INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

PAdES – Novo Padrão Brasileiro de Assinatura Digital

Wilson R Hirata

Agenda

- O Padrão de Assinatura ICP-Brasil
- Formato de Políticas de Assinatura
- PAdES ICP-Brasil
- A Regulamentação
- Embasamento Técnico
- Dúvidas

Padrão Brasileiro de Assinatura Digital

Padrão Brasileiro de Assinatura Digital

DOC-ICP-15 Visão Geral sobre Assinaturas Digitais na ICP-Brasil - v.2.1

DOC-ICP-15.01 Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil - v.2.1

DOC-ICP-15.02 Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil - v.2.1

DOC-ICP-15.03 Requisitos das Políticas de Assinatura Digital na ICP-Brasil - v.6.1

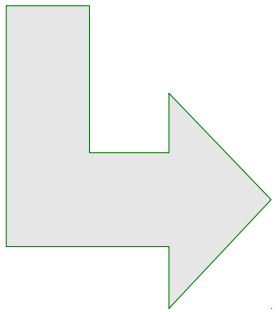
http://iti.gov.br/legislacao/143-icp-brasil/legislacao/790-doc-icp

Políticas de Assinatura Digital

- Oferece clareza, transparência e publicidade às regras de criação e validação;
- Formaliza as condições de validade de documentos assinados digitalmente;
- Preservação de informações e referências (evidências) em futuras verificações ou esclarecer eventuais conflitos (via perícia);
- Proporciona interoperabilidade.

Políticas de Assinatura - formatos disponíveis

- 5 formatos mapeados no CAdES (CMS);
- 5 formatos mapeados no XAdES (XML).



- Artefatos ASN.1 recebidos em 11/05/2010
  - LPA ASN.1 codificada em DER
  - AD-RB ASN.1 codificada em DER
  - AD-RT ASN.1 codificada em DER
  - AD-RV ASN.1 codificada em DER
  - AD-RC ASN.1 codificada em DER
  - AD-RA ASN.1 codificada em DER
- Artefatos XML recebidos em 11/05/2010
  - LPA XML
  - AD-RB XML
  - AD-RT XML
  - AD-RV XML
  - AD-RC XML
  - AD-RA XML

