Infraestrutura de Chaves Públicas Brasileira

VISÃO GERAL SOBRE

ASSINATURAS DIGITAIS NA ICP-BRASIL

DOC-ICP-15

Versão 3.0

25 de agosto de 2015

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 109, de 25/08/2015 (Versão 3.0)	Itens 6.4; 6.5.1; 6.5.4; 6.7.1; 6.8; 6.11.1; 6.12.3; 6.14.5 (novo).	Inclusão da regulamentação PAdES e ajustes de formatação.
Resolução nº 92, de 05/07/2012 (versão 2.1)	Referência 7; 6.4.2.1; figura 6.3, do item 6.7.1; 6.10.3; 6.10.4; 6.12.4 a 6.12;	Altera a referência bibliográfica do CMS, atualização da RFC 3852 para RFC 5652.
Resolução nº 72, de 31/03/2010 (Versão 2.0)	2, 4, 5 e 6	Aprimoramento do texto. O item "3 Terminologia" foi incluído. Atualização das figuras 4.1, 5.1, 6.3 e 6.4.
Resolução nº 62, de 09/01/2009 (Versão 1.0)		Aprova a versão 1.0 do documento Visão Geral Sobre Assinaturas Digitais na ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ASCII	American Stardard Cod for Information Interchange
CAdES	CMS Advanced Electronic Signatures
CMS	Cryptgraphic Message Syntax
e-PING	Padrões de Interoperabilidade de Governo Eletrônico
ETSI	European Telecommunication Standard Institute
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptgraphy Standards
PSC	Provedores de Serviço de Confiança
RFC	Request For Comments
UNCITRAL	United Nations Commission on International Trade Law
W3C	World Wide Web Consortium
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language

LISTA DE FIGURAS

LISTA DE TABELAS

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 Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.3 Ele está organizado da seguinte forma:

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

2 MOTIVAÇÕES

2.1 A ICP-Brasil instituiu uma infraestrutura 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, em que 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 TERMINOLOGIA

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

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

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

3.1.3 RECOMENDADO (R) - Esta expressão, ou o adjetivo "RECOMENDADO", significa que podem existir razões válidas, em circunstâncias particulares, para ignorar um ponto específico, mas as implicações completas precisam ser entendidas e ponderadas cuidadosamente antes de escolher um caminho diferente.

3.1.4 NÃO RECOMENDADO (NR) - Esta expressão significa que podem existir razões válidas, em circunstâncias particulares, em que o comportamento possa ser aceitável ou mesmo útil, mas as implicações completas devem ser entendidas e ponderadas cuidadosamente, antes de se realizar qualquer comportamento descrito com este rótulo.

3.1.5 PODE (P) - Esta palavra, ou o adjetivo "OPCIONAL", significa que é um item verdadeiramente opcional. Um implementador pode optar por incluir o item, enquanto outro pode omitir o mesmo item. Uma aplicação que não inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que inclui aquela opção, embora talvez com funcionalidade reduzida. No mesmo espírito, uma aplicação que inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que não a inclui (exceto, é claro, para o recurso que a opção oferece).

4 DEFINIÇÕES

4.1 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 subsequente neste seja plenamente detectável; e
d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.

4.2 Assinatura eletrônica é o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria.

4.3 BASE 64 é um método de codificação de dados. Permite transformar dados binários (sequência de bytes) em dados no formato American Standard Code for Information Interchange (ASCII), que é imprimível (texto). Assim, possibilita que dados originalmente no formato binário, após a transformação, possam ser transmitidos através de meios que não permitem dados binários **[1]**.

4.4 Cadeia de certificação é uma série hierárquica de certificados assinados por sucessivas Autoridades Certificadoras (ACs). A cadeia de certificação compreende o certificado da entidade final, assinado por uma AC, e zero ou mais certificados de ACs assinados por outras ACs, até o certificado de confiança, porém não incluindo este, conforme descrito na RFC 5280 **[2]**. A Figura 1 ilustra um exemplo de uma cadeia de certificação de um certificado ICP-Brasil.

