Infra-Estrutura de Chaves Públicas Brasileira

VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL

DOC-ICP-15
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. A não utilização desse formato 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 está organizado da seguinte forma:

Seções 1 e 2 – Introdução e Motivações
Seção 3 – Definições
Seção 4 – Organização dos Documentos sobre Assinatura Digital na ICP-Brasil
Seção 5 – Principais Conceitos sobre Assinatura Digital
Seção 6 – Bibliografia.

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 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 prazo, 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 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.

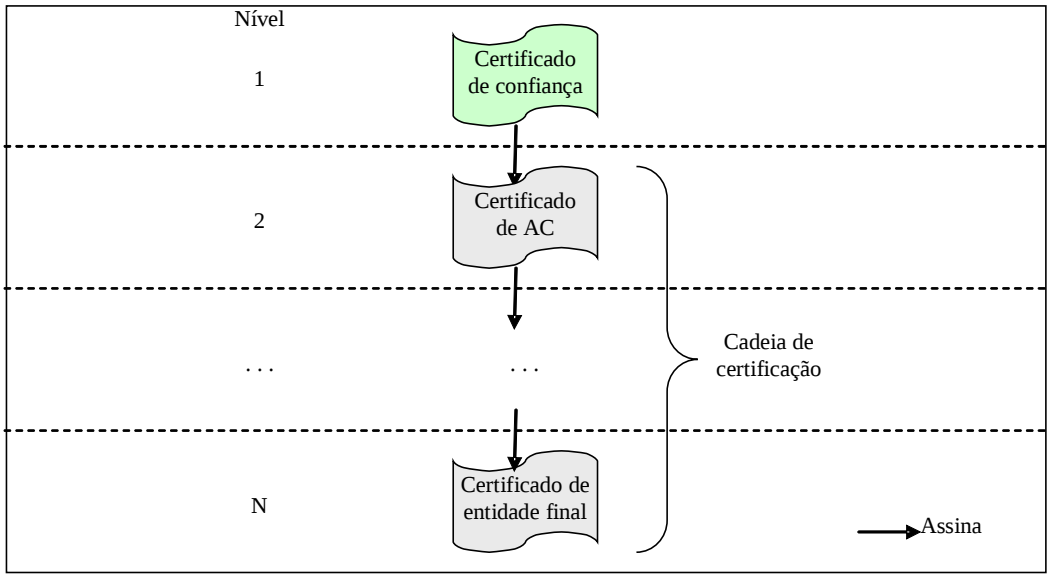

Figura 3.1 – Conceito de cadeia de certificação.