Referências aos padrões e normas internacionais

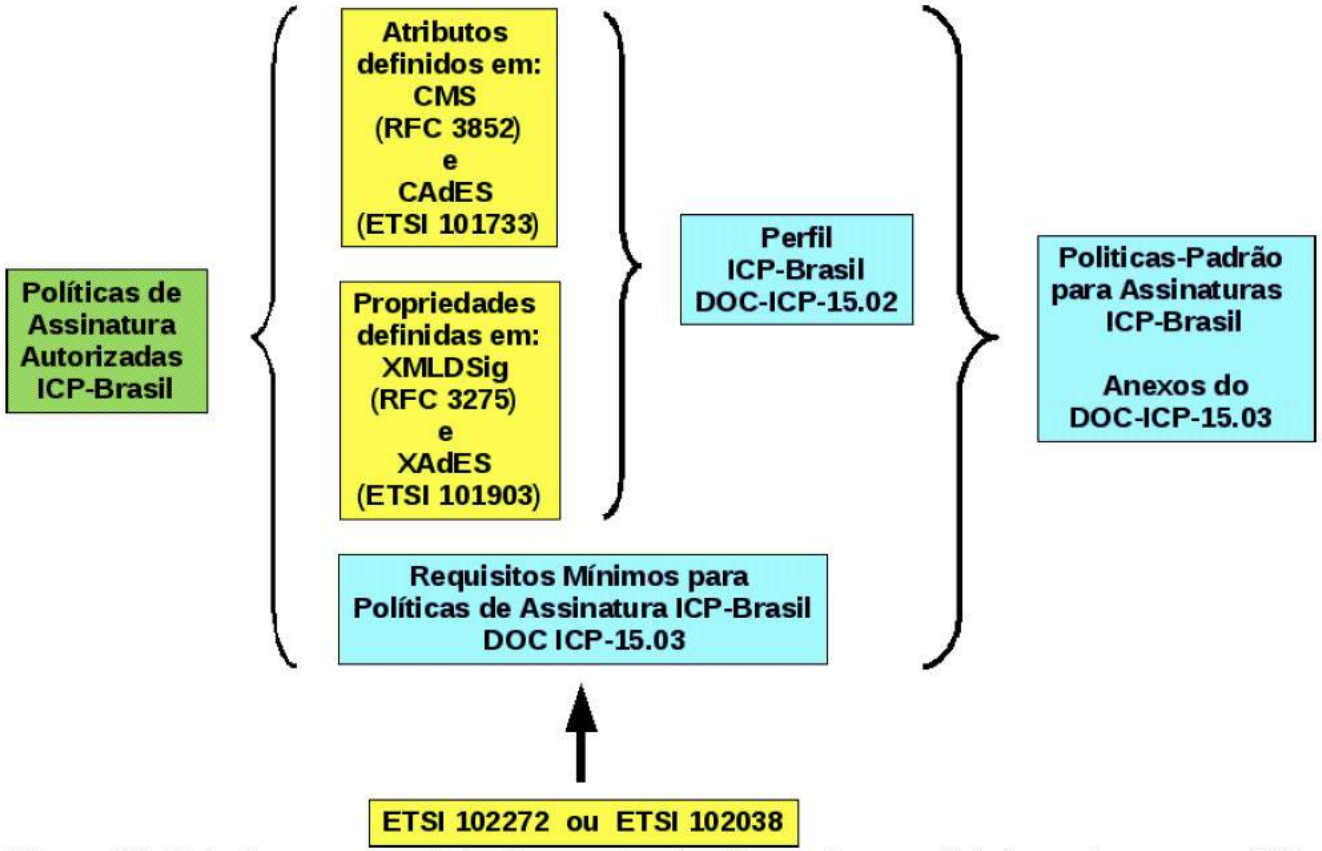
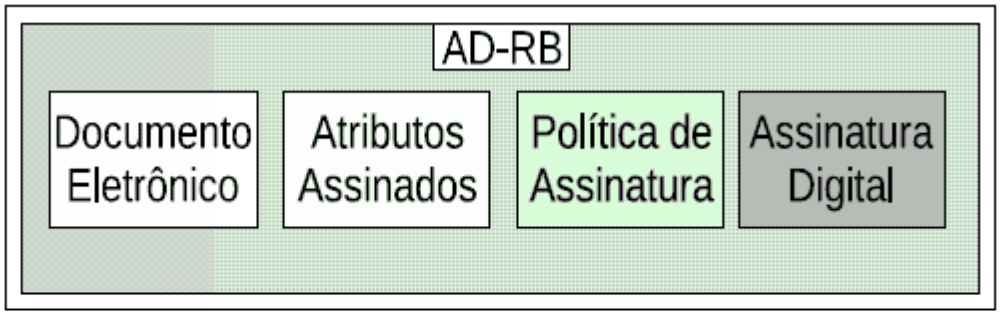


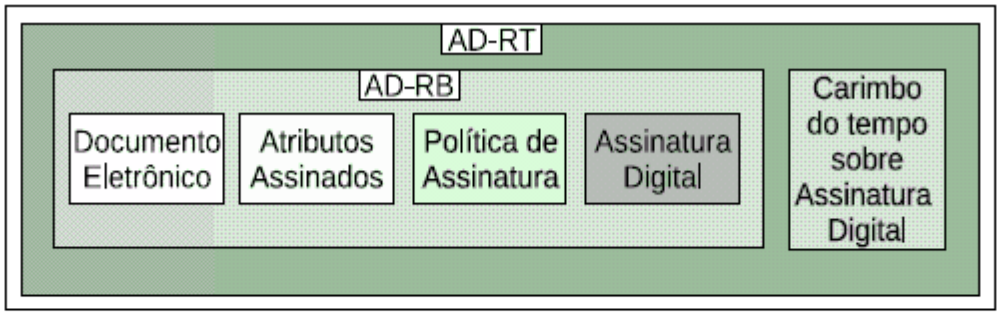
Figura 6.3: Relação entre os padrões internacionais sobre assinatura digital e os documentos ICP-Brasil