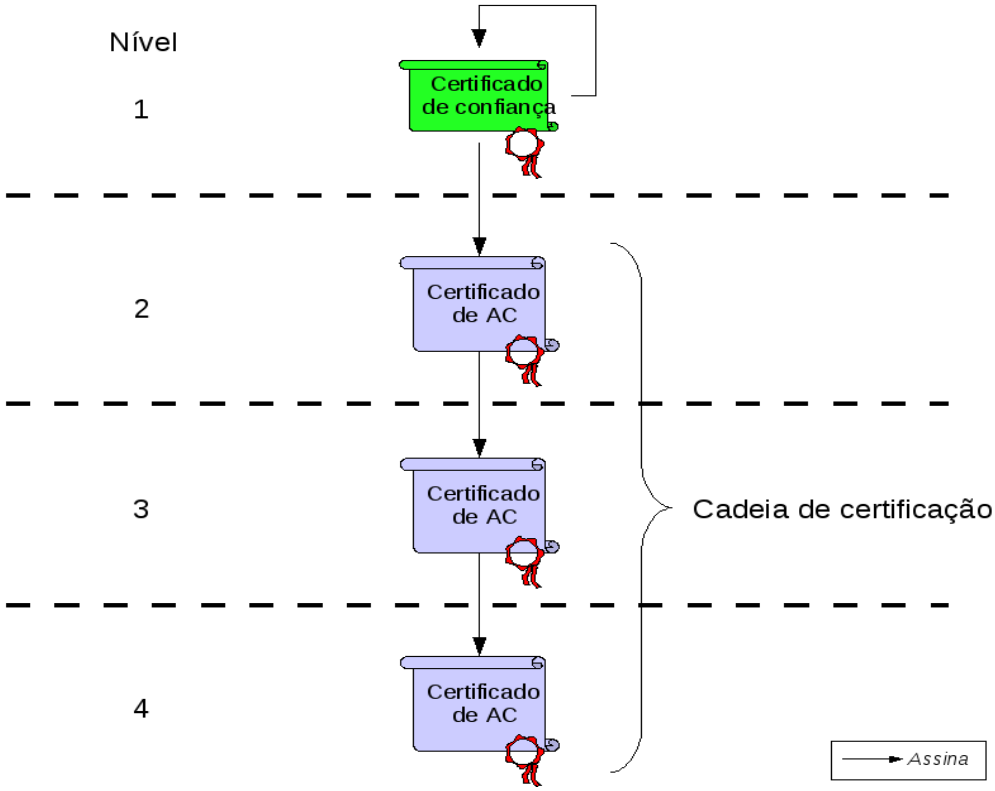

Figura 1: Exemplo de uma cadeia de certificação da ICP-Brasil

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

4.6 Chave de criação de assinatura é o conjunto de dados eletrônicos, tal como chaves criptográficas privadas, utilizado para a criação de uma assinatura eletrônica.

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

4.8 Componentes de aplicação de assinatura são produtos físicos (hardware) e lógicos (software) que:

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

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

4.9 Conteúdo digital é um documento eletrônico sobre o qual se realiza uma assinatura digital.

4.10 Dispositivo seguro de criação de assinaturas é um 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; e
d) não modifique o documento eletrônico a ser assinado.

4.11 Documento eletrônico é uma sequência de bits elaborada mediante processamento eletrônico de dados, destinada a reproduzir uma manifestação do pensamento ou um fato.

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

4.13 Identificador da política de assinatura são dados que identificam de forma unívoca uma política de assinatura, compostos por um *Object Identifier* (OID) - ou seja, um identificador - e o resumo criptográfico da política.

4.14 Resumo criptográfico ou hash é um valor calculado a partir de um documento eletrônico com a ajuda de uma função de resumo criptográfico.

4.15 *Extensible Markup Language* (XML) **[3]** é uma especificação de propósito geral para a criação de linguagens de marcação para necessidades especiais.

5 DOCUMENTOS SOBRE ASSINATURA DIGITAL NA ICP-BRASIL

Os normativos sobre Assinatura Digital na ICP-Brasil são listados na Tabela 1:

Código	Título	Conteúdo
DOC-ICP-15 (este documento)	Visão Geral sobre Assinaturas Digitais na ICP-Brasil	Define os principais conceitos e lista os demais documentos que compõem as normas da ICP-Brasil sobre o assunto.
DOC-ICP-15.01	Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil	Estabelece os requisitos obrigatórios a serem observados na criação e verificação de assinaturas digitais na ICP-Brasil.
DOC-ICP-15.02	Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil	Delimita os atributos a serem usados na geração de assinaturas digitais no âmbito da ICP-Brasil **[4]**.
DOC-ICP-15.03	Requisitos para Políticas de Assinatura Digital na ICP-Brasil	Define o formato, estrutura e sintaxes que devem ser observadas para a criação de novas políticas de assinatura digital. Apresenta, adicionalmente, as políticas padrão e o esquema de gerenciamento de políticas na ICP-Brasil **[5].**

Tabela 1: Organização dos documentos sobre Assinatura Digital na ICP-Brasil

6 PRINCIPAIS CONCEITOS

6.1 Assinatura digital x assinatura eletrônica

6.1.1 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.

6.1.2 A assinatura eletrônica, portanto, pode ser obtida por meio de diversos dispositivos ou sistemas, como login/senha, biometria, impostação de *Personal Identification Number* (PIN) etc.

6.1.3 Um dos tipos de assinatura eletrônica é a assinatura digital, que utiliza um par de chaves criptográficas associado a um certificado digital. Uma das chaves – a chave privada – é usada durante o processo de geração de assinatura e a outra – chave pública, contida no certificado digital – é usada durante a verificação da assinatura.

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

6.1.5 No contexto destes normativos é assumido que as assinaturas digitais são produzidas com a utilização de chaves criptográficas privadas associadas a certificados digitais ICP-Brasil.

6.2 Entidades envolvidas na assinatura digital

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

a) Signatário ou assinante é uma entidade que cria a assinatura digital;
b) Verificador é uma ou mais entidades que validam a assinatura digital;
c) Mediador ou árbitro é uma pessoa ou entidade que pode ser chamada para arbitrar a disputa entre o signatário e o verificador 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 apoiam o signatário e o verificador por meios de serviços de suporte, como emissão de certificados digitais, de Listas de Certificados Revogados (LCR) ou de respostas de Online Certificate Status Protocol (OCSP), emissão de carimbos do tempo.

6.3 Ciclo de vida de uma assinatura digital

6.3.1 O ciclo de vida de uma assinatura digital compreende os processos descritos na Tabela 2.

Processo	Descrição
Criação	Criação de um código logicamente associado a um conteúdo digital e à chave criptográfica privada do signatário.
Verificação ou validação	Verificação quanto à validade de uma ou mais assinaturas digitais logicamente associadas a um conteúdo digital.
Armazenamento	Guarda da assinatura digital. Compreende os cuidados para conversão dos dados para mídias mais atuais, sempre que necessário.
Revalidação	Processo que estende a validade do documento assinado, por meio da reassinatura 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 criptográficos ou tamanhos de chave utilizados.

