Laboratório de Sistemas Integráveis Tecnológico

PROJETO SREI

Sistema de Registro Eletrônico Imobiliário

Assinatura digital -
Alternativas de formatos e estrutura dos atributos de assinatura.

Título	PROJETO SREI: Assinatura digital: alternativas de formatos e estrutura dos atributos de assinatura
Versão	Versão 1.1 release 3
Data da liberação	18/01/2012
Classificação	LSI-TEC:Restrito
Autores	Volnys Bernal
Propriedade	LSI-TEC
Restrições de acesso	LSI-TEC, CNJ e ARISP

Sumário

1 Introdução

Este documento apresenta os padrões existentes relacionados à assinatura digital e sua possível aplicabilidade no projeto SREI.

São apresentadas as especificações definidas pela comunidade europeia CAdES [1], XAdES [2] e PAdES [3] no contexto da assinatura eletrônica avançada (*Advanced Electroonic Signatures* - AdES) [4]. Em seguida, é apresentado o padrão de assinatura digital definido pela ICP-Brasil.

2 Formatos de representação da assinatura digital

Os principais formatos de representação de assinatura digital existentes atualmente são CAdES [1], XAdES [2] e PAdES [3][4][5][6][7]. Tais formatos foram definidos com o intuito de adequar a tecnologia de assinatura existente (*CMS Digital Signature* [8][9][10][11][13], XML DSIG [14][15] e PDF [16]) à diretiva CE 1999/93 que trata da assinatura eletrônica avançada (*Advanced Electronic Signature* – AdES) [17] no âmbito da Comunidade Européia (CE).

A partir da Diretiva CE, o *European Telecommunication Standards Institute* (ETSI) formou um comitê técnico denominado *Electronic Signatures and Infrastructures* (ESI) para a definição dos padrões para assinatura eletrônica que atendam aos requisitos de assinatura eletrônica avançada (*Advanced Electroonic Signatures* - AdES). Estes trabalhos geraram as especificações *CMS Advanced Electronic Signature* (CAdES) [1], *XML Advanced Electronic Signature* (XAdES) [2] e, mais recentemente, a especificação *PDF Advanced Electronic Signature* (PAdES) [3][4][5][6[7], apresentadas no Quadro 1.

Quadro 1 – Padrões para formato de representação de assinatura digital.

Padrão	Descrição
CAdES	A especificação *CMS Advanced Electronic Signature* (CAdES) [1] define diversos modelos estruturais para representação de um objeto assinado, suas assinaturas e demais dados (como, por exemplo, certificados, dados de estado de revogação, carimbos de tempo, etc) construídos a partir a especificação Cryptographic Message Syntax SignedData (CMS SignedData) (RFC 5652) [13] através da inclusão de atributos assinados e não assinados
XAdES	A especificação *XML Advanced Electronic Signature* (XAdES) [2] define diversos modelos estruturais para representação de um objeto ou mais objetos assinados, suas assinaturas e demais dados (como, por exemplo, certificados, carimbos de tempo, etc) construídos a partir da especificação XML DSIG [13][14].

PAdES	A especificação *PDF Advanced Electronic Signature* (PAdES) [3][4][5][6][7] difere do CAdES e XAdES pois é voltada exclusivamente para documentos PDF [16], definindo requisitos que devem ser atendidos pelos softwares de visualização e edição PDF quando são utilizadas assinaturas digitais, além de determinar quais elementos do PDF podem constar e quais elementos não devem constar. Outra característica suportada pelo PDF é assinatura eletrônica integrada a formulários. Estas são características que distinguem a especificação PAdES do CAdES e XAdES.

Nestas especificações existe o desafio de inclusão de elementos adicionais à assinatura a fim de permitir a realização de um processo seguro de validação de assinaturas. Estes elementos são acrescentados à estrutura `CMS SignedData` na forma de atributos assinados e atributos não assinados. Dentre estes elementos que podem ser incluídos estão:

- A política de assinatura, que determina as condições e formatos que devem ser atendidos na geração e na validação da assinatura;
- O carimbo do tempo de assinatura (`signature time-stamp`), para determinar a referência de tempo segura para ser utilizada no processo de validação dos certificados da cadeia de certificação (possibilita garantir que a assinatura foi realizada antes de um determinado instante);
- As referências ao certificado e cadeia de certificação dos signatários e dos outros objetos assinados, necessários à validação da assinatura como o certificado de assinatura da Lista de Certificados Revogados (LCR), o certificado de assinatura da resposta OCSP e do certificado de assinatura do carimbo do tempo;
- As referências aos objetos de consulta sobre revogação, LCR e resposta OCSP, dos certificados utilizados;
- Os certificados e cadeias de certificação;
- Os objetos de revogação;

- O carimbo do tempo de arquivamento, para possibilitar a validação das assinaturas após vários anos da sua geração, um termo conhecido como validação a longo prazo (ou *long-term validation* - LTV).

Para possibilitar a validação de uma assinatura eletrônica, é necessária a utilização dos seguintes objetos, que devem mantidos junto ao objeto assinado ou em um outro repositório, sendo passível de recuperação:

- O certificado e cadeia de certificação dos signatários e dos outros objetos assinados necessários à validação da assinatura como o certificado de assinatura da LCR, o certificado de assinatura da resposta OCSP e do certificado de assinatura do carimbo do tempo;
- Os objetos de consulta sobre revogação, LCR e resposta OCSP, dos certificados utilizados. Estes objetos devem ser obtidos o quanto antes pois, quando um certificado expira, as informações sobre revogação presentes na LCR podem ser eliminadas, o mesmo valendo para as respostas OCSP.

Associado a uma assinatura existe, implicitamente, um compromisso assumido pelo signatário que pode ser, por exemplo, a concordância com as disposições presentes em conteúdo assinado ou a ciência de um comunicado recebido. Em alguns contextos, pode ser necessário expressar explicitamente tal compromisso. Para isso, é possível incluir na assinatura eletrônica um atributo que expresse qual é o compromisso assumido pelo signatário no momento de geração de uma assinatura eletrônica.

3 Especificação CAdES

A especificação *CMS Advanced Electronic Signature* (CAdES) [1] define diversos modelos estruturais para representação de um objeto assinado, suas assinaturas e demais dados (como, por exemplo, certificados, dados de estado de revogação, carimbos de tempo, etc) construídos a partir a especificação *Cryptographic Message Syntax SignedData* (*CMS SignedData*), definida na RFC 5652 [13], através da inclusão de atributos assinados e não assinados.

A especificação *CMS SignedData* (RFC 5652) é derivada da especificação PKCS#7 [8], originalmente definida pela RSA Laboratories. O CMS é especificado por meio da linguagem ASN.1 (*Abstract Syntax Notation One*) [18] e se utiliza da codificação BER (*Basic Encoding Rules*) [18] ou DER (*Distinguished Encoding Rules*) [18], podendo ser adicionalmente transformado em ASCII utilizando a especificação Base64.

3.1 Padrão CMS

O padrão CMS (*Cryptographic Message Syntax*) foi definido originalmente da especificação PKCS#7 versão 1.5 [8], definida pela RSA em 1993. Desde então, o IETF (*Internet Engineering Task Force*) tornou-se responsável pelo desenvolvimento e manutenção do padrão. O Quadro 2 apresenta a evolução do padrão CMS ao longo do tempo.

Quadro 2 – Versões do padrão CMS.

Documento	Entidade	Ano	Observação
PKCS#7 v. 1.5 [8]	RSA	19993	Versão original.
RFC 2315 [9]	IETF	1998	Publicação da versão original como RFC.
RFC 2630 [10]	IETF	1999	Segunda versão.
RFC 3369 [11]	IETF	2002	Terceira versão.
RFC 3852 [12]	IETF	2004	Quarta versão.
RFC 5652 [13]	IETF	2009	Quinta versão, versão atual

- Localização do signatário (`signer location`);
- Carimbo de tempo de conteúdo (`content time stamp`).

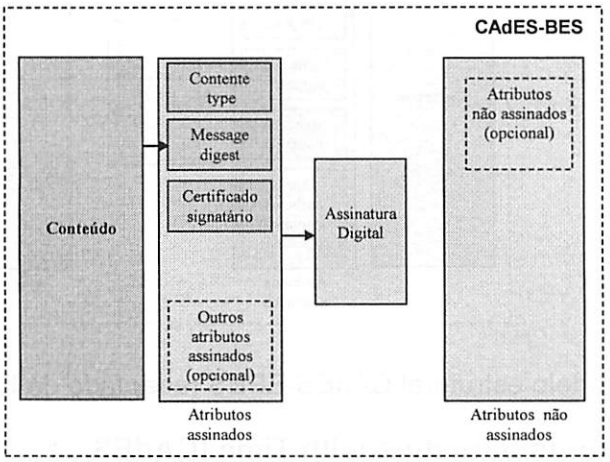


Figura 4 – Formato CAdES-BES (adaptado de ETSI TS 101 733 CAdES).

Nestes modelos estruturais, o conteúdo assinado pode estar inclúdo na estrutura `CMS SignedData`, sendo denominado `CMS SignedData attached`, ou estar destacado, sendo denominado `CMS SignedData Detached`.

3.3.2 CAdES Explicit Policy-based Electronic Signatures (CAdES-EPES)

O modelo estrutural *CAdES Explicit Policy-based Electronic Signatures* (CAdES-EPES) é semelhante ao CAdES-BES, com a obrigatoriedade de informar a política de assinatura (`signature policy identifier`).

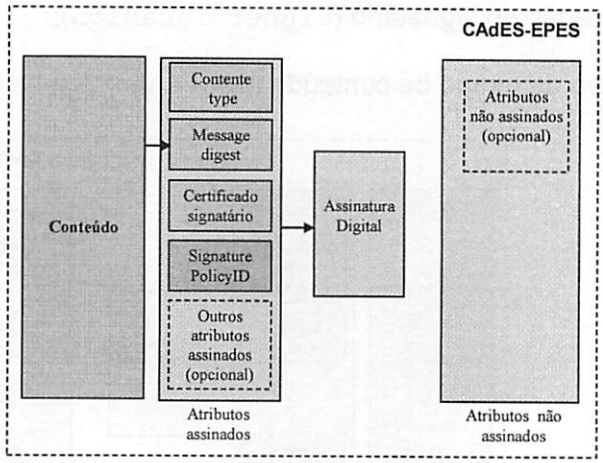
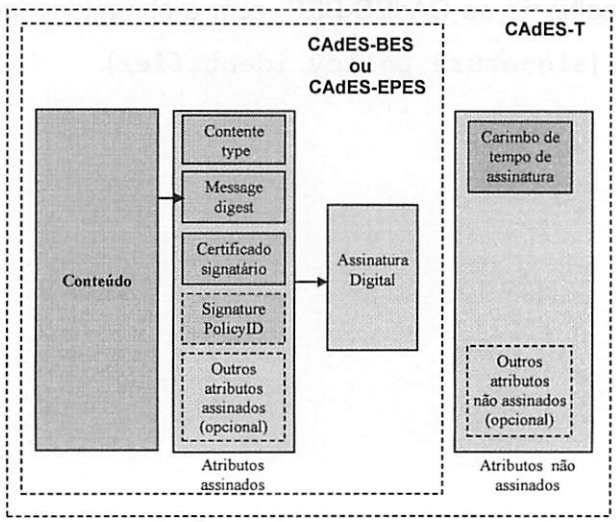


Figura 5 - Modelo estrutural CAdES-EPES (adaptado de ETSI TS 101 733 CAdES).

3.3.3 Electronic Signature with Time (CAdES-T)

O modelo estrutural *Electronic Signature with Time* (CAdES-T) é baseado no CAdES-BES ou CAdES-EPES com a obrigatoriedade da inclusão do atributo de carimbo do tempo da assinatura. O carimbo de tempo de assinatura contém o instante de referência seguro (âncora temporal) para a validação da cadeia de certificação do certificado do signatário. A especificação admite, também, a possibilidade de utilização do CAdES-BES ou CAdES-EPES com uma marcação de tempo (*log*) segura disponível para auditoria.



- Conteúdo anexado: quando o conteúdo digital é incluído na estrutura CMS;
- Conteúdo separado: quando o conteúdo digital não é incluído na estrutura CMS, sendo referenciado indiretamente através do seu resultado hash.

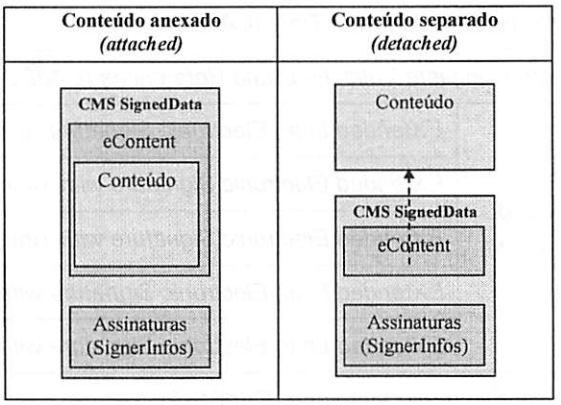


Figura 3 – CMS com conteúdo anexado ou separado.

3.3 Modelos estruturais da especificação CAdES

O formato para representação da assinatura digital utilizado na especificação CAdES é o `CMS SignedData`, no qual são incluídos diversos atributos assinados e não assinados, formando uma nova estrutura. Por este motivo será utilizado o termo "modelo estrutural" para referenciar os diversos tipos de estruturas, pois o formato é ainda um CMS SignedData.

Os modelos estruturais de assinatura eletrônica definidos pela especificação CAdES estão apresentados no Quadro 3.

Os modelos estruturais de assinatura eletrônica estendida são utilizados para possibilitar a validação de assinaturas em longo prazo e para prevenir algumas situações catastróficas de comprometimento de chaves de AC, chaves de LCR ou chaves do serviço OCSP.

As seções a seguir apresentam algumas informações adicionais sobre cada um destes modelos estruturais.

Quadro 3 – Modelos estruturais da especificação CAdES.