AD de referência básica
AD-RB



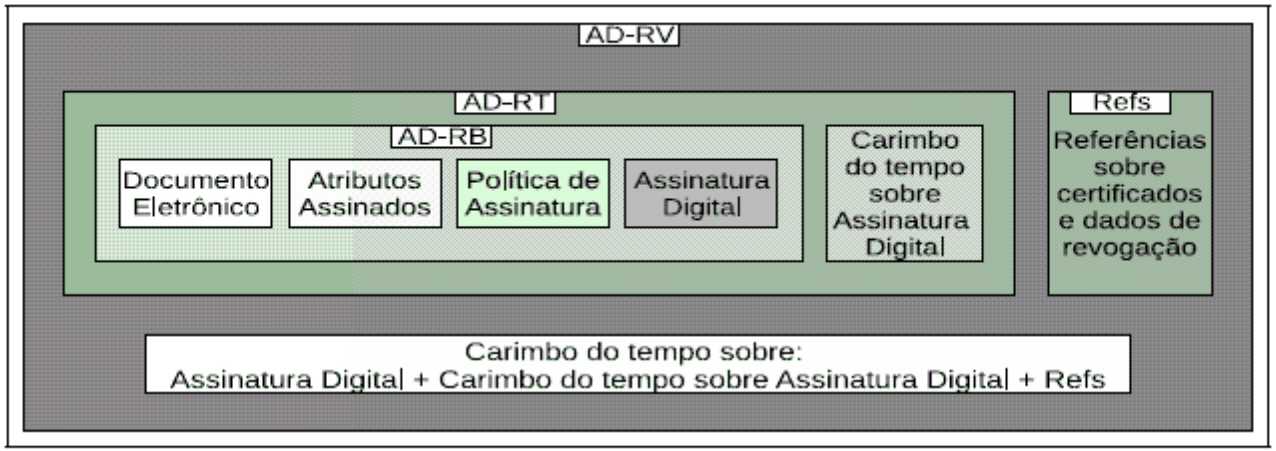
- **Campo de Aplicação**
  - segurança na autenticação do signatário
  - integridade do conteúdo digital
  - sem referências temporais
  - múltiplas assinaturas