Tabela 2: Ciclo de Vida de uma Assinatura Digital

6.3.2 É recomendado que as assinaturas digitais sejam criadas com características apropriadas à finalidade e longevidade esperada. Uma assinatura digital pode incorporar elementos que permitam uma validação confiável a longo prazo, o que, em contrapartida, aumenta o tamanho do arquivo e o tempo gasto na geração da assinatura.

6.3.3 A Figura 2 apresenta, de forma simplificada, o processo criptográfico de criação de uma assinatura digital:

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

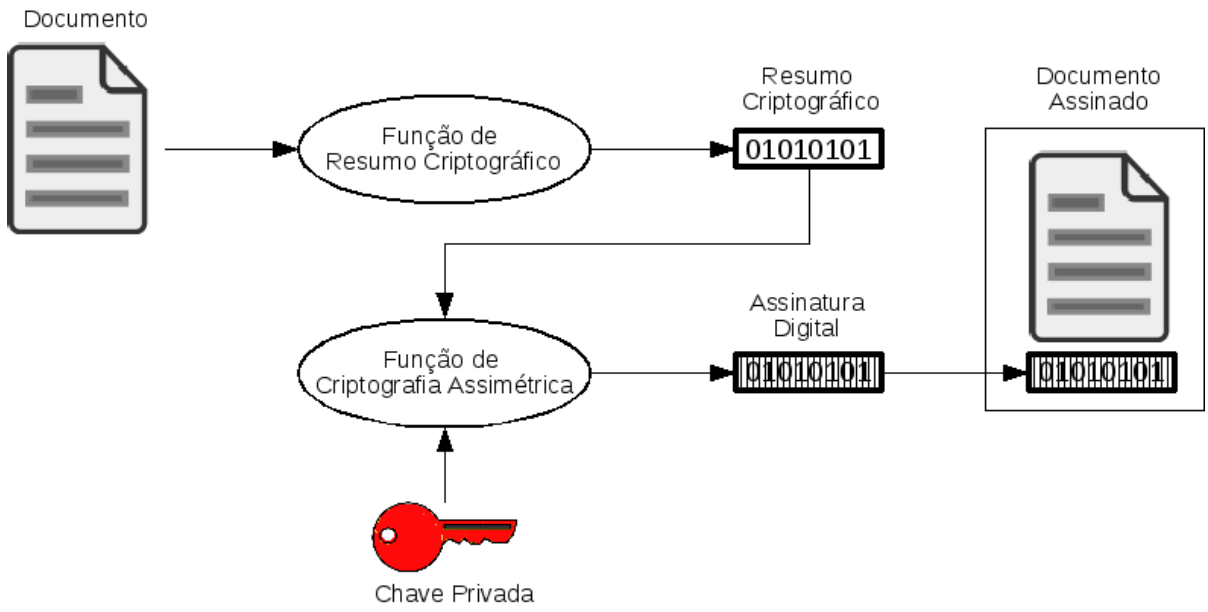

Figura 2: Diagrama simplificado de criação de assinatura digital

6.3.4 A Figura 3 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 resumo criptográfico do documento eletrônico;
c) o verificador decifra a assinatura digital com a chave pública do signatário, contida no certificado digital, obtendo o resumo criptográfico gerado e cifrado pelo signatário no momento da assinatura;
d) o verificador compara os resumos criptográficos 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.