Sem dados de validação	*CAdES Basic Electronic Signature (CAdES-BES)*	
	CAdES Explicit Policy-based Electronic Signatures (CAdES-EPES)	
Com dados de validação	*Electronic Signature with Time (CAdES-T)*	
	ES with Complete Validation Data References (CAdES-C)	
	Extended (CAdES-X)	*EXtended Long Electronic Signature (CAdES-X Long)*
		EXtended Electronic Signature with Time Type 1 (CAdES-X Type 1)
		EXtended Electronic Signature with Time Type 2 (CAdES-X Type 2)
		EXtended Long Electronic Signature with Time (CAdES-X Long Type 1)
		EXtended Long Electronic Signature with Time (CAdES-X Long Type 2)
	Archival Electronic Signature (CAdES-A)	

3.3.1 CAdES Basic Electronic Signature (CAdES-BES)

O modelo estrutural *CAdES Basic Electronic Signature* (CAdES-BES) é o mais simples de todos. Ele fornece funcionalidades para a realização de autenticação básica e proteção de integridade.

Este modelo exige a obrigatoriedade de somente os seguintes atributos assinados:

- Tipo de conteúdo (`content type`)
- Hash da mensagem (`message digest`)
- Certificado do signatário v1 (`ESS signing certificate`) ou Certificado do signatário v2 (`ESS signing certificate v2`)

Existem também outros atributos assinados opcionais:

- Identificador da política de assinatura (`signature policy identifier`);
- Indicação de tipo de compromisso (`commitment type indication`);
- Atributos do signatário (`signer attributes`);
- Instante da assinatura (`signing time`);

O padrão CMS define estruturas para vários tipos de documentos. O tipo `CMS SignedData` é voltado especificamente para a organização de dados relacionados à assinatura digital. Ele possibilita incluir ou referenciar:

- O conteúdo digital assinado;
- Informações sobre cada signatário, tais como:
  - Dados de identificação do signatário;
  - Blocos de assinaturas digitais gerados por cada signatário;
  - Algoritmos criptográficos utilizados nos processos de assinatura digital;
  - Atributos assinados e não assinados relacionados à assinatura digital;
- Certificados digitais dos signatários e respectivas cadeias de certificação; e
- Objetos relacionados à verificação de revogação como listas de certificados revogados (LCR) e/ou respostas OCSP.

A Figura 1 ilustra um conteúdo tipo `CMS Signed-data` com conteúdo incluído e contendo três signatários, cada qual com seu respectivo tipo `SignerInfo`.

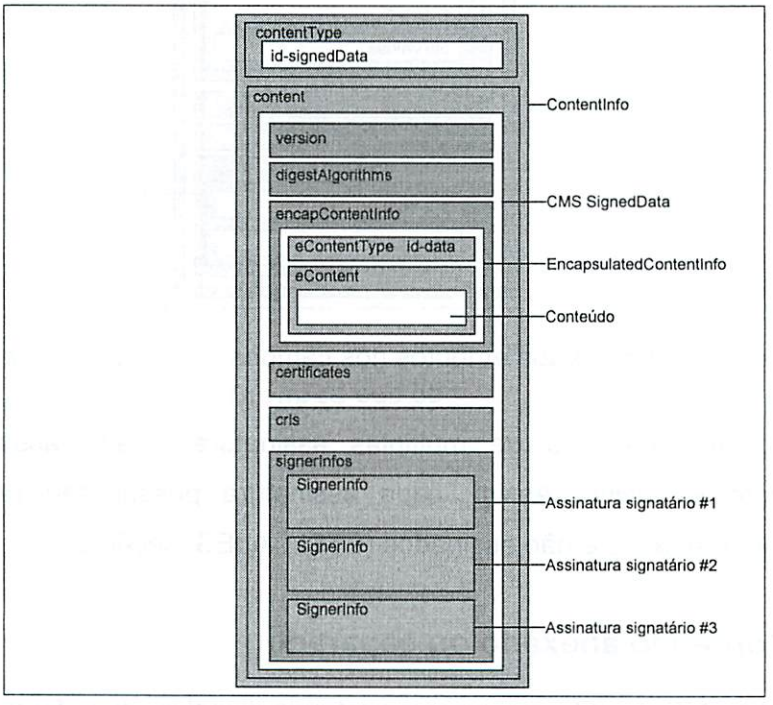


Figura 1 – Ilustração do tipo `CMS Signed-data` com conteúdo incluído e contendo três signatários.

Os atributos, individuais a cada signatário e incluídos na sua estrutura `signerInfo`, estão organizados em:

- Atributos assinados: são aqueles que podem ser incluídos no campo `signedAttrs` do tipo `SignerInfo`;
- Atributos não assinados: são aqueles que podem ser incluídos no campo `unsignedAttrs` do tipo `SignerInfo`.

A Figura 2 ilustra o tipo `SignerInfo` com alguns atributos nos campos `signedAttrs` e `unsignedAttrs`.

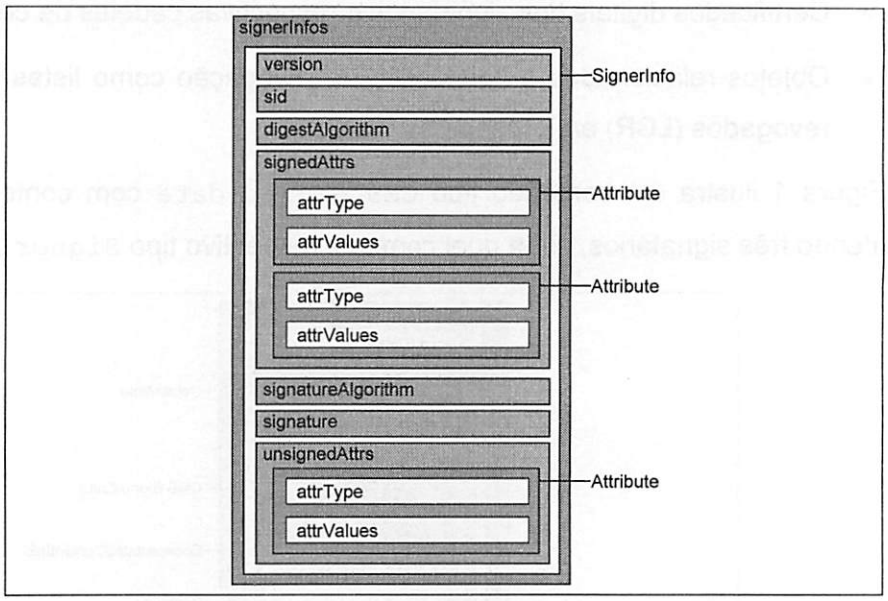


Figura 2 – Ilustração dos atributos nos campos `signedAttrs` e `unsignedAttrs` do tipo `SignerInfo`.

Quando da existência de múltiplas assinaturas, cada assinatura possui seu SignerInfo exclusivo. Assim, cada assinatura possui seu próprio conjunto de atributos assinados e não assinados (ETSI CAdES, seção 6).

3.2 Conteúdo anexado ou separado

O padrão CMS permite organizar o conteúdo digital de duas formas:

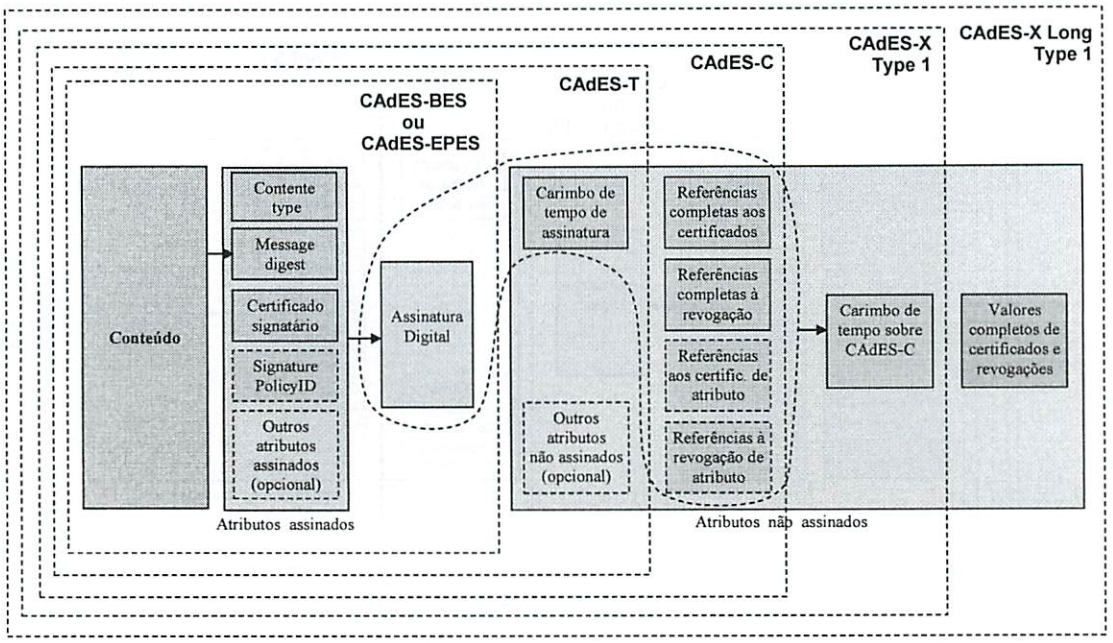


Figura 13 - Modelo estrutural CAdES-X Long Type 1 (adaptado de ETSI TS 101 733 CAdES).

3.3.9 EXtended Long Electronic Signature with Time (CAdES-X Long Type 2)

O modelo estrutural *EXtended Long Electronic Signature with Time* (CAdES-X Long Type 2) representa a combinação dos modelos estruturais CAdES-X-Long com CAdES-X Type 2.

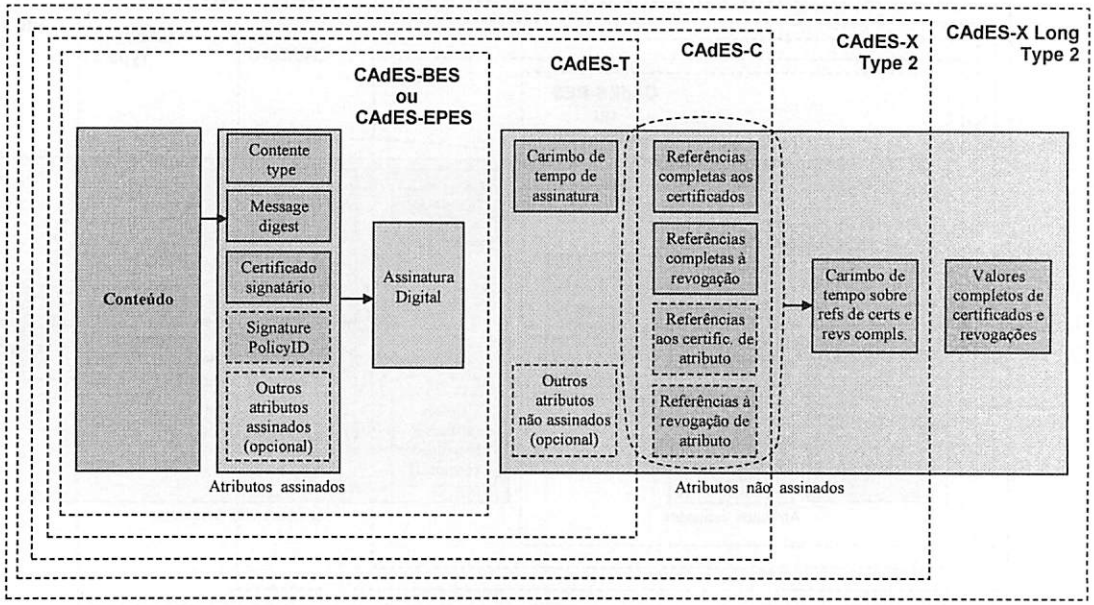


Figura 14 - Modelo estrutural CAdES-X Long Type 2 (adaptado de ETSI TS 101 733 CAdES).

3.3.10 Archival Electronic Signature (CAdES-A)

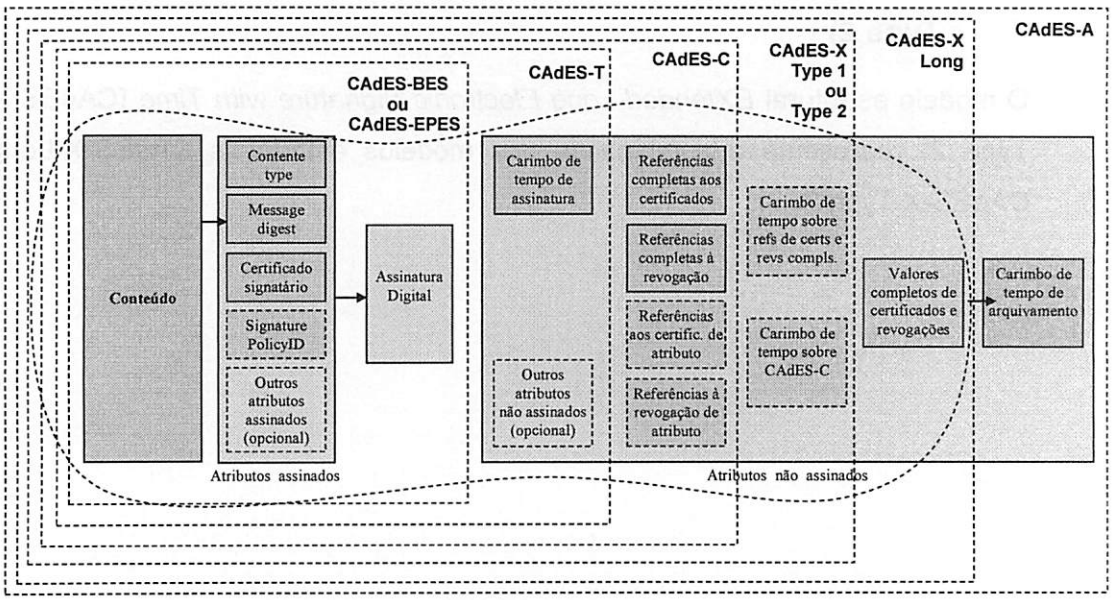


Figura 15 - Modelo estrutural CAdES-A (adaptado de ETSI TS 101 733 CAdES).