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

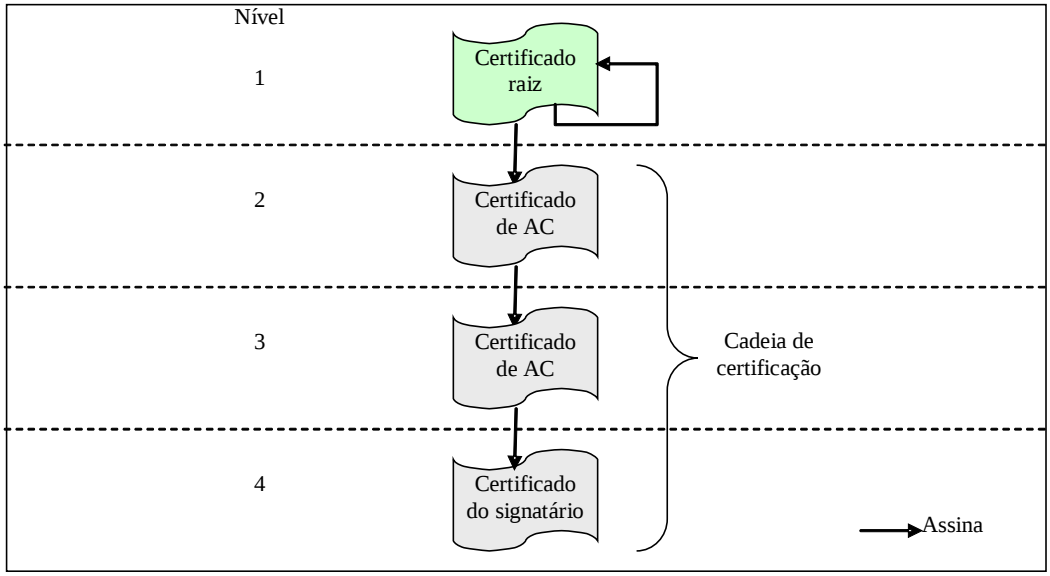

Figura 3.2 – Exemplo de uma cadeia de certificação da ICP-Brasil

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. DOCUMENTOS SOBRE ASSINATURA DIGITAL NA ICP-BRASIL

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

a) VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15 (este documento) – traz uma visão geral do tema, define os principais conceitos e lista os demais documentos que compõem as normas da ICP-Brasil sobre o assunto;

b) REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15.01 – estabelece os requisitos obrigatórios a serem observados na criação e verificação de assinaturas digitais na ICP-Brasil. Possui como anexos os seguintes documentos: TIPOS DE COMPROMISSO PARA USO EM ASSINATURAS DIGITAIS.

c) PERFIL DE USO GERAL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15.02 – delimita os atributos a serem usados na geração de assinaturas digitais no âmbito da ICP-Brasil. Possui como anexo o seguinte documento: MANUAL DE IMPLEMENTAÇÃO;

d) REQUISITOS MÍNIMOS PARA POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL – DOC-ICP-15.03 – define o formato, estrutura e sintaxes a serem adotadas pelas entidades ao criar políticas de assinatura digital. Possui como anexos os documentos POLÍTICAS DE ASSINATURA-PADRÃO PARA A ICP-BRASIL e GERENCIAMENTO DE POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL.