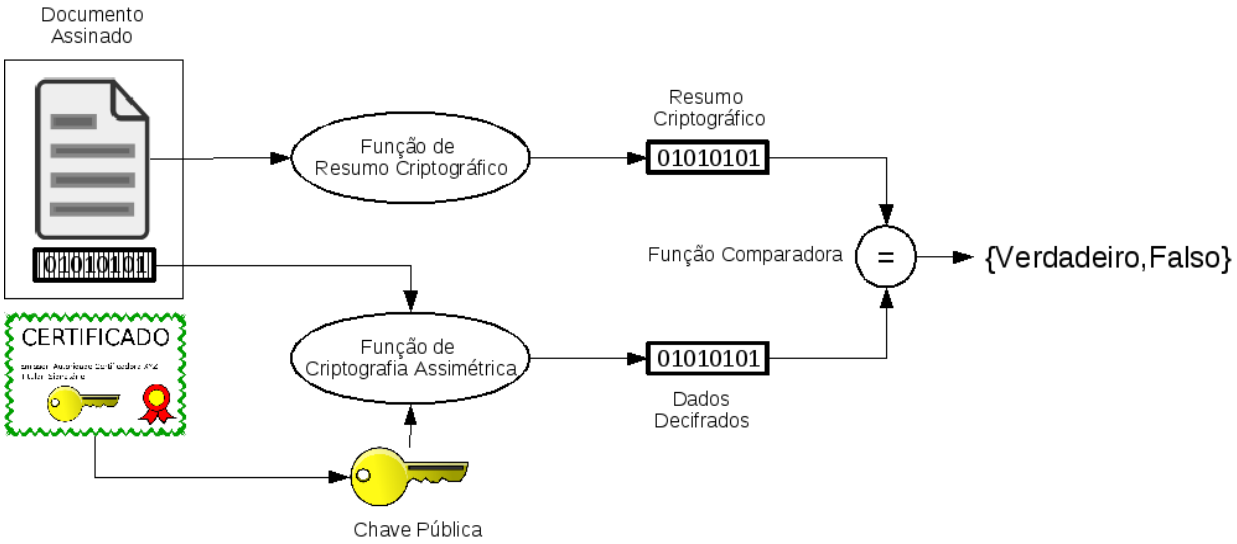

Figura 3: Diagrama simplificado de verificação de assinatura digital

6.4 Padrões para assinatura digital

6.4.1 Na ICP-Brasil podem ser usados três formatos para representação de assinaturas digitais:

a) assinatura eletrônica avançada sobre o CMS;
b) assinatura eletrônica avançada sobre o XMLDsig;
c) assinatura eletrônica avançada sobre o PDF.

6.4.2 CMS *Advanced Electronic Signature*

6.4.2.1 O padrão CMS é uma evolução do padrão *Public-Key Cryptography Standards* #7 (PKCS#7) [6]. A versão CMS utilizada como referência neste documento é a descrita na RFC 5652 [7]. O padrão CMS descreve uma estrutura para armazenamento de conteúdos (dados) assinados digitalmente, conteúdos cifrados, conteúdos autenticados e conteúdos com resumos criptográficos. Este documento trata especificamente do tipo de conteúdo *Signed-data*, relevante para o contexto de assinatura digital.

6.4.2.2 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.

6.4.2.3 Quando usado para representar o conteúdo digital assinado, a inclusão 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.

6.4.2.4 Além dos atributos assinados (ou seja, que fazem parte do cálculo do resumo criptográfico, 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 Seção 6.9). O CMS não permite, todavia, assinar partes de um documento, somente o documento como um todo.

6.4.2.5 O CMS *Advanced Electronic Signature* (CAdES) é uma extensão do padrão CMS, descrita no documento ETSI TR 102 733 **[8]**, criada com vistas a prover as assinaturas digitais de informações que permitam sua validação por longo prazo.

6.4.2.6 CAdES-ICP-Brasil é toda assinatura no formato CAdES que, além de seguir os requisitos de Assinatura Digital ICP-Brasil, descritas na Seção 4.1, possui um identificador de política de assinatura pertencente ao conjunto de políticas de assinatura divulgadas e aprovadas conforme o DOC-ICP 15.03 **[5]**.

6.4.2.7 A validação de uma assinatura digital de acordo com o padrão CAdES-ICP-Brasil deve exigir que essa assinatura esteja de acordo com uma das políticas de assinatura aprovadas pela ICP-Brasil (ver Seção 6.6).

6.4.2.8. 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.

6.4.3 XMLDSig *Advanced Electronic Signature*

6.4.3.1 Em XML utiliza-se o *XMLSignature* **[9]** para a representação de assinaturas digitais, cuja especificação é mantida pelas organizações *World Wide Web Consortium* (W3C) e *Internet Engineering Task Force* (IETF).

6.4.3.2 Sua última especificação é dada pela RFC 3275 **[10]**. 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.

6.4.3.3 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.

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

6.4.3.5 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.

6.4.3.6 O padrão XML *Advanced Electronic Signature* (XAdES) é uma extensão do *XMLSignature*, descrita no documento ETSI TS 101 903 [11]. Promove, de maneira semelhante ao CAdES, padronização de formatos de assinaturas, os quais incluem formatos para assinaturas de longo prazo.

6.4.3.7 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.

6.4.3.8 XAdES-ICP-Brasil é toda assinatura no formato XAdES que, além de seguir os requisitos de Assinatura Digital ICP-Brasil, descritas na Seção 4.1, possui um identificador de política de assinatura pertencente ao conjunto de políticas de assinatura divulgadas e aprovadas conforme o DOC-ICP 15.03 **[5]**.

6.4.3.9 A validação de uma assinatura digital de acordo com o padrão XAdES-ICP-Brasil deve exigir que essa assinatura esteja de acordo com uma das políticas de assinatura aprovadas pela ICP-Brasil (ver Seção 6.6).

6.4.4 PDF *Advanced Electronic Signature*

6.4.4.1 O padrão PDF – *Portable Document Format* - é um formato de arquivo definido nas especificações da PDF ISO 32000-1 [20] para codificação de documentos eletrônicos que apresenta aparência exata que os documentos terão se forem impressos.

6.4.4.2 O PDF *Advanced Electronic Signature* (PAdES) é um formato específico para assinaturas eletrônicas avançadas construídas sobre o padrão PDF ISO 32000-1 **[20]** e descrita nos documentos ETSI TS 102 778 partes 1 à 6, criada com vistas a prover as assinaturas digitais de informações que permitam sua validação por longo prazo.

6.4.4.3 O PDF possui uma estrutura para suportar e incluir informações relevantes às assinaturas digitais. Nessa estrutura, um CMS é o padrão de assinatura digital usado para proteger os dados assinados.

6.4.4.4 O PAdES deve ser usado sempre em documentos no padrão PDF. Um CMS *detached* é inserido dentro da estrutura de dados do PDF. O conteúdo assinado pelo CMS deve ser todos os *bytes* do PDF, menos o bloco de *bytes* do próprio CMS.