O valor utilizado no carimbo de tempo de arquivamento é resultado *hash* da concatenação dos seguintes elementos da estrutura `CMS SignedData`:

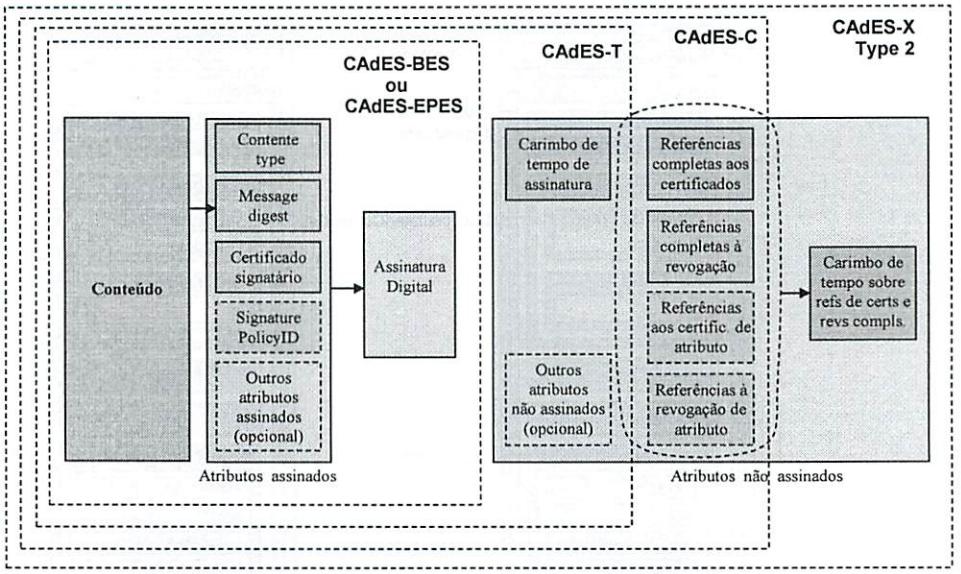


Figura 11 - Modelo estrutural CAdES-X Type 2 (adaptado de ETSI TS 101 733 CAdES).

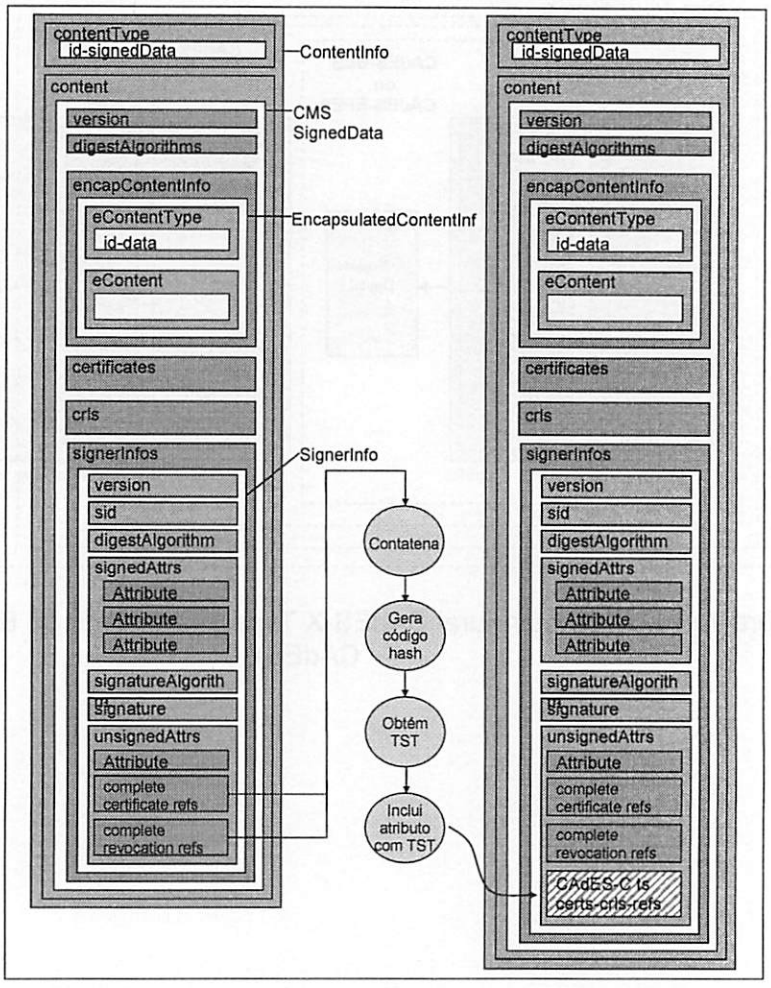


Figura 12 - Ilustração da inclusão de um atributo "carimbo de tempo das referências".

3.3.8 EXtended Long Electronic Signature with Time (CAdES-X Long Type 1)

O modelo estrutural *EXtended Long Electronic Signature with Time* (CAdES-X Long Type 1) representa a combinação dos modelos estruturais CAdES-X-Long com CAdES-X Type 1.

values). Este modelo estrutural é autocontido, pois inclui todas as informações necessárias para a validação da assinatura eletrônica.

No exemplo apresentado anteriormente, quando for necessário enviar a uma entidade externa um documento com assinatura eletrônica no modelo estrutural CAdES-C, é possível compor uma instância deste documento assinado a partir do CAdES-C, incluindo os certificados e objetos de revogação recuperados da base de dados.

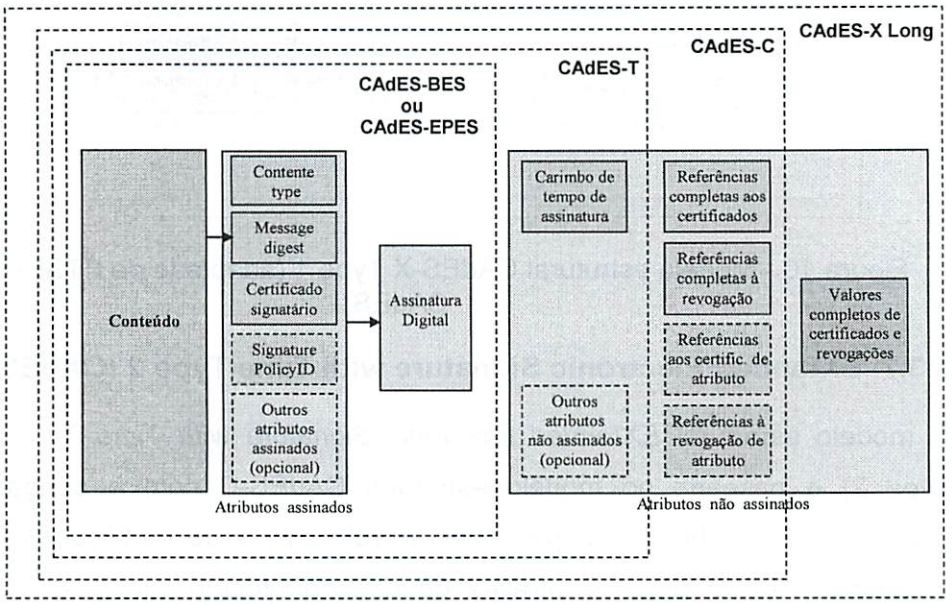


Figura 9 - Modelo estrutural CAdES-X Long (adaptado de ETSI TS 101 733 CAdES).

3.3.6 EXtended Electronic Signature with Time Type 1 (CAdES-X Type 1)

O modelo estrutural *EXtended Electronic Signature with Time Type 1* (CAdES-X Type 1) é baseado no modelo estrutural CAdES-C com a obrigatoriedade de inclusão do carimbo de tempo sobre o modelo CAdES-C. Isto é possível através do uso do atributo `CAdES-C-time-stamp`, cujo *hash* envolve o valor da assinatura digital, do carimbo de tempo de assinatura e dos atributos de referência.

Este modelo de estrutural previne algumas situações catastróficas de comprometimento de chaves de AC, chaves de LCR ou chaves do serviço OCSP, propiciando uma redundância criptográfica sobre a assinatura eletrônica.

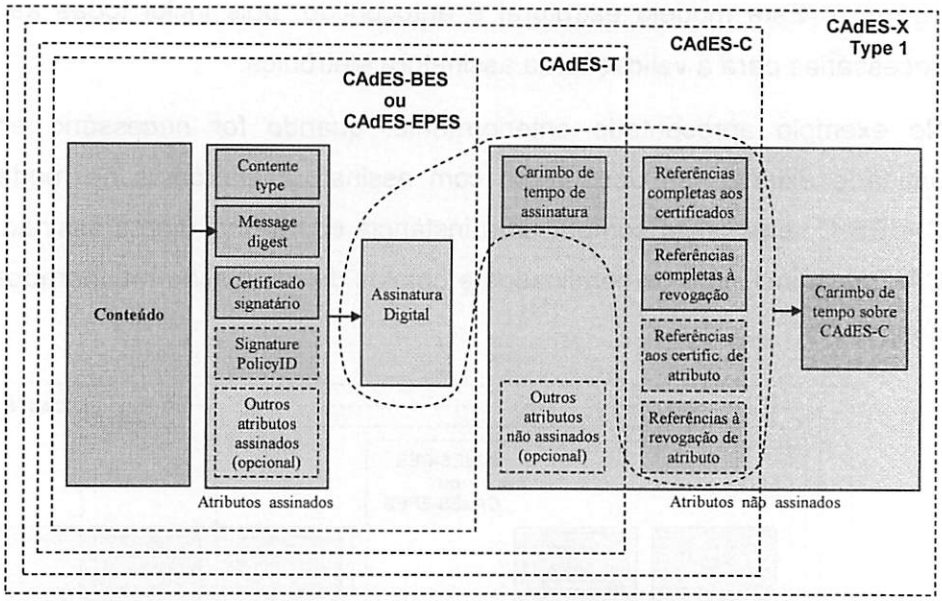


Figura 10 - Modelo estrutural CAdES-X Type 1 (adaptado de ETSI TS 101 733 CAdES).

3.3.7 EXtended Electronic Signature with Time Type 2 (CAdES-X Type 2)

O modelo estrutural *EXtended Electronic Signature with Time Type 2* (CAdES-X Type 2) é baseado no modelo estrutural CAdES-C com a obrigatoriedade de inclusão do carimbo de tempo sobre as referências de certificados e objetos de revogação. Isto é possível através do uso do atributo `CAdES-C-time-stamp-certs-crls-references`, cujo *hash* envolve os atributos de referência a certificados e objetos de revogação.

Segundo a especificação CAdES, este modelo estrutural previne os mesmos riscos que o CAdES-X Type 1.

Figura 6 - Modelo estrutural CAdES-T (adaptado de ETSI TS 101 733 CAdES).

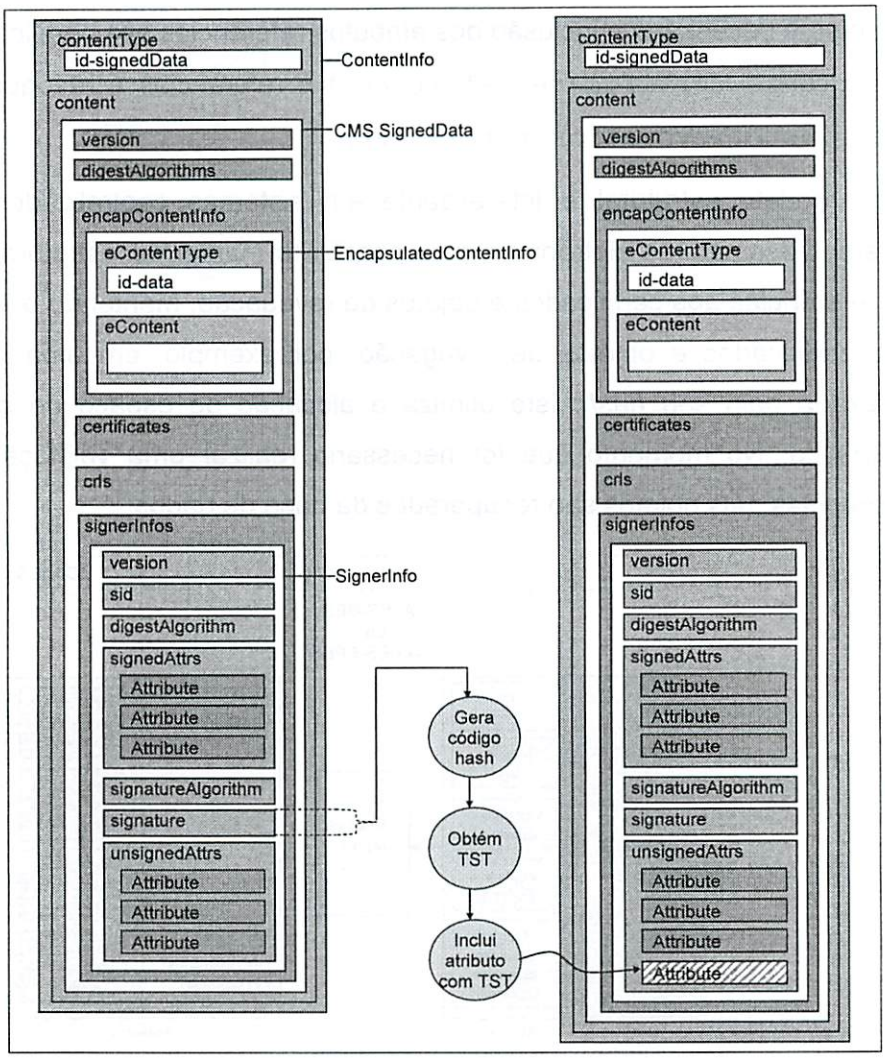


Figura 7 - Ilustração da inclusão de um atributo "carimbo de tempo de assinatura".