4.2 A organização desses documentos está retratada na figura abaixo.

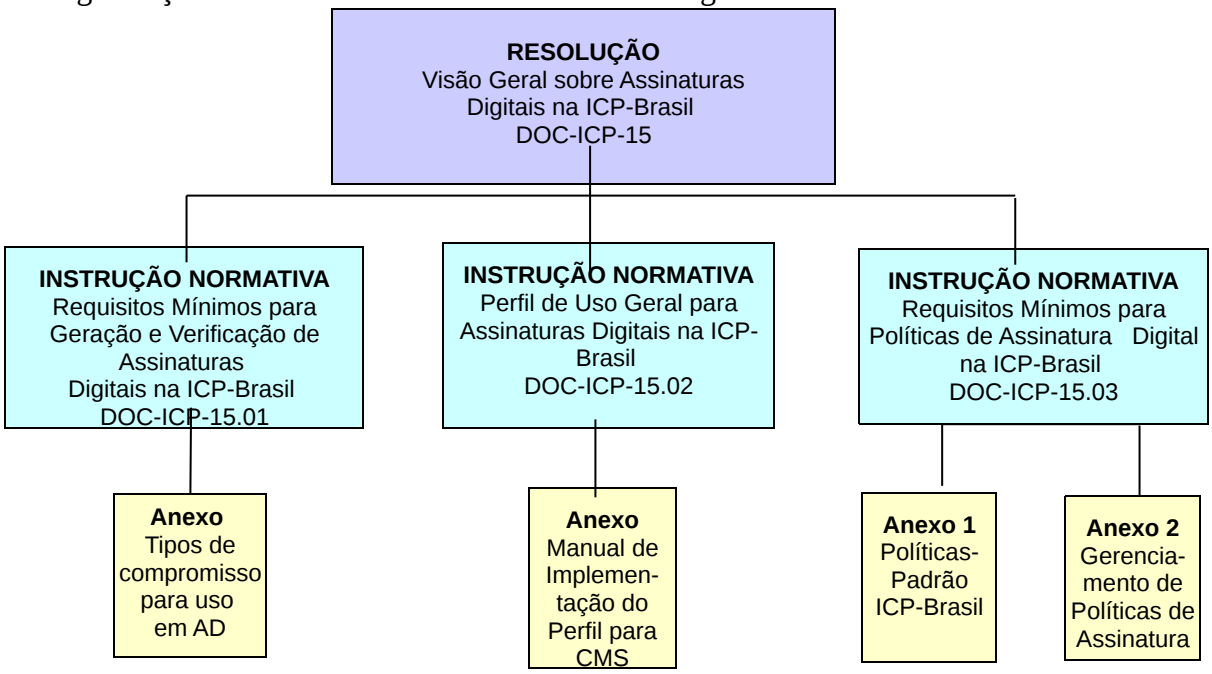

Figura 4.1 – Organização dos documentos sobre Assinatura Digital na ICP-Brasil

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, isso representa um dos compromissos listados no Anexo 1 do DOC-ICP-15.01 – Tipo de compromisso para AD na ICP-Brasil.
b) 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 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 do 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 privada 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. Compreende, 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 do 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 É recomendado que as assinaturas digitais sejam criadas com características apropriadas à finalidade e longevidade esperada. Adiante veremos que uma assinatura digital pode 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 A Figura 5.1 apresenta, de forma simplificada, o processo criptográfico de criação de uma assinatura digital:

a) O signatário gera um resultado *hash* de um documento eletrônico;
b) O signatário cifra o resultado *hash* com sua chave privada, associada a uma chave publica constante do seu certificado digital, gerando a assinatura digital;
c) O documento eletrônico e a assinatura digital ficam associados, para futura validação.

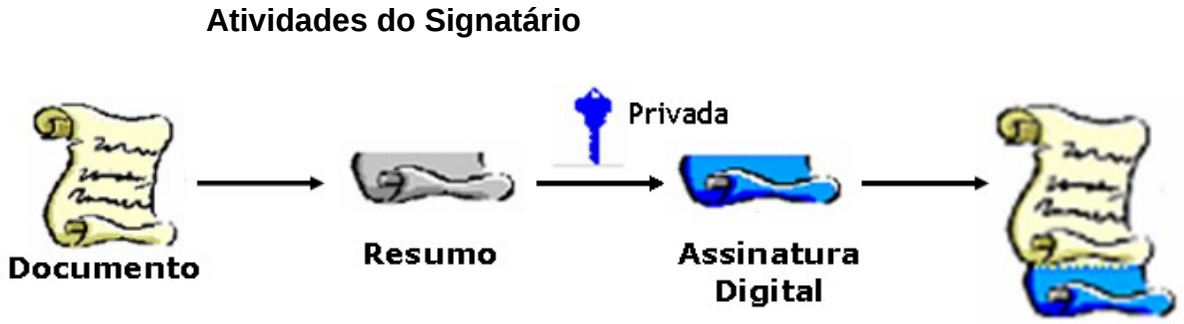

Figura 5.1 – Diagrama simplificado de criação de assinatura digital

5.3.4 A Figura 5.2 apresenta, de forma simplificada, o processo criptográfico de verificação de uma assinatura digital:

a) O documento eletrônico e a assinatura digital associada são disponibilizados para o verificador**,** juntamente com o certificado digital do signatário.
b) O verificador calcula novamente o resultado *hash* do documento eletrônico;
c) O verificador decifra a assinatura digital com a chave pública do signatário, contida no certificado digital, obtendo o resultado *hash* gerado pelo signatário;
d) O verificador compara os resultados *hash* obtidos nos passos b) e c). Se forem iguais, significa que o documento eletrônico esta íntegro e que é possível identificar o signatário por meio do certificado digital. Caso contrário, a assinatura digital é inválida.