6.4.4.5 Pelo fato de existir uma estrutura no PDF para armazenar algumas informações sobre a assinatura, há algumas restrições quanto ao uso dos atributos no CMS. Essas restrições estão descritas no documento DOC-ICP-15.02 **[4]** na Tabela 7. Um exemplo disso é a hora que o assinante declara que assinou, pois no PDF há uma entrada no dicionário de assinatura, chamada de "M", e no CMS há um atributo assinado, chamado de "*signing-time*". Como os dois possuem a mesma informação, quando for de interesse do desenvolvedor incluir tal informação na assinatura, então, a entrada "M" deve ser codificada e o atributo "*signing-time*" não deve ser codificado.

6.4.4.6 PAdES-ICP-Brasil é toda assinatura no formato PAdES que, além de seguir os requisitos de Assinatura Digital ICP-Brasil, descritas na Seção 4.1, possui um identificador de política de assinatura pertencente ao conjunto de políticas de assinatura divulgadas e aprovadas conforme o DOC-ICP 15.03 **[5]**.

6.4.4.7 A validação de uma assinatura digital de acordo com o padrão PAdES-ICP-Brasil deve exigir que essa assinatura esteja de acordo com uma das políticas de assinatura aprovadas pela ICP-Brasil (ver Seção 6.6).

6.4.4.8 Como uma assinatura PAdES é diretamente relacionada com um arquivo PDF, é necessário que o arquivo PDF esteja na versão 1.7 para que todas as características do PAdES funcionem corretamente em um leitor PDF aderente ao padrão PDF ISO 32000-1 **[20]**. Adicionalmente, no documento ETSI TS 102 778-4 **[16]**, em sua seção 4.4, é descrito o uso de extensões de dicionário, que são estruturas usadas para informar ao leitor PDF aderente que aquele PDF possui determinadas características.

6.4.4.9 O PAdES também admite que se incorporem às assinaturas digitais dados adicionais, 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.

6.4.4.10 O PAdES permite que as assinaturas fiquem visíveis aos usuários que estão "lendo" o documento assinado. No entanto, essa visualização não substitui a validação da assinatura nem acrescenta segurança ao processo. Nesta representação visual podem ser inclusas imagens sem vínculo com o assinante.

6.5 Perfis de assinatura digital

6.5.1 Os padrões CAdES, XAdES e PAdES disponibilizam uma diversificada gama de atributos, propriedades ou entradas de dicionários, que permitem às entidades envolvidas incorporar às assinaturas digitais informações com os mais diferentes objetivos.

6.5.2 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.

6.5.3 Para maximizar a interoperabilidade das assinaturas digitais é 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 **[12]** e ETSI TS 102 904 **[13]**.

6.5.4 Para a ICP-Brasil, foi definido um perfil de assinatura para uso geral, baseado nos padrões CAdES, XAdES e PAdES, que sintetiza os principais atributos e propriedades a serem utilizados nas assinaturas digitais. Podem ser criados outros perfis, para uso em segmentos específicos de atividade, como Governo Eletrônico, se julgado necessário.

6.6 Políticas de assinatura

6.6.1 Uma política de assinatura é um conjunto de regras que formaliza os processos de criação e verificação de uma assinatura digital e define as bases para que a assinatura digital possa ser considerada válida.

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

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

6.6.4 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.

6.6.5 Na ICP-Brasil, o formato e a estrutura a serem usados para criação de políticas de assinatura estão estabelecidos no DOC-ICP-15.03 **[5]**, que foi elaborado com base nos documentos ETSI TR 102 272 **[14]** e ETSI TR 102 038 **[15]**.

6.7 Relação entre os padrões internacionais e os documentos ICP-Brasil

6.7.1 A Figura 4 ilustra a relação existente entre os padrões internacionais que tratam de assinatura digital, os perfis e políticas de assinatura e demais documentos ICP-Brasil