3.3.4 ES with Complete Validation Data References (CAdES-C)

O modelo estrutural *Electronic Signature (ES) with Complete Validation Data References* (CAdES-C) é basado no CAdES-T com a obrigatoriedade de inclusão de referências aos certificados da cadeia de certificados do signatário e de referências às LCRs e respostas OCSP necessárias para sua validação. Isto é obtido através do uso de dois atributos referências completas aos certificados (`complete certificate references`) e referências completas à revogação (`complete`

`revogation references`). Caso sejam utilizados certificados de atributos também é necessária a inclusão dos atributos referências aos certificados de atributo (`attribute certificate references`) e referências à revogação de atributo (`attribute revogation references`).

Este modelo estrutural é interessante em sistemas centralizados que mantém diversas assinaturas eletrônicas, pois possibilita manter na estrutura CMS somente as referências aos certificados e objetos de revogação, mantendo o armazenamento dos certificados e objetos de revogação, por exemplo, em uma base de dados indexada pelo seu *hash*. Isto otimiza a alocação de espaço de armazenamento eletrônico. No momento que for necessário realizar uma validação, através das referências, tais objetos são recuperados da base de dados.

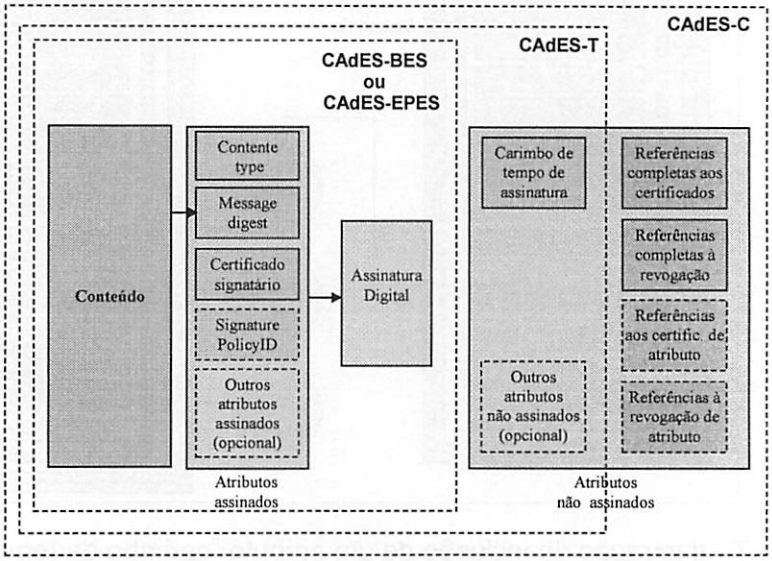


Figura 8 - Modelo estrutural CAdES-C (adaptado de ETSI TS 101 733 CAdES).

3.3.5 EXtended Long Electronic Signature (CAdES-X Long)

O modelo estrutural *EXtended Long Electronic Signature* (CAdES-X Long) é baseado no modelo estrutural CAdES-C com a obrigatoriedade de inclusão da cadeia de certificados dos signatários e das respectivas LCRs e respostas OCSP necessárias para validação. Isto é possível através do uso dos atributos "valores dos certificados" (`certificate values`) e "valores de revogação" (`revocation`

- `SigningCertificate` – Certificado de assinatura: Contém a referência ao certificado utilizado pelo signatário para geração da assinatura;
- `SigningTime` - Instante de assinatura: Instante alegado pelo signatário da geração da assinatura;
- `DataObjectFormat` – Formato do objeto de dados: Identifica o formato do objeto de dados assinado;
- `CommitmentTypeIndication` – Indicação do tipo de finalidade: Identifica a finalidade da assinatura determinada pelo signatário em relação ao objeto de dados assinado;
- `SignatureProductionPlace` – Local da produção da assinatura: Indica o local da produção da assinatura alegado pelo signatário;
- `SignerHole` – Papel do signatário: Contém o papel assumido pelo signatário quando da criação da assinatura. O papel pode ser alegado ou certificado. Papel certificado depende da inclusão do certificado de atributo.
- `CounterSignature` – Contra-assinatura: Contém uma outra assinatura aplicada sobre a anterior.

4.2.1 Modelos estruturais definidos pela especificação XAdES

A especificação XAdES, atualmente, define quatro modelos estruturais básicos, de uso obrigatório, e seis modelos, de uso opcional, voltados ao armazenado de longo prazo, apresentados no Quadro 6.

Quadro 6 – Modelos estruturais obrigatórios para assinaturas eletrônicas XAdES.

<table>
<tr><td colspan="2">XAdES Basic Electronic Signature (XAdES-BES)</td><td rowspan="4">Suporte obrigatório</td></tr>
<tr><td colspan="2">XCAdES Explicit Policy-based Electronic Signatures (XAdES-EPES)</td></tr>
<tr><td colspan="2">Electronic Signature with Time (XAdES-T)</td></tr>
<tr><td colspan="2">ES with Complete Validation Data References (XAdES-C)</td></tr>
<tr><td rowspan="2"></td><td>EXtended Electronic Signature with Time Type 1 (XAdES-X Type 1)</td><td rowspan="2"></td></tr>
<tr><td>EXtended Electronic Signature with Time Type 2 (XAdES-X Type 2)</td></tr>
</table>

Extended (XAdES-X)	*EXtended Long Electronic Signature (XAdES-X L)*	*Suporte opcional*
	EXtended Long Electronic Signature with Time (XAdES-X L Type 1)	
	EXtended Long Electronic Signature with Time (XAdES-X L Type 2)	
Archival Electronic Signature (XAdES-A)		

Os modelos estruturais são equivalentes, do ponto de vista funcional, aos modelos estruturais definidos em CAdES.

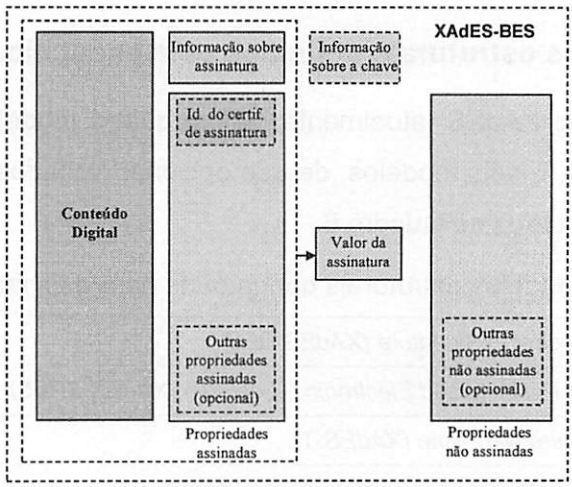
As seções a seguir apresentam um resumo destes modelos estruturais.

4.2.2 XAdES-BES

O modelo estrutural *XAdES Basic Electronic Signature* (XAdES-BES) é o mais simples de todos. Ele fornece funcionalidades para a realização de autenticação básica e proteção de integridade.

Este modelo não exige a obrigatoriedade de nenhuma propriedade assinada ou não assinada.

Caso o certificado do signatário não tenha sido informado no elemento KeyInfo, é obrigatório a existência da propriedade assinada "certificado do signatário" (`SigningCertificate`).



- Relacionadas à política de assinatura:
  - `SignaturePolicyIdentifier` - Identificador da política de assinatura: Contém informação que permite identificar a política de assinatura que deve ser utilizada no processo de produção e verificação da assinatura. É utilizada clarificar o papel e comprometimento do signatário com respeito ao conteúdo assinado;
- Relacionadas à validação da assinatura:
  - `CompleteCertificateRefs` - referências completas aos certificados: Contém referências aos certificados de AC utilizados no processo de validação da assinatura;
  - `CompleteRevocationRefs` – referências completas a dados de revogação: Contém referências ao conjunto completo de informação de revogação (LCR e OCSP) utilizado para verificação da assinatura;
  - `AttributeCertificateRefs` – Referências aos certificados de atributo: Contém referências ao conjunto completo de Certificados de Autoridade de Atributo que utilizado para validação dos certificados de atributo;
  - `AttributeRevocationRefs` – Referências à dados de revogação de atributo: Contém referências ao conjunto completo de informação de revogação utilizado para validar um certificado de atributo presenta na assinatura.
  - `CertifcateValues` – Valores dos certificados: Contém os certificados utilizados no processo de validação da assinatura.
  - `RevocationValues` – Valores de revogação: Contém os objetos que contém informação sobre revogação de certificado como, por exemplo, LCR e OCSP;
  - `AttrAuthoritiesCertValues` – Valores dos certificados de autoridade de atributo: Contém os certificados das autoridade de atributos utilizados no processo de validação dos certificados de atributo.

- `AttributeRevocationValues` – Valores dos dados de revogação de atributo: Contém os dados de revogação utilizados no processo de validação dos certificados de atributo.

- Relacionadas à carimbo de tempo:
  - `SignatureTimeStamp` – Carimbo do tempo da assinatura: Contém um carimbo de tempo obtido a partir do *hash* de uma determinada assinatura. O instante de tempo contido no carimbo de tempo é utilizado como a âncora temporal para validar o certificado utilizado na assinatura associada;
  - `SigAndRefsTimeStamp` – Carimbo do tempo da assinatura e referências: Contém um ou mais carimbos de tempo, obtidos de diferentes ACs. O *hash* do carimbo do tempo é computado sobre o elemento `SignatureValue` e as propriedades `SignatureTimeStamp`, se presente, `CompleteCertificateRefs` e `CompleteRevocationRefs`;
  - `RefsOnlyTimeStamp` – Carimbo do tempo somente das referências: Contém um ou mais carimbos de tempo, obtidos de diferentes ACs. O hash do carimbo do tempo é computado sobre as propriedades `CompleteCertificateRefs` e `CompleteRevocationRefs`;
  - `xadesv141:ArchiveTimeStamp` – Carimbo do tempo de arquivamento: Contém um carimbo do tempo, cujo hash é computado sobre o conteúdo digital, informações de assinatura e propriedades não assinadas. Utilizado para proteção contra comprometimento de algoritmos criptográficos;
- Relacionadas á validação de carimbo do tempo:
  - `xadesv141:TimeStampValidationData` – Dados de validação do carimbo do tempo: Contém certificados e dados de revogação (LCR, OCSP) utilizados para validar um determinado carimbo do tempo.
- Relacionadas a outras propriedades:

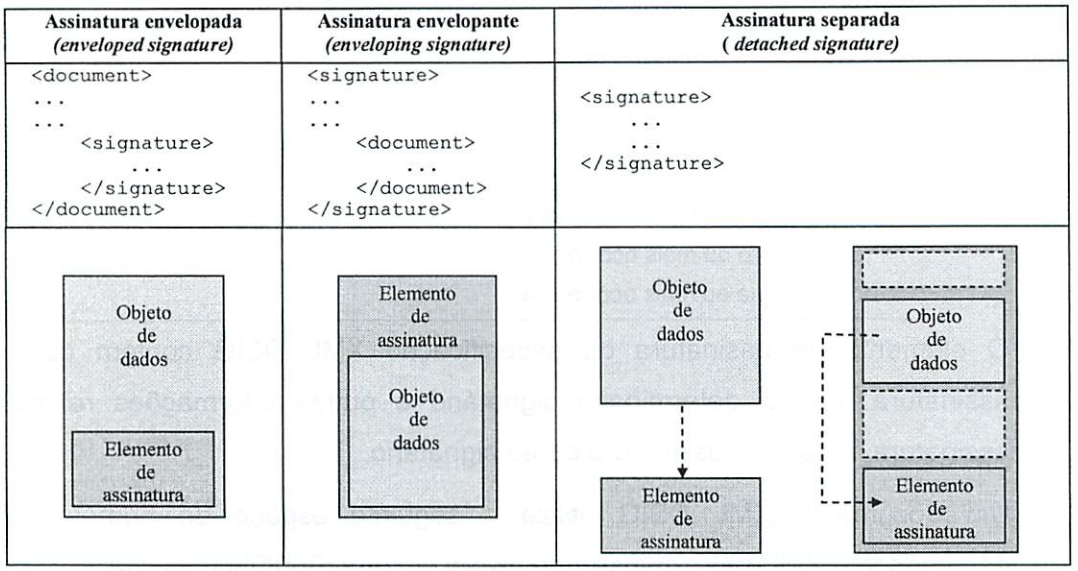


Figura 17 – Tipos de assinatura XML DSIG.

4.1.2 Visão geral da assinatura

Uma assinatura XML DSIG pode ser aplicada a qualquer conteúdo digita (objetos de dados - *data objects*) de forma indireta: é calculado o *hash* do conteúdo digital e o resultado é armazenado em um elemento XML (com outras informações relevantes) sobre o qual é novamente calculado o *hash* e criptograficamente assinado.

Uma assinatura digital XML DSIG é representada no XML pelo elemento `signature`, cuja estrutura está apresentada no Quadro 5.

Quadro 5 – Estrutura do elemento `signature` do XML DSIG.

```
<Signature ID?>
     <SignedInfo>
          <CanonicalizationMethod/>
          <SignatureMethod/>
          (<Reference URI? >
               (<Transforms>)?
                <DigestMethod>
                <DigestValue>
          </Reference>)+
     </SignedInfo>
     <SignatureValue>
```

```
    (<KeyInfo>)?
    (<Object ID?>)*
</Signature>
```

Legenda:

?	Zero ou uma ocorrência
*	Zero ou mais ocorrências
+	Uma ou mais ocorrências

O elemento de assinatura da especificação XML DSIG contém os dados de assinatura de um determinado signatário e outras informações relacionadas à assinatura, ao ato da assinatura ou ao signatário.

Um documento XML DSIG utiliza o seguinte espaço de nomes XML (XML namespace – XML-ns): xmlns="http://www.w3.org/2000/09/xmldsig#"

4.2 Especificação XAdES

A especificação XADES utiliza como base especificação XML DSIG, com o acréscimo de determinadas propriedades associadas à assinatura e ao conteúdo digital.