AD com referência de tempo
AD-RT



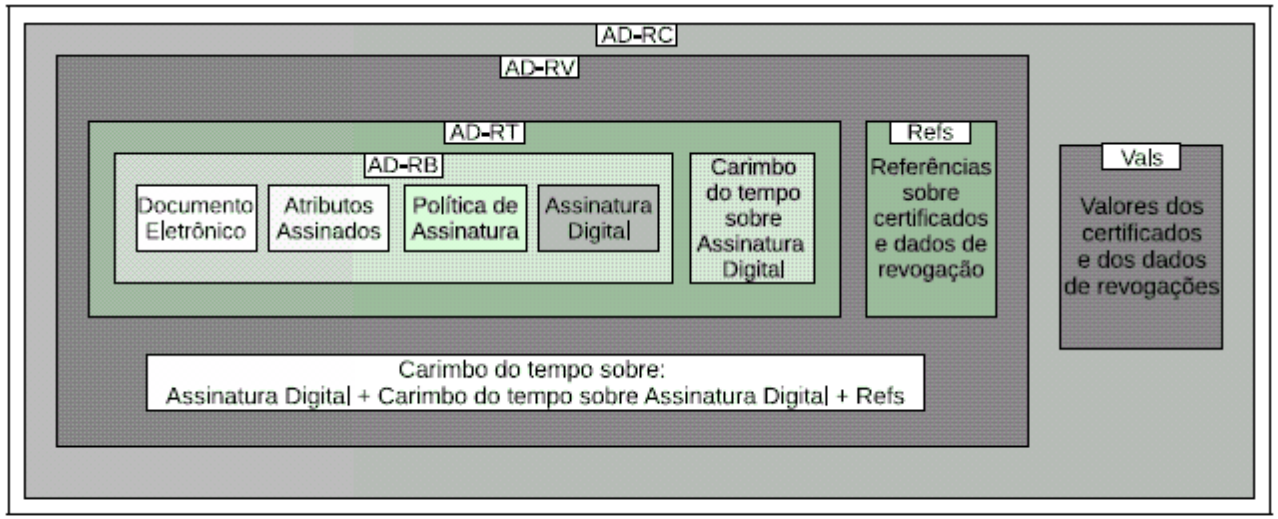
- **Campo de Aplicação**
  - além das propriedades da AD-RB, maior segurança em relação à irretratabilidade do momento de geração
  - referência de tempo
  - LCRs ou respostas OCSP (referências de revogação) obtidos externamente.

AD com referência de validação AD-RV



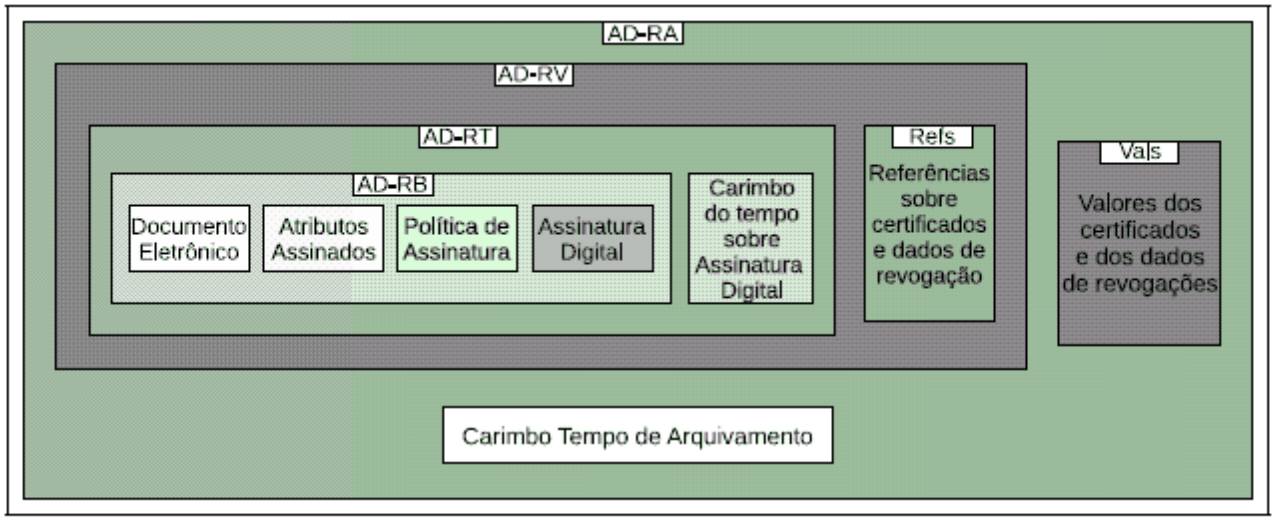
- **Campo de Aplicação**
  - inclui referências sobre a cadeia de certificação
  - referências de revogação (LCR ou resposta OCSP)
  - proteção de mais um carimbo do tempo

AD com referência completa AD-RC



- **Campo de Aplicação**
  - além das referências, guarda os valores da LCR ou resposta OCSP
  - requer maior capacidade de armazenamento
  - possibilita a validação mesmo em situação de contingência da AC