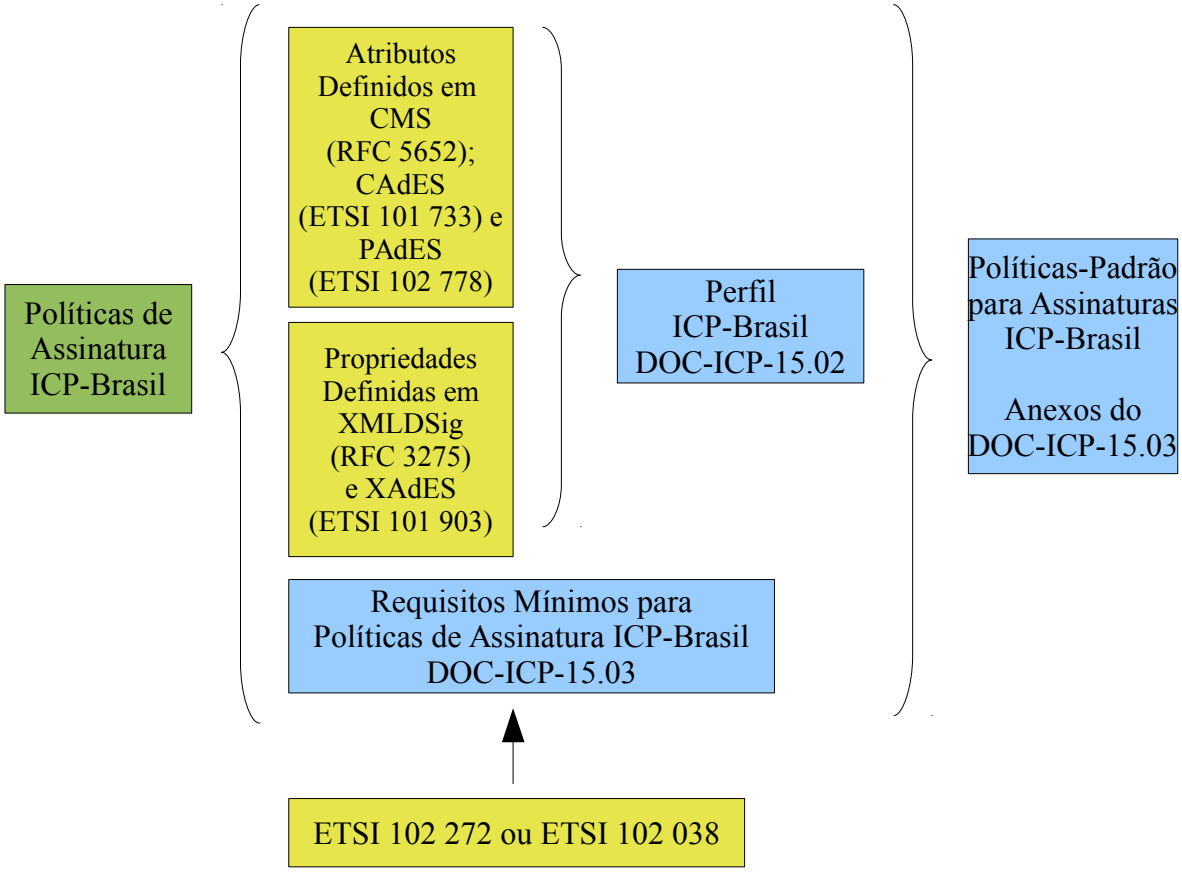

Figura 4: Relação entre padrões internacionais sobre assinatura digital e os documentos ICP-Brasil

6.8 Documentos eletrônicos com mais de uma assinatura digital

6.8.1 Com relação ao processo de geração de assinatura digital, podemos ter contextos diferentes:

a) assinaturas digitais simples, coassinaturas digitais e contra-assinaturas digitais, para assinaturas baseadas no padrão *CAdES* e *XAdES*; e
b) assinaturas digitais simples e assinaturas digitais seriais, para assinaturas baseadas no padrão PAdES.

6.8.1.1 Assinatura Simples - A geração de assinatura digital simples ocorre quando uma única assinatura digital é gerada sobre um conteúdo digital disponível. Esta propriedade pode ocorrer para os padrões CAdES, XAdES e PAdES. A Figura 5 apresenta a implementação de uma assinatura simples.

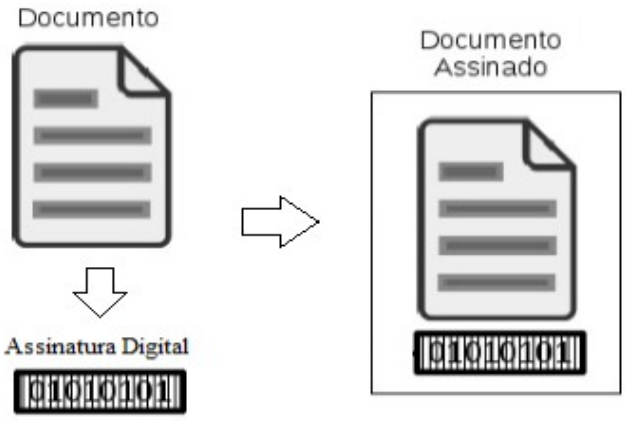

Figura 5: Assinatura simples em um documento

6.8.1.2 Coassinatura - A geração de coassinaturas digitais ou assinatura paralela ocorre quando duas ou mais assinaturas digitais são geradas de forma paralela e independente pelos signatários, utilizando conteúdos digitais idênticos. Cada coassinatura gerada pode conter atributos assinados e não assinados próprios. Esta propriedade ocorre somente para os padrões CAdES e XAdES. A Figura 6 apresenta a implementação de coassinaturas.

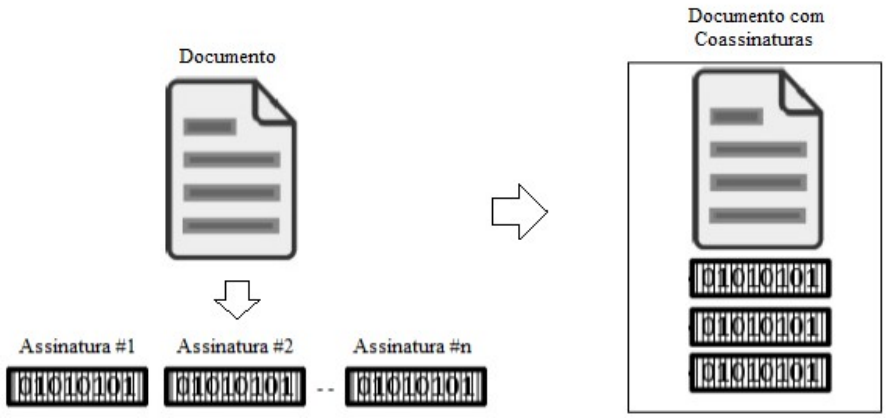

Figura 6: Coassinaturas em um documento

6.8.1.3 Contra-assinatura - A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre a sequência de bytes (bloco) que representa uma assinatura digital já existente. Uma contra-assinatura pode conter outros atributos assinados próprios. Esta propriedade ocorre somente para os padrões CAdES e XAdES. A Figura 7 apresenta a implementação de contra-assinatura.