Existem dois tipos de propriedades: propriedades assinadas e propriedades não assinadas. As propriedades assinadas (elemento `SignedProperties`), são objetos de dados adicionais que fazem parte do conteúdo assinado pelo signatário. As propriedades não assinadas (elemento `UnsignedProperties`), são objetos de dados adicionados pelo usuário, pelo verificador ou por outra parte após a produção da assinatura e não fazem parte do conteúdo assinado pelo signatário. Estas propriedades podem ser envolvidas na computação de valores utilizados em outros processos de integridade, como, por exemplo, carimbos de tempo.

Na especificação XAdES, as propriedades são incluídas em um documento XML DSIG através de um `ds:Object` e o valor da assinatura deve ser computada sobre o conteúdo digital (de acordo com a especificação XML DSIG) e, também, sobre o conjunto completo de propriedades assinadas.

A seguir estão relacionadas algumas propriedades.

4 Especificação XAdES

A especificação *XML Advanced Electronic Signature* (XAdES) [2] define diversos modelos estruturais para representação de um ou mais objetos assinados, suas assinaturas e demais dados (como, por exemplo, certificados, carimbos de tempo, etc) construídos a partir da especificação XML DSIG [14][15].

4.1 Especificação XML DSIG

A especificação XML DSIG especifica as regras de processamento e sintaxe da assinatura digital baseada em XML.

Uma assinatura XML DSIG fornece serviços de integridade, autenticação de mensagem e/ou autenticação do signatário para conteúdo digital (objeto de dados) de qualquer tipo.

A primeira versão da especificação XML DSIG foi elaborada em conjunto entre o IETF e o W3C. O Quadro 4 apresenta as versões da especificação XML DSIG.

Quadro 4 – Versões da especificação XML DSIG.

Documento	Entidade	Ano	Observação
Primeira versão [14]	IETF e W3C	2002	Produzida em conjunto pelo IETF e pelo W3C XML Signature Working Group e publicada como RFC 3275 em março de 2002.
Segunda versão [15]	W3C	2008	Produzida pelo W3C XML Security Specifications Maintenance Working Group. Ela adiciona e recomenda o uso do algoritmo Canonical XML 1.1, entre outras alterações menores.

Para entendimento dos tipos de assinatura XML DSIG, é importante distinguir os seguintes elementos:

- Elemento de assinatura (*signature element*): elemento definido pelo XML DSIG que permite representar a assinatura digital de um signatário e outros atributos associados a esta assinatura;

- Conteúdo digital ou objeto de dados (*data object*): No contexto da especificação XML DSIG [14][15], representa a sequencia de bits que é assinada. O conteúdo digital assinado pode ser, por exemplo, um documento XML, um recurso externo (arquivo) ou mesmo uma parte do documento XML.

4.1.1 Tipos de assinatura XML DSIG

A especificação XML Dsig define três formas de organização de objetos de dados e assinatura:

- Assinatura envelopada (*enveloped signature*):

  A assinatura é aplicada sobre o conteúdo XML que contém a assinatura como um elemento. O conteúdo digital (objeto de dados assinado) representa o elemento raiz do documento XML;

- Assinatura envelopante (*enveloping signature*):

  A assinatura é aplicada sobre o conteúdo digital (objeto de dados) contido em um elemento `object` que, por sua vez, está contido no elemento de assinatura (*signature element*). O elemento `object` é identificado através de uma `reference` (através de um identificador de fragmento URI ou transformação);

- Assinatura separada (*signature detached*):

  A assinatura é aplicada sobre um conteúdo digital (objeto de dados) externo ao elemento de assinatura, sendo o objeto de dados identificado pela URI ou transformação.

  Esta forma de assinatura é utilizada em duas situações principais: (a) Quando o objeto de dados é um recurso (ex. arquivo) e o elemento de assinatura outro recurso (ex. outro arquivo) ou (b) quando o objeto de dados (fragmento do XML) e o elemento de assinatura são elementos irmãos de um documento XML;

- O campo `encapContentInfo`;
- O conteúdo externo protegido pela assinatura digital; se o campo `eContent` do `encapContentInfo` não estiver presente (conteúdo destacado);
- O campo `certificates` (se presente);
- O campo `crls` (se presente);
- A estrutura `SignerInfo`.

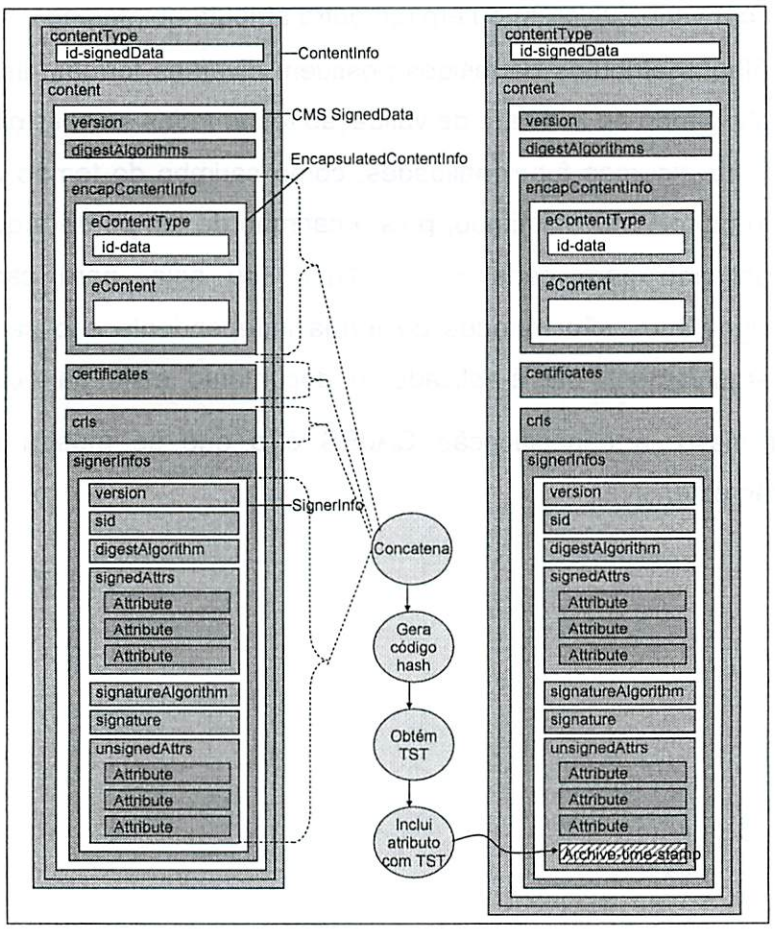


Figura 16 – Ilustração da inclusão de um atributo "carimbo de tempo de arquivamento".

3.4 Conclusão

A especificação CAdES vem de encontro à necessidade de um padrão de assinatura eletrônica que possibilite incorporar os diferentes elementos de dados sobre o

conteúdo assinado, a assinatura realizada, propriedades do signatário, certificados utilizados, dados de revogação e outros elementos de validação necessários.

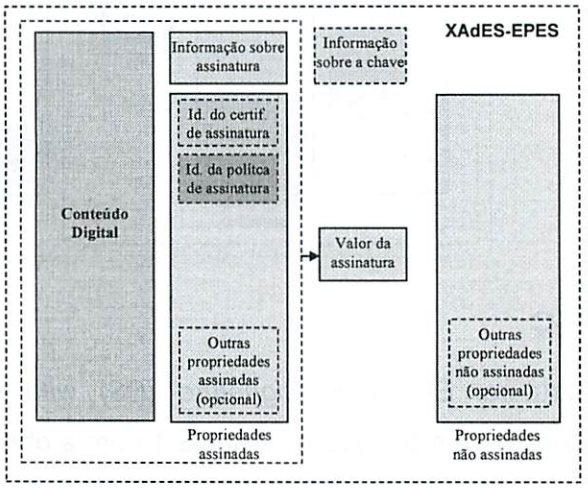
Porém, a especificação apresenta alguns problemas em relação à interoperabilidade. Por exemplo:

- Para alguns atributos que podem possuir mais que um valor, não é definido de forma precisa se devem ser incluídos com no mesmo atributo (um atributo com vários valores) ou em um outro atributo no mesmo `SignerInfo`;
- Alguns atributos permitidos possuem diversas formas distintas de utilização, obrigando ao software de validação testar todas as possibilidades;
- Para algumas funcionalidades, como carimbo de tempo de arquivamento, o formato CMS é limitado, pois o carimbo de tempo de arquivamento deve ser aplicado para cada `signerInfo` (ou seja, para cada signatário). Os signatários são tratados de forma independente e o carimbo de tempo de arquivamento não é aplicado ao "documento" e sim para cada assinatura.

Apesar disso, a especificação CAdES é a que se mostra mais madura para utilização extensiva.

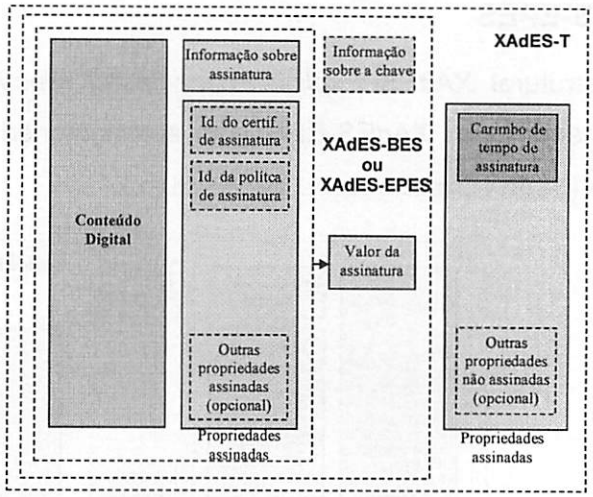
4.2.3 XAdES-EPES

O modelo estrutural *XAdES Explicit Policy-based Electronic Signatures* (XAdES-EPES) é semelhante ao XAdES-BES, com a obrigatoriedade de informar a política de assinatura (`SignaturePolicyIdentifier`).



4.2.4 XAdES-T

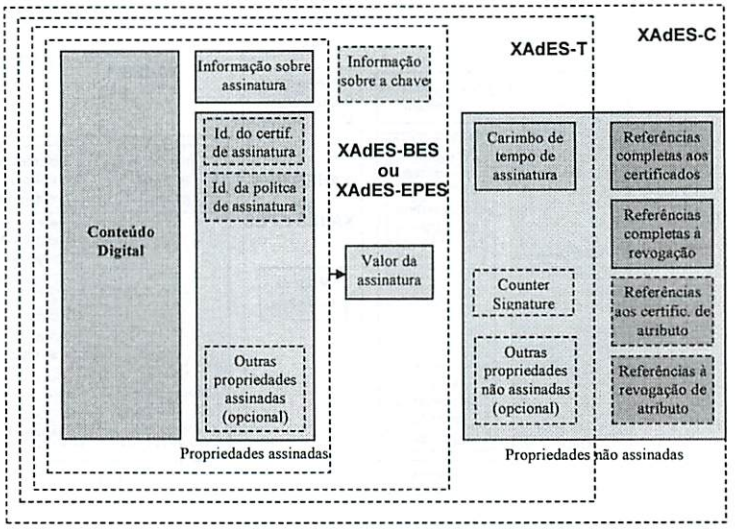
O modelo estrutural *Electronic Signature with Time* (XAdES-T) é baseado no XAdES-BES ou XAdES-EPES com a obrigatoriedade da inclusão do atributo de carimbo do tempo da assinatura (`SignatureTimeStamp`). O carimbo do tempo da assinatura contém o instante de referência seguro (âncora temporal) para a validação da cadeia de certificação do certificado do signatário.



4.2.5 XAdES-C

O modelo estrutural *Electronic Signature (ES) with Complete Validation Data References* (XAdES-C) é basado no XAdES-T com a obrigatoriedade de inclusão de referências aos certificados da cadeia de certificados do signatário e de referências às LCRs e respostas OCSP necessárias para sua validação. Isto é obtido através do uso de dois atributos referências completas aos certificados (`CompleteCertificateRefs`) e referências completas à revogação (`CompleteRevocationRefs`). Caso sejam utilizados certificados de atributos também é necessária a inclusão dos atributos referências aos certificados de atributo (`AttributeCertificateRefs`) e referências à revogação de atributo (`AttributeRevocationRefs`).

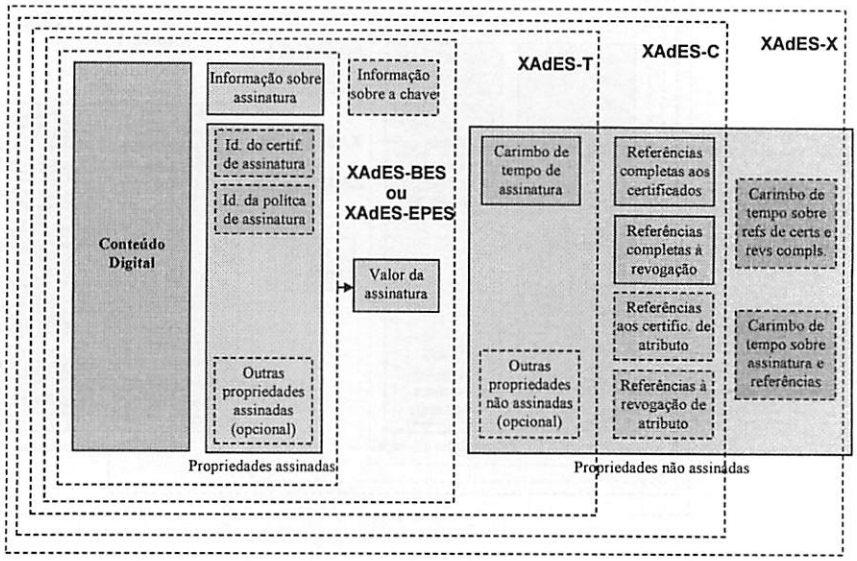
Este modelo estrutural é interessante em sistemas centralizados que mantém diversas assinaturas eletrônicas, pois possibilita manter na estrutura XML somente as referências aos certificados e objetos de revogação, mantendo o armazenamento dos certificados e objetos de revogação, por exemplo, em uma base de dados indexada pelo seu *hash*. Isto otimiza a alocação de espaço de armazenamento eletrônico. No momento que for necessário realizar uma validação, através das referências, tais objetos são recuperados da base de dados.