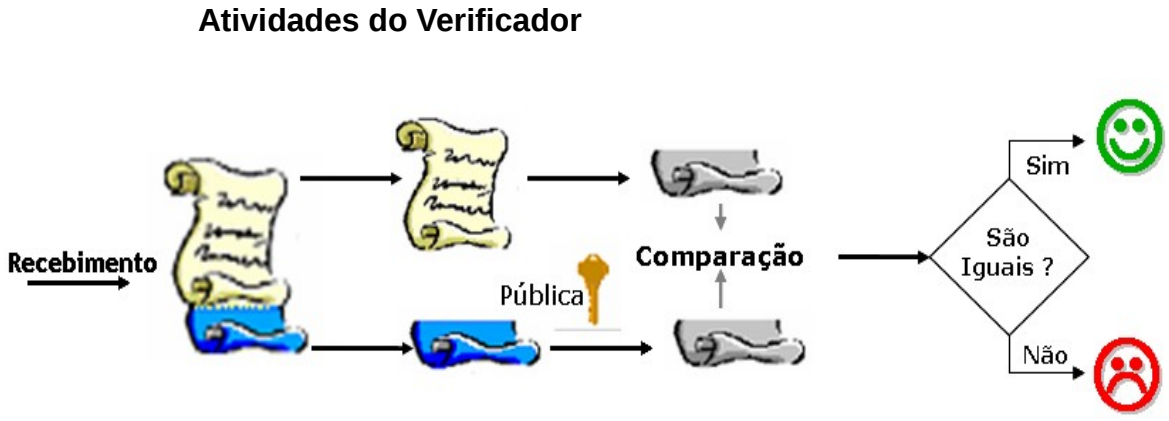

Figura 5.2 – Diagrama simplificado de verificação de assinatura

5.4 Padrões para assinatura digital

5.4.1 CAdES - CMS Advanced Electronic Signature

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 anexado (*attached*): neste caso, o conteúdo digital está incluído na estrutura CMS;
b) Estrutura assinada com conteúdo digital separado (*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], criada 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 essa esteja de acordo com uma das políticas de assinatura definidas ou aprovadas pela ICP-Brasil (ver item 5.6).

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 - XAdES – XMLdSIG Advanced Electronic Signature

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 com conteúdo digital separado (*detached*): neste caso, o conteúdo digital não está incluído na estrutura XMLSignature;
b) Estrutura assinada com conteúdo digital anexado (*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 O padrão XAdES é uma extensão do XMLSignature, descrita no documento ETSI TS 101903 [10], que provê as assinaturas digitais de informações que permitem sua validação a mais longo prazo.
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 das assinaturas digitais pode ser necessário identificar um subconjunto de opções que sejam apropriadas para as diferentes comunidades de usuários. Tal seleção é chamada de perfil. Exemplos de perfil estão nos documento ETSI TS 102 734 [8] e ETSI TS 102 904 [11].
5.5.4 Para a ICP-Brasil, foi definido um perfil de assinatura para uso geral, baseado nos padrões CadES e XadES, que sintetiza os principais atributos e propriedades a serem utilizados nas assinaturas digitais no País. Podem ser criados outros perfis, para uso em segmentos específicos de atividade, como Governo Eletrônico, se julgado necessário.

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.
5.6.2 Uma assinatura digital é 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 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.
5.6.7 As políticas podem ser criadas pelo signatário, pelo verificador ou por qualquer outra entidade que julgue apropriado fazê-lo.
5.6.8 Na ICP-Brasil, o formato e a estrutura a serem usados para criação de políticas de assinatura estão estabelecidos no DOC-ICP-15.03, que foi elaborado com base nos documentos ETSI TR 102 272 [6] e ETSI TR 102 038 [9].