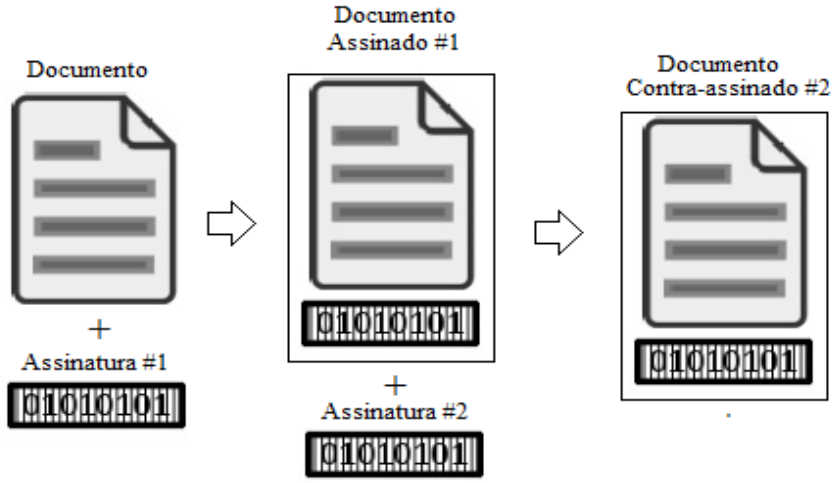

Figura 7: Contra-assinatura em um documento

6.8.1.4 Assinatura Serial - A geração de assinaturas digitais seriais, conforme definido no ETSI TS 102 778.1-2009 [16], ocorre quando uma assinatura digital é realizada sobre toda a estrutura do documento assinado, inclusive assinaturas anteriores, quando houver. Esta propriedade pode ocorrer somente no padrão PAdES. A Figura 8 apresenta a implementação de assinaturas seriais em PDF.

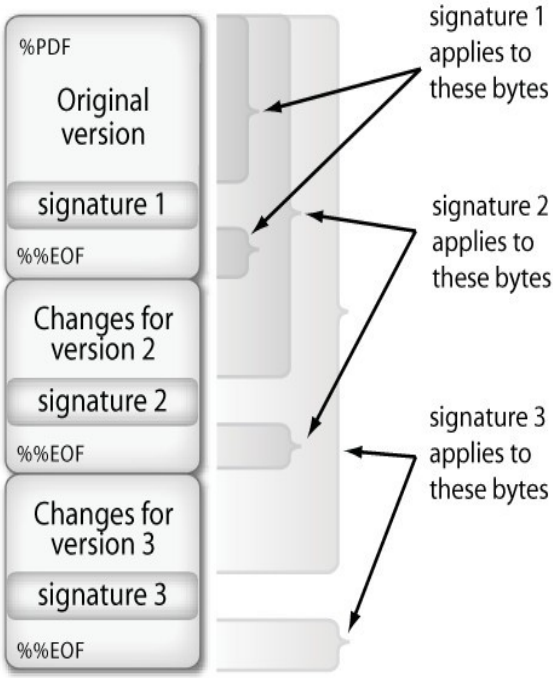

Figura 8: Assinatura Serial em PDF

Fonte: ETSI.org

6.9 Assinaturas digitais em lote

6.9.1 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 sequenciais utilizando a mesma chave assimétrica privada do signatário.

6.9.2 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 está sendo assinado.

6.10 Formato do documento eletrônico

6.10.1 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.

6.10.2 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.

6.10.3 Para possibilitar a interoperabilidade entre setores do governo, é recomendada a adoção dos formatos definidos no documento de referência e-PING **[17]**.

6.11 Formato do arquivo gerado com a assinatura digital

6.11.1 É RECOMENDADO que os arquivos com assinaturas digitais ICP-Brasil sejam gerados com as extensões p7s **[18]**, xml **[9]** e pdf**[20]**.

6.12 Referências temporais

6.12.1 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.

6.12.2 As referências temporais e os intervalos de tempo mais relevantes nos processos de assinatura digital são descritos na Tabela 3.

Referência/Intervalo	Descrição
Tdec	Instante de geração da assinatura digital declarado pelo signatário
Tref	Instante de verificação de um certificado digital utilizado para gerar uma assinatura digital
Tec	Instante de emissão do certificado digital do signatário
Tivc	Instante de início do tempo de vida do certificado digital do signatário
Trc	Instante de revogação do certificado digital do signatário
Ttvc	Instante de término do tempo de vida do certificado digital do signatário
Ivc	Intervalo de vida do certificado digital do signatário correspondendo ao intervalo de tempo delimitado por Tivc e Ttvc
Ivu	Intervalo de validade de uso do certificado digital do signatário correspondendo ao intervalo de tempo delimitado por Tivc e o valor mínimo entre o Trc e o Ttvc, o que ocorrer primeiro

Tabela 3: Referências Temporais e Intervalos de Tempo

A Figura 9 ilustra essas referências temporais e os intervalos de tempo.