4.2.6 XAdES-X

O modelo estrutural *EXtended Electronic Signature with Time Indication* (XAdES-X) é baseado no modelo estrutural XAdES-C com a obrigatoriedade de inclusão do carimbo de tempo `SigAndRefsTimeStamp` (XAdES-X type 1) ou `RefsOnlyTimeStamp` (XAdES-X type 2).

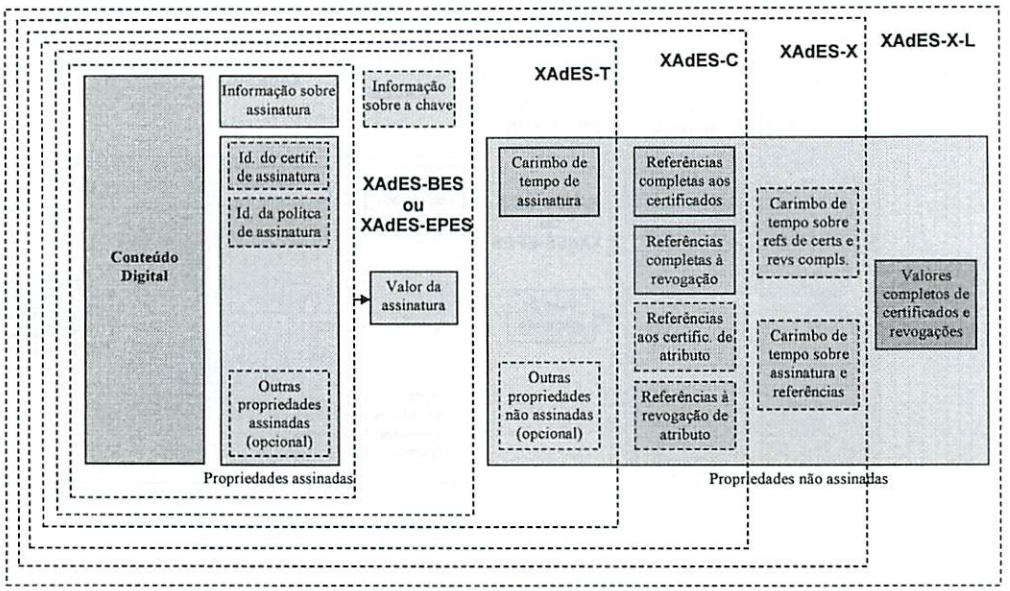
Este modelo de estrutural previne algumas situações catastróficas de comprometimento de chaves de AC, chaves de LCR ou chaves do serviço OCSP, propiciando uma redundância criptográfica sobre a assinatura eletrônica.



4.2.7 XAdES-X-L

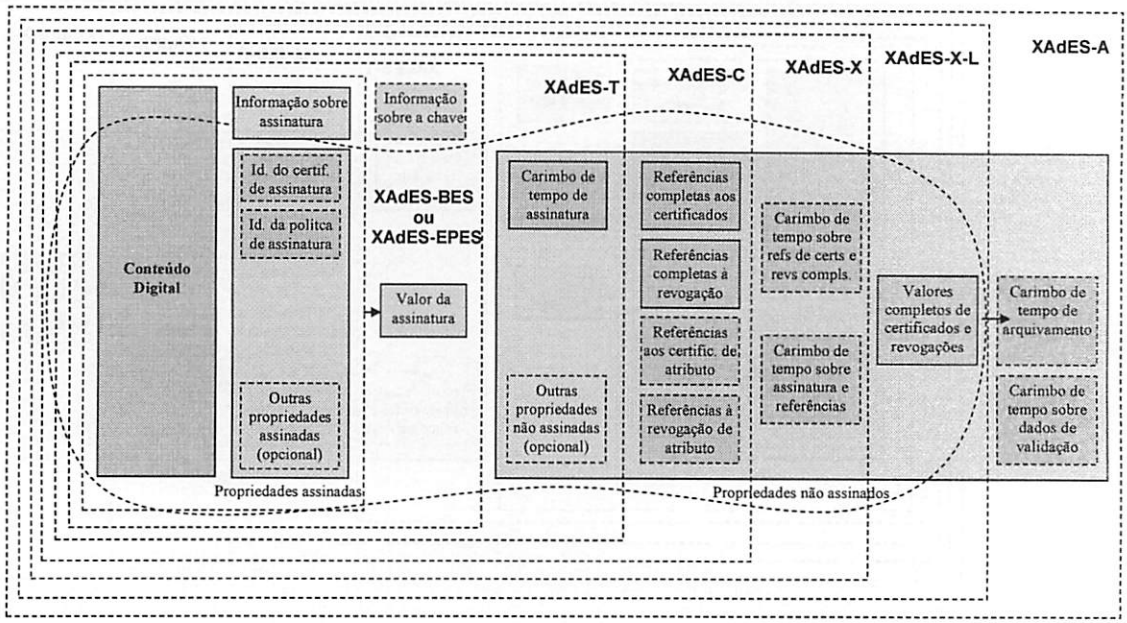
O modelo estrutural *EXtended* O modelo estrutural *Archival Electronic Signature* (CAdES-A) é baseado nos modelos estruturais CAdES-X-Long, CAdES-X-Long Type 1 ou CAdES-X-Long Type 2 com a obrigatoriedade de inclusão de um carimbo do tempo de arquivamento. Isto é possível através do uso do atributo carimbo de tempo de arquivamento (`archive-time-stamp`). Este modelo estrutural é utilizado para armazenar assinaturas eletrônicas por longo prazo.

Long Electronic Signature with Time Indication (XAdES-X-L) é baseado no modelo estrutural XAdES-X type 1 ou XAdES-X type 2 com a obrigatoriedade de inclusão das propriedades não assinadas `CertificateValues` e `RevocationValues`.



4.2.8 XAdES-A

O modelo estrutural *Archival Electronic Signatures* (XAdES-A) é baseado nos modelos estruturais CAdES-X-L, com a obrigatoriedade de inclusão de um carimbo do tempo de arquivamento (`xadesv141:ArchiveTimeStamp`). Este modelo estrutural é utilizado para armazenar assinaturas eletrônicas por longo prazo.


XAdES-A
XAdES-X-L
XAdES-X
XAdES-C
XAdES-T
Conteúdo Digital
Informação sobre assinatura
Informação sobre a chave
Id. do certif. de assinatura
Id. da politca de assinatura
Outras propriedades assinadas (opcional)
XAdES-BES ou XAdES-EPES
Valor da assinatura
Carimbo de tempo de assinatura
Outras propriedades não assinadas (opcional)
Referências completas aos certificados
Referências completas à revogação
Referências aos certific. de atributo
Referências à revogação de atributo
Carimbo de tempo sobre refs de certs e revs compls.
Carimbo de tempo sobre assinatura e referências
Valores completos de certificados e revogações
Carimbo de tempo de arquivamento
Carimbo de tempo sobre dados de validação
Propriedades assinadas
Propriedades não assinadas

5 Especificação PAdES

Os documentos no formato PDF [16 são largamente utilizados em todas as áreas e suportam, há mais de dez anos, diversos tipos de assinatura, dentre elas, a assinatura criptográfica de chave pública (*public key cryptographic signature*) e o formato *Criptographic Message Syntax - SignedData* (*CMS SignedData*).

5.1 Tipos de assinatura digital PDF

Um documento PDF suporta três tipos de assinatura digital, cada uma com finalidades diferentes:

- Assinatura de aprovação (*approval signature*);
- Assinatura de certificação (*certification signature*);
- Assinatura de direito de uso (*usage rights signature*).

A assinatura digital no PDF é armazenada em uma estrutura de dados denominada dicionário de assinatura (`signature dictionary`) de tipo dicionário (`dictionary`) (ISO 32000-1, seção 12.8.1, tabela 252) que contém todos os dados a respeito da assinatura digital. Um destes dados é a estrutura `CMS Signed Data`, codificada em DER, contendo a assinatura digital e alguns atributos.

5.1.1 Assinatura de aprovação

Um documento PDF pode conter uma ou mais assinaturas de aprovação (*approval signature*). A assinatura de aprovação é aquela assinatura tradicional realizada pelo usuário. A assinatura abrange a totalidade do documento.

5.1.2 Assinatura de certificação

A assinatura de certificação (*certification signature*) permite garantir a integridade e origem de formulários. É um tipo de assinatura que permite realizar alterações em determinadas partes do documento para, por exemplo, possibilitar o preenchimento de formulário e inserção de comentários mantendo a assinatura de certificação ainda

válida. Um documento PDF pode conter no máximo uma assinatura de certificação e utiliza a funcionalidade MDP (*Modification Detection Permissions*) que permite que o documento seja modificado em certas partes.

5.1.3 Assinatura de direito de uso

O último tipo de assinatura, a assinatura de direito de uso (*usage right signature*) é utilizada para habilitar funcionalidades especiais interativas no documento.

5.2 Suporte do PDF ao AdES

Recentemente, o comitê técnico ETSI/ESI iniciou estudos para definição de uma especificação para assinatura eletrônica avançada (*Advanced Electronic Signature – AdES*) exclusiva para PDF, denominada *PDF Advanced Electronic Signature* (PAdES).

A especificação PAdES difere do CAdES e XAdES pois é voltada exclusivamente para documentos PDF, definindo requisitos que devem ser atendidos pelos softwares de visualização e edição PDF quando são utilizadas assinaturas digitais, além de determinar quais elementos do PDF podem constar e quais elementos não devem constar. Outra característica interessante suportada pelo PDF é assinatura eletrônica integrada a formulários. Estas são características chaves que distinguem a especificação PAdES do CAdES e XAdES.

Como resultado deste trabalho, em junho de 2009, o ETSI/ESI definiu pela publicação de um conjunto de especificações para PAdES dividida em 5 partes, apresentadas no Quadro 7.

Quadro 7 - Partes da especificação *PDF Advanced Electronic Signature* (PAdES).

Especificação		Título
Parte1	*PAdES Overview* [3]	*A framework document for PAdES1*
Parte 2	*PAdES Basic* [4]	*CMS Profile based on ISO 32000*
Parte 3	*PAdES Enhanced* [5]	*PAdES-BES and PAdES-EPES Profiles*
Parte 4	*PAdES Long Term* [6]	*PAdES-LTV Profile*
Parte 5	*PAdES for XML Content* [7]	*Profiles for XAdES signatures of XML content in PDF*

		files

A parte1 desta especificação apresenta uma visão geral das outras partes do documento. A parte 2 descreve o perfil de assinatura eletrônica *PAdES Basic* a ser utilizado no PDF para aderência ao AdES (*Advanced Electronic Signature*) baseado somente nos recursos disponíveis atualmente pela especificação ISO 32.000-1 (PDF 1.7).

A parte 3 (*PAdES Enhanced*) define perfis aderentes ao CAdES-BES e CAdES-EPES, chamados de PAdES-BES e PAdES EPES. Este perfil procura incorporar o CAdES aos arquivos PDF.

A parte 4 trata das questões relacionadas à validação em longo prazo (*long-term validation - LTV*) no PDF.

A parte 5 descreve como incorporar XAdES ao PDF (XML-DSIG é suportada atualmente pelo ISO 32.000-1).

As características propostas para as partes 3 a 5 foram submetidas à ISO para inclusão na próxima revisão da norma ISO 32.000-1, com expectativa de publicação no final de 2011.

5.2.1 PAdES Basic

Com base no conjunto de funcionalidades existentes atualmente no padrão ISO 32.000-1 (PDF 1.7) [16] foi selecionado um perfil próximo às funcionalidades existentes no padrão ETSI CAdES.

Assim, dentre as diversas tecnologias e formatos suportados na ISO 32.000-1 para assinatura digital, foi selecionada a tecnologia de assinatura criptográfica de chave pública (*public key cryptographic signature*) e o formato *Criptographic Message Syntax (CMS) SignedData* derivada da especificação *PKCS#7 Signed Data*. Além disso, também suporta assinatura serial, inclusão de carimbo do tempo de assinatura e inclusão de dados sobre estado de revogação do certificado digital.

5.2.1.1 Visão geral das características *PAdES Basic*

As principais características do perfil *PAdES Basic* são apresentadas na Tabela 6:

Quadro 8 - Principais características do *PAdES Basic* e sua comparação com CAdES.

Característica PAdES	Comparação com CAdES
Tecnologia de assinatura criptográfica de chave pública	Idêntico ao CAdES
Formato CMS	Idêntico ao CAdES
Suporte a assinatura serial	A assinatura serial utiliza recursos internos do PDF, não utilizando os recursos do CMS e, portanto, difere do CAdES.
Permite a inclusão de carimbo de tempo de assinatura	Idêntico ao CAdES
Permite a inclusão da cadeia de certificação	Incluído no campo `Certificates` do `CMS SignedData`
Permite a inclusão de certificado de atributo.	Idêntico ao CAdES. Na validação de assinatura, não existe obrigatoriedade de validação dos certificados de atributo.
Permite a inclusão de dados sobre estado de revogação de certificado digital	Utiliza um atributo assinado específico, incluído no CMS. Permite incluir LCR e OCSP
Permite a inclusão do instante de assinatura.	Instante de assinatura é armazenada em um campo específico (M) do dicionário de assinatura.
Possibilidade de inclusão da razão da assinatura.	Razão da assinatura é armazenada em um campo específico (Reason) do dicionário de assinatura.
Possibilidade de inclusão da localização do signatário.	Localização do signatário é armazenada em um campo específico (*Location*) do dicionário de assinatura.
Possibilidade de inclusão de informações de contato do signatário.	Contato do signatário é armazenado em um campo específico (*ContactInfo*) do dicionário de assinatura.

