Brasil, se possível utilizando algoritmos mais fortes (ou comprimentos de chaves maiores) do que no carimbo de tempo original. Essa operação, que pode 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 de tempo embutidos.

6.3.3 Validação de uma assinatura digital ICP-Brasil

6.3.3.1 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) a chave pública correspondente à chave privada por meio da qual a assinatura digital ICP-Brasil foi criada;

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

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

6.3.3.2 Para validar uma assinatura digital ICP-Brasil, realizada sobre um documento eletrônico com base nos dados mencionados no parágrafo 6.3.3.1, 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 6.3.2.2 e 6.3.2.3;
   ii. validade da assinatura digital da entidade que emitiu o certificado do signatário.

6.3.3.3 A validade de uma assinatura digital ICP-Brasil não pode ser verificada se o verificador não dispuser dos dados listados no item 6.3.3.1, acima.

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

a) a validade da assinatura digital ICP-Brasil conforme itens 6.3.3.1 e 6.3.3.2, acima;

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

6.3.3.5 A validação de uma **assinatura digital ICP-Brasil com informação completa 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 de tempo, conforme item 6.3.3.4.

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

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

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

c) a validade da assinatura com carimbo de tempo, emitida conforme item 6.3.3.4.

6.3.3.8 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.

6.3.3.9 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.

6.3.3.10 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 podem estar 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.

6.3.3.11 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.

6.3.4 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.

6.3.5 Assinaturas Digitais em Lote

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

6.3.5.2 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.

6.3.5.3 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.

6.4 Registros de auditoria de assinatura digital ICP-Brasil

6.4.1 Para fins de auditoria e rastreabilidade, os processos de geração e verificação de assinatura digital devem possibilitar a realização, visualização e armazenamento de registros eletrônicos ou *logs* de suas atividades.

6.4.2 Nos registros realizados, no mínimo as seguintes informações devem estar presentes:

a) Resultado hash do arquivo assinado ou verificado;

b) Tipo de certificado digital ICP-Brasil utilizado (A1, A2, A3, A4);

c) Identificação do proprietário do certificado digital de assinatura (signatário – “campo Subject”);

d) Identificação do emissor (“campo Issuer”) e número serial (“campo serialNumber”) do certificado digital de assinatura (signatário);

e) Data da realização da atividade;

f) Resultado e/ou problemas encontrados nos processos de geração e verificação da assinatura digital;

g) Resultado e/ou problemas encontrados no processo de verificação do certificado digital dos signatários. Neste caso, qualquer não conformidade encontrada deve ser registrada com informações suficientes que possibilitem o seu entendimento. Caso a verificação do certificado digital não tenha sido realizada, o registro deve indicar claramente tal situação.

6.5 Políticas de assinatura digital ICP-Brasil

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

6.5.2 Com vistas a facilitar a adoção de políticas de assinaturas digitais e a estabelecer um patamar mínimo de segurança, foram criadas pelo ITI uma POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES e uma POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO XADES, que trazem os requisitos mínimos que devem ser observados na geração e validação de uma assinatura digital.

6.5.3 As políticas de assinatura ICP-Brasil estão definidas nos documentos DOC-ICP-15.04 e DOC-ICP-15.05 e encontram-se também publicadas no site www.iti.gov.br. A partir delas, pode-se construir outras políticas, com mais requisitos (por exemplo, aposição obrigatória de um carimbo de tempo). Pode-se também criar assinaturas mais sofisticadas usando a política , sabendo-se que pelo menos os requisitos mínimos de segurança para geração e validação da assinatura serão observados.

6.5.4 As entidades que desejarem criar suas próprias políticas de assinatura devem utilizar o padrão definido no DOC-ICP-15.03 e solicitar à AC-Raiz da ICP-Brasil um identificador único (OID) para a política, na forma expressa naquele documento.

6.6 Perfis de assinaturas digitais ICP-Brasil

6.6.1 Com o objetivo de orientar os desenvolvedores de aplicações , definimos perfis de assinatura que incorporam as principais informações julgadas relevantes para o contexto brasileiro. Tais perfis encontram-se detalhados nos documentos DOC-ICP-15.01 e DOC-ICP-15.02 para CADES e XADES, respectivamente.

6.6.2 A adoção desses perfis não é obrigatória, mas recomendável, com vistas a permitir a interoperabilidade entre diferentes aplicações.

6.6.3 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].

6.7 Formato do documento eletrônico assinado

6.7.1 Como já citado, cabe ao signatário escolher o formato a ser utilizado no documento eletrônico e ao verificador decidir se aceita ou não aquele formato.

6.7.2 Tendo em vista a interoperabilidade e longevidade dos documentos eletrônicos assinados, recomenda-se fortemente a adoção dos formatos relacionados no Documento de Referência da e-Ping que estejam com *status* Recomendado ou Adotado (ver http://www.eping.e.gov.br).

6.7.3 Especificamente para as entidades credenciadas ou cadastradas na ICP-Brasil é obrigatória a adoção do disposto no parágrafo anterior 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.

7 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 – **Documento em elaboração**

[21] ITI. PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL. DOC-ICP-01.01 Instituto Nacional de Tecnologia da Informação. Versão 2.0 - **Documento em elaboração**

[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.