5.7 Relação entre os 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

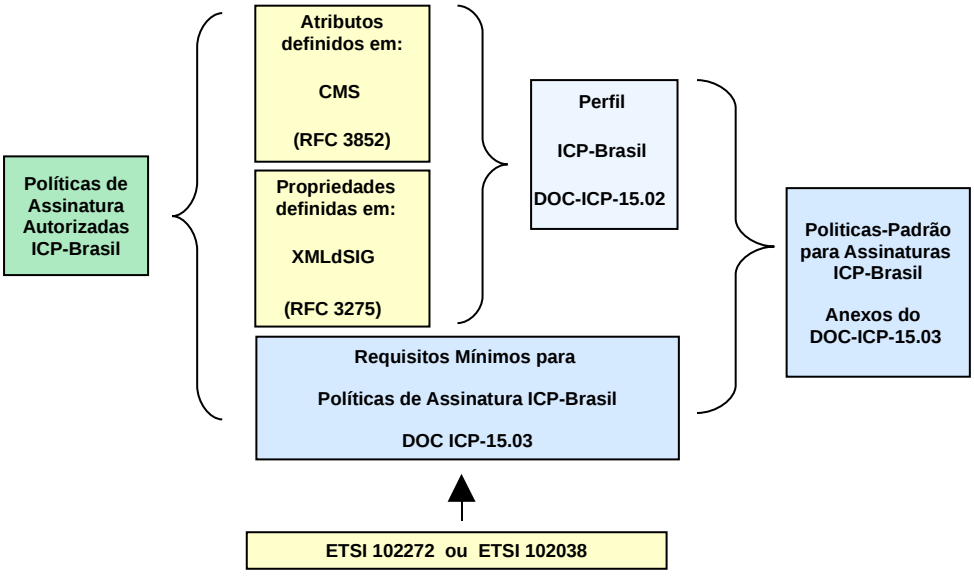

Figura 5.4 – Relação entre padrões internacionais sobre assinatura digital e os documentos ICP-Brasil

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 são geradas de forma paralela e independente pelos signatários, utilizando conteúdos digitais idênticos. Cada co-assinatura gerada pode conter atributos assinados e não 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.
5.9.2 Apesar de a assinatura em lote viabilizar a automação de diversos processos, ela traz o risco de o signatário não tomar conhecimento do conteúdo que esta sendo assinado.

5.10 Formato do documento eletrônico

5.10.1 É recomendado que o documento eletrônico a ser assinado seja criado em formatos públicos, pois possibilitam a recuperação do conteúdo do documento eletrônico mesmo que esses formatos venham a ser descontinuados.
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.
5.10.3 Para possibilitar a interoperabilidade e propiciar a identificação do formato, é recomendada a codificação do documento eletrônico no formato MIME [24], com tipos registrados MIME, antes de sua assinatura.
5.10.4 Para possibilitar a interoperabilidade entre setores do governo, é recomendada a adoção dos formatos definidos no documento de referência e-ping [23].

5.11 Formato do arquivo gerado com a assinatura digital

5.11.1 É RECOMENDADO que os arquivos contendo assinaturas digitais ICP-Brasil sejam gerados com as extensões **p7s** [24] e **xml** [19].

5.12 Referências temporais

5.12.1 As referências temporais são elementos importantes relacionados aos processos de assinatura digital. Existem diversas referências temporais, algumas relacionadas ao instante de geração da assinatura digital e outras relacionadas ao tempo de vida do certificado digital e ao intervalo de validade de uso do certificado digital.

5.12.2 As referências temporais mais relevantes nos processos de assinatura digital são:

a) **Tdec:** Instante de geração da assinatura digital declarado pelo signatário;
b) **Tref:** Instante de verificação de um certificado digital utilizado para gerar uma assinatura digital;
c) **Tec:** Instante de emissão do certificado digital do signatário;
d) **Tivc:** Instante de início do tempo de vida do certificado digital do signatário;
e) **Trc:** Instante de revogação do certificado digital do signatário;
f) **Ttvc:** Instante de término do tempo de vida do certificado digital do signatário.