5.2.1.2 Suporte a múltiplas assinaturas (em paralelo ou serial)

A especificação PDF não admite a existência de assinaturas de aprovação em paralelo (*co-sign*), ou seja, várias assinaturas relacionadas ao mesmo conteúdo. Porém, admite assinaturas seriais, ou seja, assinatura realizada sobre um documento já assinado, como ilustrado na Figura 18.

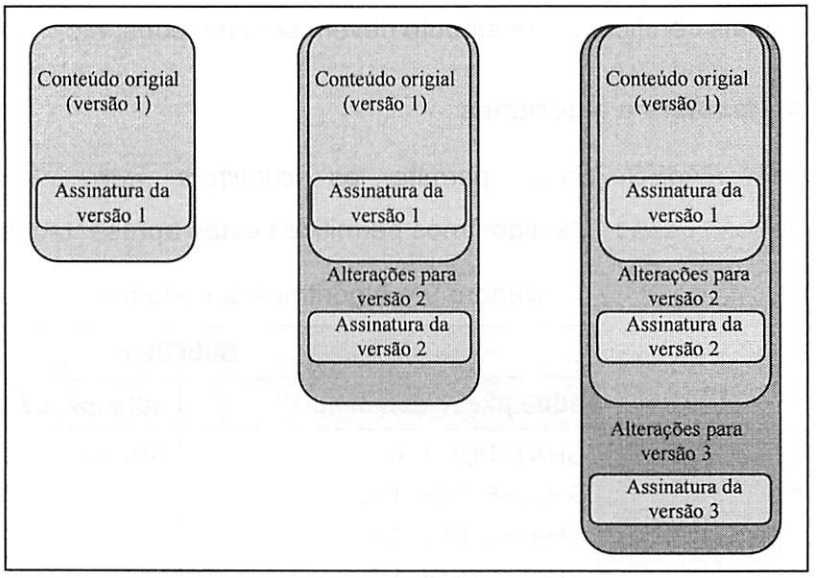


Figura 18 – Exemplo de aplicação de assinaturas de aprovação seriais no PDF.

Esta forma de assinatura serial é diferente da contra assinatura (*counter signature*) suportada no CMS. No CMS, a contra assinatura corresponde à assinatura do bloco de assinatura de um signatário anterior incluída no atributo CMS não assinado `counter signature`. Sendo a assinatura realizada sobre uma assinatura já existente, o documento assinado é o mesmo.

No PDF, o conteúdo associado a cada assinatura pode conter revisões (alterações, adições e supressões).

5.2.1.3 Dicionário de valores semente

O dicionário de valores semente (*seed value dictionary*) (ISO 32000-1, seção 12.7.4.5, tabela 234) contém dados relacionados a determinadas regras definidas pelo autor de um documento ou formulário acerca de como deve ser realizada a assinatura digital. As descrições podem ser requisitos ou recomendações.

Os valores sementes permitem especificar, por exemplo:

- Qual algoritmo *hash* deve ser utilizado na assinatura;
- Qual informação de revogação deve ser incluída;
- Qual autoridade de carimbo de tempo deve ser utilizada;

- Quais certificados de atributo devem ser anexados, etc.

5.2.1.4 *Handlers* e algoritmos

O perfil *PAdES Basic* permite os *subfilters* `adbe.pkcs7.detached` e `adbe.pkcs7.sha1`. Os algoritmos permitidos estão apresentados no Quadro 9.

Quadro 9 – Algoritmos suportados.

	SubFilter	
	adbe.pkcs7.detached	**adbe.pkcs7.sha1**
Hash	SHA1 (PDF 1.3) SHA256 (PDF 1.6) SHA384 (PDF 1.7) SHA512 (PDF 1.7) RIPEMD160 (PDF 1.7)	SHA1 (PDF 1.3)
RSA	Up to 1024-bit (PDF 1.3) Up to 2048-bit (PDF 1.5) Up to 4096-bit (PDF 1.5)	Up to 1024-bit (PDF 1.3) Up to 2048-bit (PDF 1.5) Up to 4096-bit (PDF 1.5)

5.2.1.5 Limitações

A principal limitação do PAdES Basic é a não possibilidade de inclusão de atributos para validação a longo prazo (cadeias de certificados dos signatários, dados de revogação e carimbos de tempo de arquivamento). Isto ocorre, inclusive, devido à definição de uma área de tamanho fixo para armazenamento da estrutura `CMS SignedData`.

5.2.2 PAdES Enhanced

A especificação do perfil *PAdES Enhanced* procura compatibilizar a estrutura `CMS SignedData` existente atualmente no dicionário de assinatura do PDF para aderência completa ao CAdES-BES, CAdES-EPES e CAdES-T.

Esta proposta foi submetida à ISO para a nova versão do padrão ISO 32.000-2.

Em relação às limitações, novamente, a principal limitação do *PAdES Enhanced* é a não possibilidade de inclusão de atributos para validação a longo prazo (cadeias de

certificados dos signatários, dados de revogação e carimbos do tempo de arquivamento). Isto ocorre, inclusive, devido à definição de uma área de tamanho fixo para armazenamento da estrutura `CMS SignedData`.

5.2.3 PAdES Long Term

A especificação do perfil *PAdES Long Term* trata das questões relacionadas à validação em longo prazo (*long-term validation - LTV*) no PDF.

Este perfil estende o perfil PAdES Basic ou *PAdES Enhanced* de forma a possibilitar a adição de:

- Dados para validação dos certificados da cadeia de certificação;
- Dados para validação de LCR e de respostas OCSP;
- Dados para validação do carimbo de tempo;
- Carimbo de tempo de arquivamento.

O carimbo de tempo de arquivamento é um controle para proteção do documento em longo prazo.

A especificação do perfil *PAdES Long Term* é funcionalmente equivalente ao *CAdES-X-Long* e *CAdES-A.*

Para possibilitar a validação a longo prazo é necessário incluir, no documento PDF, todos os dados necessários para a validação da assinatura, já que tais elementos podem não estar disponíveis no futuro. Os dados necessários para validação incluem as cadeias de certificados dos signatários e as LCR ou respostas OCSP necessárias à validação do certificado. Estes dados não são alocados na estrutura `CMS SignedData`, mas em uma área específica, ao final do documento PDF. Esta funcionalidade é funcionalmente equivalente ao *CAdES-X-Long*.

Em um documento assinado digitalmente, com o passar do tempo, os riscos de vulnerabilidades criptográficas aumentam. Por este motivo é recomendada a inclusão de um carimbo do tempo para arquivamento a fim de garantir a integridade do certificado digital do signatário e a integridade da assinatura digital do

documento. *PAdES Long Term* difere do *CAdES-A* por alocar áreas específicas ao final do documento PDF para adição do carimbo do tempo para arquivamento.

Esta estratégia possibilita resolver um dos grandes problemas existentes no *CAdES-A*: da não existência de um local adequado na estrutura `CMS SignedData` para armazenamento de dados globais às assinaturas. Na estrutura `CMS SignedData` os atributos são sempre relacionados a um determinado `SignerInfo` (ou seja, a um determinado signatário).

A Figura 17 ilustra a aplicação de dados de validação e a aplicação de carimbo do tempo para arquivamento para proteção da assinatura do documento e dos certificados digitais (do signatário e do restante da sua cadeia de certificação).

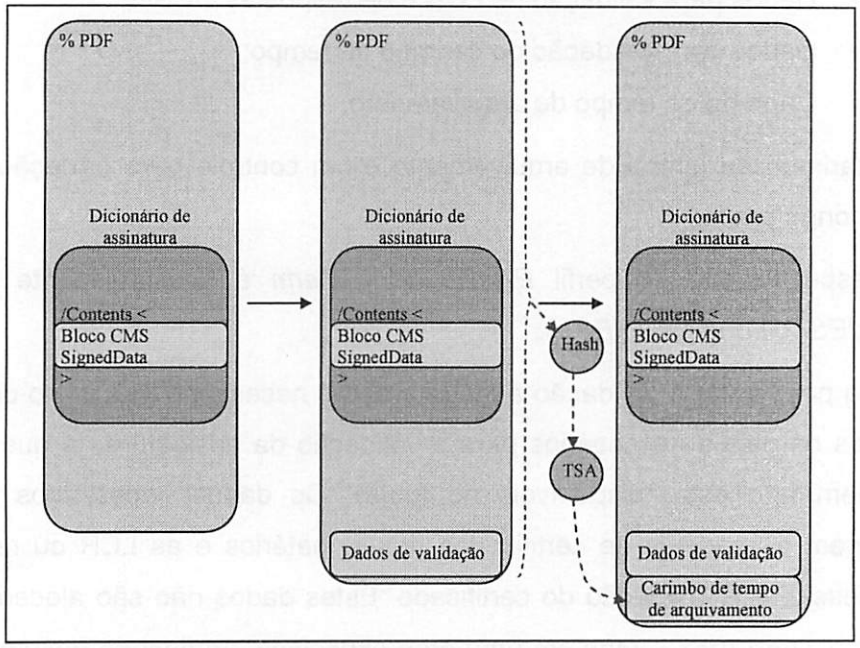


Figura 19 – Exemplo de *PAdES Long Term*.

Com o passar do tempo, o próprio carimbo de tempo de arquivamento torna-se vulnerável, necessitando da reaplicação de outro carimbo de tempo de arquivamento.

O perfil *PAdES Long Term* permite a inclusão repetida de dados para validação (tipicamente os certificados digitais da cadeia de certificação do certificado utilizado

pelo TSA para assinatura do carimbo de tempo) e de outro carimbo de tempo de arquivamento, como ilustrado na Figura 18.

Para armazenamento dos dados para validação em longo prazo (*long-term validation – LTV*) foi proposta a utilização da estrutura DSS (*Document Security Store*) do Acrobat 9.1. Nela seriam armazenados os certificados, LCRs e OCSPs necessários para validação completa.

Para armazenamento do carimbo do tempo de arquivamento (*Document TimeStamp*) foi proposto uma variante do dicionário de assinatura existente atualmente, com tipo /Type/DocTimeStamp, com subfilter /Subfilter/ETSI.RFC3161 e com hash sendo calculado sobre todo ByteRange.

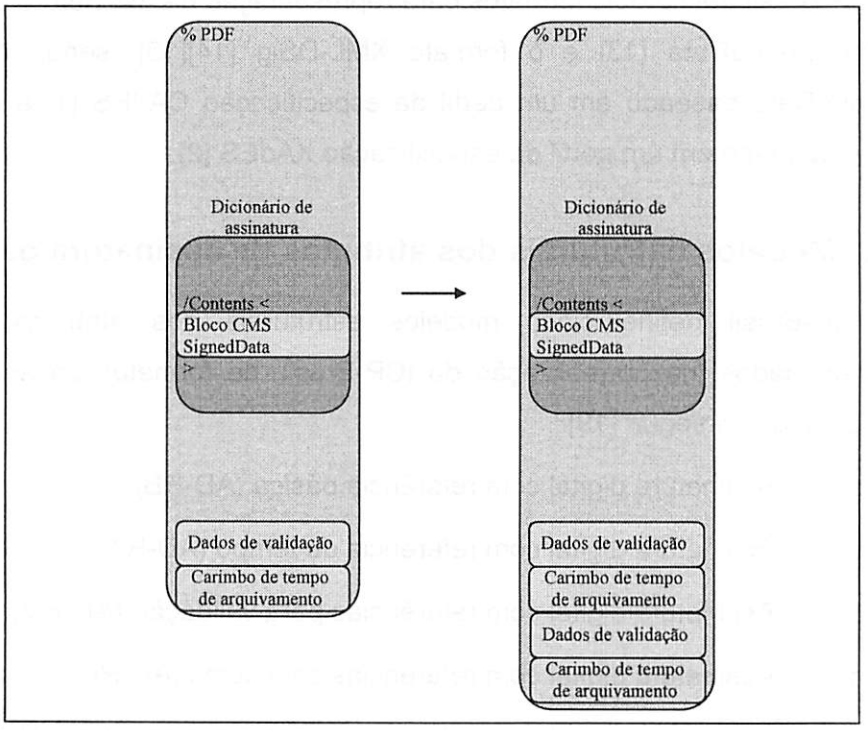


Figura 20 – Exemplo de *PAdES Long Term* para proteção contra expiração do carimbo de tempo de arquivamento.

Estas propostas foram submetidas à ISO para a nova versão do padrão ISO 32.000-2.

6 Normalização da ICP-Brasil

Segundo o DOC-ICP-15 [19], "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 Formatos de representação de assinatura digital da ICP-Brasil

A ICP-Brasil define dois formatos para representação da assinatura digital: o formato CMS SignedData [13] e o formato XML-DSig [14][15], sendo o formato CMS SignedData baseado em um perfil da especificação CAdES [1] e o formato XML-DSig baseado em um perfil da especificação XAdES [2].

6.2 Modelos estruturais dos atributos de assinatura da ICP-Brasil

A ICP-Brasil define cinco modelos estruturais dos atributos de assinatura (denominados, na normalização da ICP-Brasil, de formatos de assinatura digital), relacionados a seguir [19]:

a) Assinatura digital com referência básica (AD-RB);

b) Assinatura digital com referência de tempo (AD-RT);

c) Assinatura digital com referências para validação (AD-RV);

d) Assinatura digital com referências completas (AD-RC);

e) Assinatura digital com referências para arquivamento (AD-RA).

Estes modelos estruturais dos atributos de assinatura devem ser utilizados tanto no tanto com o formato CMS SignedData quanto com o formato XML DSig, sendo de fato, perfis da ICP-Brasil da especificação CAdES e XAdES.

Na ICP-Brasil, é obrigatório a inclusão do atributo política de assinatura, sendo definidas políticas de assinatura: para cada modelo estrutural e para cada formato (CMS SignedData e XML DSig). Tais políticas são registradas pela ICP-Brasil.

6.2.1 Assinatura digital com referência básica (AD-RB)

O modelo estrutural AD-RB é o mais simples de todos. Este modelo estrutural é equivalente ao CAdES-EPES e XAdES-EPES.