AD com referência para arquivamento AD-RA



- **Campo de Aplicação**
  - além de todas as propriedades anteriores, segurança arquivamento por longos períodos
  - inclusão de novos carimbos do tempo
  - manutenção da segurança criptográfica

O PAdES

- PAdES – PDF *Advanced Electronic Signatures*;

- Baseado nas especificações do ETSI;

- PDF é um formato aberto, normatizado pela ISO 32.000-1 (2008);

- Característica principal é permitir a visualização eletrônica da mesma forma que a impressa.

Breve Histórico do PAdES na ICP-Brasil

- **2012** - CGICP-Br demandou criação de GT para proposição de regulamentação do PAdES na ICP-Brasil;
- **2013** – CGICP-Br aprovou proposta de regulamentação do PAdES na ICP-Brasil baseado em Políticas de Assinatura, em similaridade com CAdES e XAdES, já regulamentado;
  - CGICP-Br demandou a criação de GT para especificar a regulamentação PAdES-ICP-Brasil;
- **2015** – GT PAdES concluiu a regulamentação e colocou a especificação em consulta pública;
  - GT PAdES promoveu ajustes e submeteu ao CGICP-Br;
  - ITI estabeleceu cooperação com UnB para desenvolvimento de *Plug-in* PAdES ICP-Brasil.

PAdES na ICP-Brasil

- Uso de extensões para implementação das Políticas de Assinatura e LPAs;
- Criação de 4 Políticas de Assinatura e não 5 conforme CAdES e XAdES:
  - Referência Básica – AD-RB;
  - Referência do Tempo – AD-RT;
  - Referências Completas – AD-RC;
  - Referências para Arquivamento – AD-RA.
- Necessidade de *Plugin* para visualizadores de PDF (*Readers*) se tornarem potenciais verificadores de assinatura PAdES ICP-Brasil.

O PAdES na ICP-Brasil

- Facilita o intercâmbio de documentos eletrônicos assinados digitalmente;

- Possui recursos de visualização avançada com foco no usuário comum;

- Adota padrão aberto para criação e validação;

- Possibilita validação de assinaturas digitais com uso aplicações preexistentes e abertas;

- Conformidade com o e-PING.

A Regulamentação

- Políticas Assinatura ETSI Estendida atende a demanda da ICP-Brasil
- Testes realizados não apresentaram inconsistência nos aplicativos leitores de PDF
- Mantém similaridade com PAs já regulamentadas

Referências ETSI

Especificações PAdES (série ETSI TS 102 778)

Part 1: PAdES Overview – a framework document for PAdES

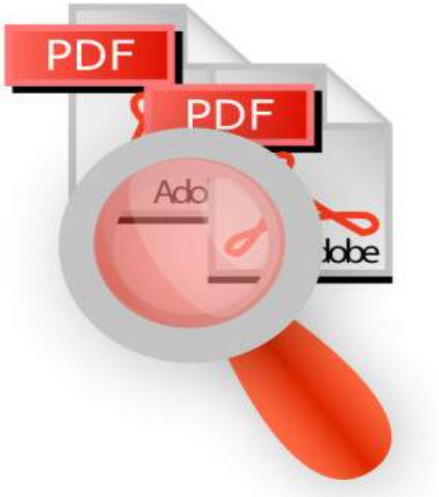
Part 2: PAdES Basic – Profile based on ISO 32000-1

Part 3: PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles

Part 4: PAdES Long Term – PAdES-Long Term Validation Profile

Part 5: PAdES for XML Content – Profiles for XAdES signatures of XML content in PDF files

Part 6: Visual Representation of Electronic Signatures



ISO 32000-1:2008

Grato pela atenção !

Wilson R Hirata

wilson.hirata@iti.gov.br

ICP Brasil
O Brasil na era da certificação digital