5.12.3 Essas referências temporais geram alguns intervalos de tempo importantes, a saber:

a) **Ivc:** Intervalo de vida do certificado digital do signatário correspondendo ao intervalo de tempo delimitado por Tivc e Ttvc;
b) **Ivu:** Intervalo de validade de uso do certificado digital do signatário correspondendo ao intervalo de tempo delimitado por Tivc e Min(Trc,Ttvc);

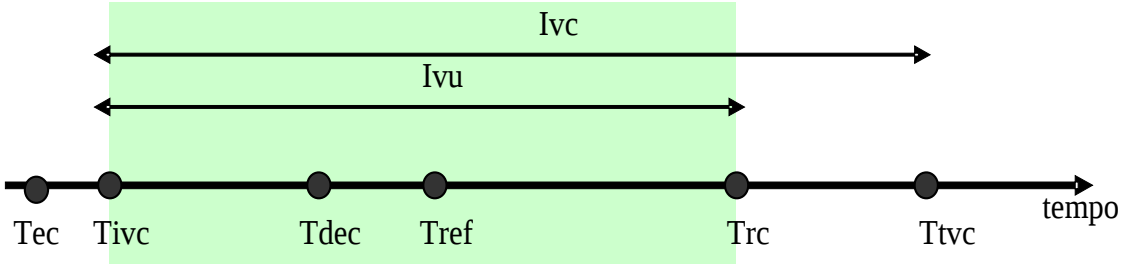

Figura 5.5 Referências Temporais dos Processos de Assinatura Digital

5.12.4 O instante referente a geração de uma assinatura digital a ser utilizado é o **Tdec**. O instante **Tdec** é comumente representado em conteúdos digitais assinados pelo atributo *Signing Time*.
5.12.5 O instante a ser utilizado para verificar o estado de revogação do certificado digital do signatário é o **Tref**. O instante **Tref** pode ser representado por um carimbo do tempo sobre a assinatura.
5.12.6 A Tabela 5.1 mostra as fontes principais de obtenção de algumas referências temporais que são utilizadas nos processos de assinatura digital.

Referência Temporal	Fonte principal
Tdec	Signing time (fonte não confiável)
Tref	Carimbo do tempo de assinatura (fonte confiável)
Tivc	Certificado digital (fonte confiável)
Ttvc	Certificado digital (fonte confiável)
Trc	LCR ou OCSP (fonte confiável)

Tabela 5.1 Referências Temporais e Fontes Principais de Obtenção

5.13 Registros de auditoria

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

5.13.2 Nos registros realizados, é recomendado que no mínimo as seguintes informações estejam presentes:

a) Resultado hash do arquivo assinado ou verificado;
b) Tipo de certificado digital ICP-Brasil utilizado;
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.

5.14 Documento original e cópia

5.14.1 Segundo a UNCITRAL [25], em algumas situações, a legislação impõe restrições ao uso dos meios modernos de comunicação impondo, por exemplo, o uso de documento "escrito", "assinado" e "original".

5.14.2 Com respeito à noção de "escrito", "assinado" e "original", o "Modelo de Lei para Comércio Eletrônico da UNCITRAL" [25] adota o conceito baseado na equivalência funcional.

5.14.3 Em relação especificamente ao conceito de "documento original", em alguns processos já estabelecidos, que utilizam assinatura de documentos em papel, é possível a exigência de "documentos assinados originais". Nesse caso, "documentos assinados originais" são aqueles contendo as assinaturas manuscritas. Esta exigência é decorrente, principalmente, da dificuldade existente de detecção de alterações nas cópias eventualmente produzidas.

5.14.4 No cenário digital, porém, em conteúdos assinados digitalmente não é relevante o conceito de original e cópia. Funcionalmente, original e cópia são equivalentes. Do ponto de vista da validação de alterações não existe diferença entre o original e a cópia. O original e a cópia são idênticos, ou seja, podem ser validados da mesma maneira.

6 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)
[26] RFC 4648 - “The Base16, Base32, and Base64 Data Encodings”
[27] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

7. 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