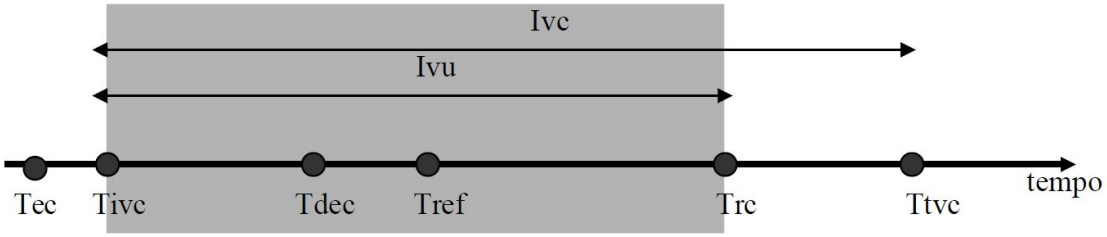

Figura 9: Referências Temporais dos Processos de Assinatura Digital

6.12.3 O instante referente a geração de uma assinatura digital a ser utilizado é o Tdec. O instante Tdec é comumente representado no CMS/CAdES pelo atributo *id-signingTime,* em XML-DSIG/XAdES pela propriedade *SigningTime* e em PDF/PAdES pela chave de entrada M do dicionário de assinatura.

6.12.4 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.

6.12.5 A Tabela 4 mostra as fontes principais de obtenção de algumas referências temporais que são utilizadas nos processos de assinatura digital.

Referência Temporal	Fonte Principal	Confiabilidade na Fonte Principal
Tdec	Data declarada	Não
Tref	Carimbo do tempo de assinatura	Sim
Tivc	Certificado digital	Sim
Ttvc	Certificado digital	Sim
Trc	LCR ou OCSP	Sim

Tabela 4: Principais fontes de obtenção de referências temporais

6.13 Registros de auditoria

6.13.1 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 (*logs*) de suas atividades.

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

a) resumo criptográfico 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.

6.14 Documento original e cópia

6.14.1 Segundo a United Nations Commission on International Trade Law (UNCITRAL) **[19]**, 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".

6.14.2 Com respeito à noção de "escrito", "assinado" e "original", o "Modelo de Lei para Comércio Eletrônico da UNCITRAL" **[19]** adota o conceito baseado na equivalência funcional.

6.14.3 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.

6.14.4 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.

6.14.5 Importante destacar que no padrão PAdES um conteúdo assinado digitalmente acrescenta conteúdo digital ao arquivo PDF, embora preserve dentro do arquivo PDF o conteúdo original.

BIBLIOGRAFIA

[1] JOSEFSSON, S. The Base16, Base32, and Base64 Data Encodings. IETF, out. 2006. RFC 4648 (Proposed Standard). (Request for Comments, 4648). Disponível em: <http://www.ietf.org/rfc/rfc4648.txt>.

[2] COOPER, D. et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF, maio 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

[3] CONSORTIUM, W. W. W. Extensible Markup Language (XML). fev. 1998. Disponível em: <http://www.w3.org/XML/>.

[4] ITI. Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil. v.1.0. Brasília. DOC-ICP-15.02.

[5] ITI. Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil. v.1.0. Brasília. DOC-ICP-15.03.

[6] KALISKI, B. PKCS #7: Cryptographic Message Syntax Version 1.5. IETF, mar. 1998. RFC 2315 (Informational). (Request for Comments, 2315). Disponível em: <http://www.ietf.org/rfc/rfc2315.txt>.

[7] HOUSLEY, R. Cryptographic Message Syntax (CMS). IETF, set. 2009. RFC 5652 (Internet Standard). (Request for Comments, 5652). Obsoletes RFC 3852. Disponível em: <http://www.ietf.org/rfc/rfc5652.txt>.

[8] ETSI. CMS Advanced Electronic Signatures (CAdES). 1.7.4. ed. [S.l.], 2008. Acesso em: 23/02/2009.

[9] EASTLAKE, D. E.; REAGLE, J. M.; SOLO, D. XML-Signature Syntax and Processing. fev. 2002. World Wide Web Consortium, Recommendation REC-xmldsig-core-20020212.

[10] 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>.

[11] ETSI. XML Advanced Electronic Signatures (XAdES). 1.3.2. ed. [S.l.], 2006. Acesso em: 23/02/2009.

[12] ETSI. Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES). 1.1.1. ed. [S.l.], 2007. Acesso em: 23/02/2009.

[13] ETSI. Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES). 1.1.1. ed. [S.l.], 2002. Acesso em: 23/02/2009.

[14] ETSI. ASN.1 format for signature policies. 1.1.1. ed. [S.l.], 2003. Acesso em: 23/02/2009.

[15] ETSI. XML Format for Signature Policies. 1.1.1. ed. [S.l.], 2002. Acesso em: 23/02/2009.

[16] ETSI. PDF Advanced Electronic Signature Profiles; Parte 1: PAdES Overview. 1.1.1. ed 2009. Acesso em: 20/01/2015.

[17] ELETRONICO, 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.

[18] DUSSE, S. et al. S/MIME Version 2 Message Specification. IETF, mar. 1998. RFC 2311 (Informational). (Request for Comments, 2311). Disponível em: <http://www.ietf.org/rfc/rfc2311.txt>.

[19] NATIONS, U. United Nations Commission on International Trade Law, Model Law on Electronic Signatures with Guide to Enactment. 2001. Disponível em: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>. Acesso em: 11 ago. 2009.

[20] PDF ISO 32000-1. Document Management – Portable Document Format – Part 1: PDF 1.7. First Edition – 01/07/2008.

[21] ETSI. PDF Advanced Electronic Signature Profiles; Parte 4: PAdES Long Term – PAdES LTV Profile. 1.1.2. ed 2009. Acesso em: 20/03/2015.