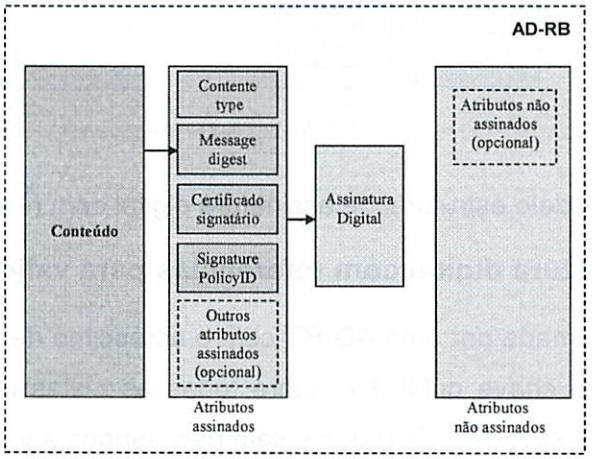


Figura 21 - Modelo estrutural de assinatura digital com referência básica (AD-RB).

6.2.2 Assinatura digital com referência de tempo (AD-RT)

A AD-RT é formada por uma AD-RB com o acréscimo de um carimbo do tempo de assinatura. Este modelo estrutural é equivalente ao CAdES-T e XAdES-T.

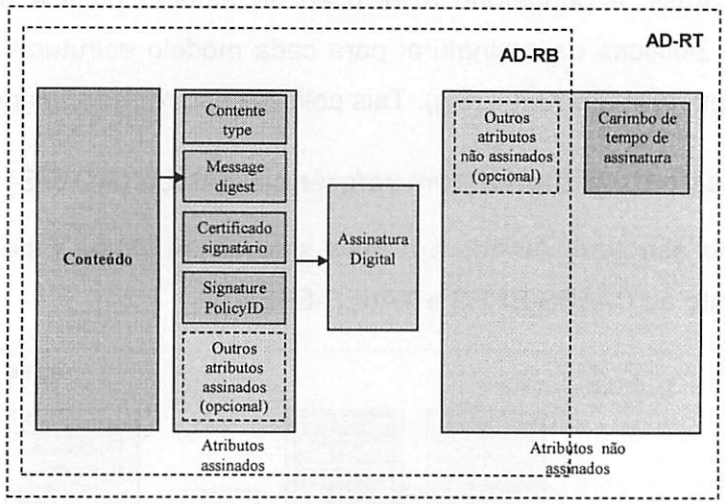


Figura 22 - Modelo estrutural de assinatura digital com referência de tempo (AD-RT).

6.2.3 Assinatura digital com referências para validação (AD-RV)

A AD-RV é formada por uma AD-RT com o acréscimo de referências sobre todos os certificados de chave pública e sobre todas as Listas de Certificados Revogados (LCR) ou respostas de OCSP que sejam necessários à validação daquela assinatura. Sobre esses dados é acrescentado (ou logicamente conectado) um carimbo do tempo de validação. Este modelo estrutural é equivalente ao CAdES-X-Type 1 e XAdES-X-Type 1.

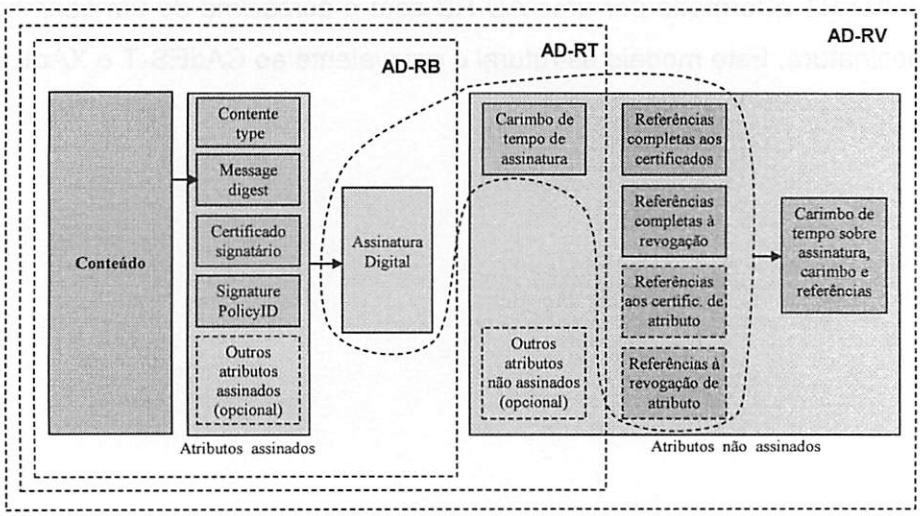


Figura 23 - Modelo estrutural de assinatura digital com referências para validação (AD-RV)

6.2.4 Assinatura digital com referências completas (AD-RC)

Uma AD-RC é formada por uma AD-RV com o acréscimo de todos os dados necessários para validação da assinatura. Este modelo estrutural é equivalente ao CAdES-X-Long Type 1 e XAdES-X-L-Type 1.

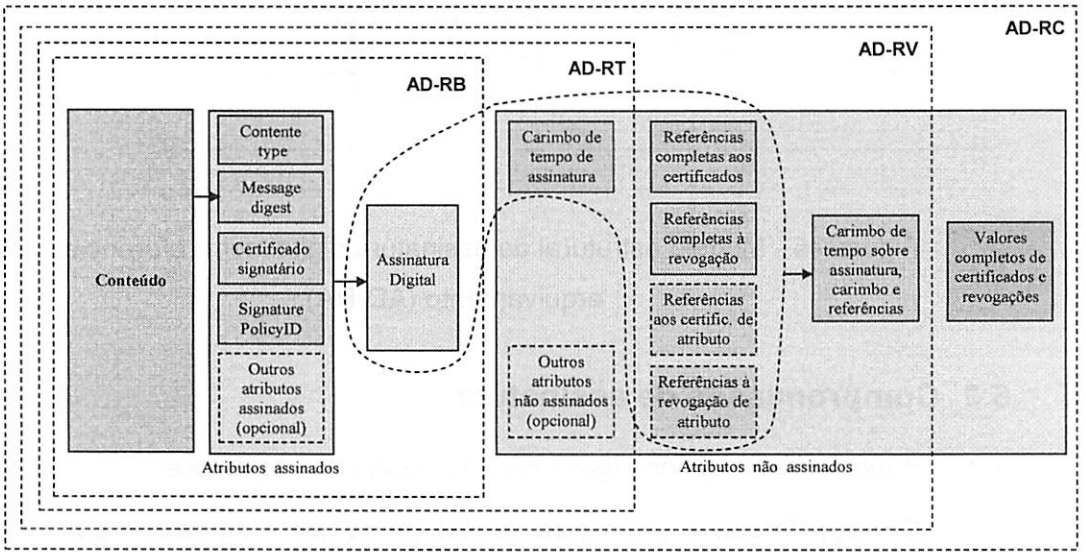


Figura 24 - Modelo estrutural de assinatura digital com referências completas (AD-RC)

6.2.5 Assinatura digital com referências para arquivamento (AD-RA)

Uma AD-RC é formada por uma AD-RT com o acréscimo de todas as referências de validação e todos os dados necessários para validação da assinatura. O carimbo do tempo de validação é opcional. Este modelo estrutural é equivalente ao CAdES-A e XAdES-A.

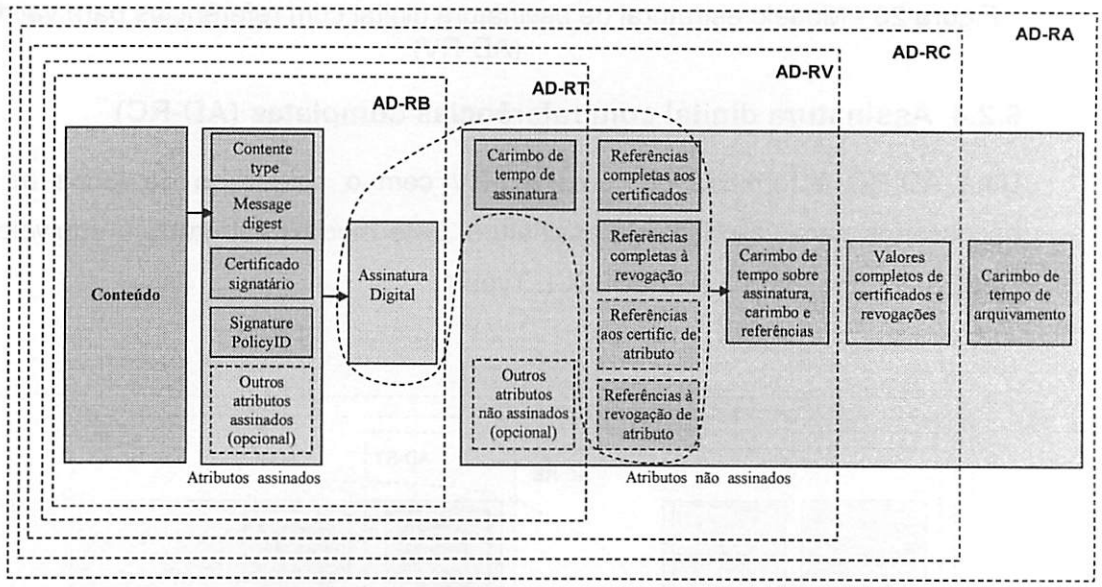


Figura 25 - Modelo estrutural de assinatura digital com referências para arquivamento (AD-RA).

6.3 Compromissos de assinatura

A ICP-Brasil também define alguns compromissos de assinatura:

- **Concordância**: A assinatura aposta indica que o signatário concorda com o conteúdo assinado;
- **Autorização**: A assinatura aposta indica que o signatário autoriza o constante no conteúdo assinado;
- **Testemunho**: A assinatura aposta indica o compromisso detestemunhodo signatário. Não necessariamente indica a concordância do signatário com o conteúdo;
- **Autoria**: A assinatura aposta indica que o signatário foi autor do conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo;
- **Conferência**: A assinatura aposta indica que o signatário realizou a conferência do conteúdo;

- **Revisão**: A assinatura aposta indica que o signatário revisou o conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo;
- **Ciência**: A assinatura aposta indica que o signatáriotomou ciência do conteúdo assinado. Não necessariamente indica concordância do signatário com o conteúdo;
- **Publicação**: A assinatura tem o propósito de indicar que o signatário publicou o documento em algum meio de comunicação externo à entidade que o originou;
- **Protocolo**: A assinatura aposta indica a intenção do signatário em protocolar o conteúdo.
- **Integridade**: A assinatura aposta indica a intenção do signatário em garantir somente a integridade da mensagem.
- **Autenticação**: A assinatura aposta é utilizada somente como de usuário prova de autenticação do signatário;
- **Teste**: A assinatura aposta indica a intenção do signatário em realizar um teste.

Na última versão da normalização da ICP-Brasil sobre assinatura digital (DOC-ICP-15) tais compromissos foram retirados do documento de normalização. Assim, restaram somente os compromissos genéricos definidos na especificação CAdES e XAdES:

- **Prova de origem:** A prova de origem indica que o signatário reconhece ter criado, aprovado e disponibilizado o conteúdo assinado.

  OID = id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1};

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin;
- **Prova de recepção**: A prova de recepção indica que o signatário reconhece ter recebido o conteúdo assinado. Equivale a um visto.

  OID = id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2};

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt;

- **Prova de entrega**: A prova de entrega indica que o signatário, um provedor confiável de serviço (*Trusted Service Provider - TSP*), disponibilizou o conteúdo assinado em um local acessível ao destinatário.

  OID = id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3};

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery;

- **Prova de encaminhamento:** A prova de encaminhamento indica que o signatário encaminhou o conteúdo assinado, mas não necessariamente criou ou aprovou o conteúdo.

  OID = id-cti-ets-proofOfSender OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 4} ;

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfSender;

- **Prova de aprovação:** A prova de aprovação indica que o signatário aprovou o conteúdo da mensagem.

  OID = id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5};

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfApproval;

- **Prova de criação:** A prova de criação indica que o signatário criou o conteúdo, mas não necessariamente o aprova.

  OID = id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6};

  URI = http://uri.etsi.org/01903/v1.2.2#ProofOfCreation;

7 Certificado de atributo

O certificado de atributo possibilita automatizar o processo da verificação da assinatura, permitindo verificar de forma segura se o signatário possui autoridade para assinatura do documento.

O certificado de atributo é um recurso definido inicialmente na especificação x509 (a mesma que definiu o certificado digital), sendo o perfil definido na RFC 3281 o mais utilizado atualmente.

No contexto do SREI, o certificado de atributo poderia ser utilizado para verificar a autoridade do signatário dos documentos emitidos pelo cartório (certidões, notas de exigência, etc) e dos documentos presentes nos livros eletrônicos.

Os certificados de atributo são emitidos pelas fontes de autoridade, entidades detentoras do direito de emissão dos privilégios.

No contexto do Registro de Imóveis, o Poder Judiciário é o responsável pela atribuição de poder aos Oficiais Registradores. Assim, seriam os responsáveis pela emissão, para cada Oficial Registrador, do certificado de atributo.

O certificado de atributo é gerado pela Autoridade de Atributo. Assim, o Poder Judiciário teria uma Autoridade de Atributo.

O certificado de atributo, neste caso, deveria informar:

- Nome do oficial registrador;
- Privilégio "Oficial de Registro de Imóveis";
- Identificação do cartório;
- Possibilidade de delegação deste privilégio uma única vez.

Este certificado deveria possuir validade de alguns anos, com possibilidade de revogação.

O Oficial deveria poder, a seu critério, delegar este privilégio para seus prepostos, gerando certificados de atributos para eles Isto é realizado pelo Oficial com o auxílio

de um programa, emitindo e assinado, utilizando a chave privada associada a seu certificado digital, o certificado de atributo do seu preposto. O certificado de atributo dos prepostos não deveria possuir revogação. Por este motivo, deveria possuir validade curta (por exemplo, alguns dias).

Com a utilização do certificado de atributo, uma pessoa que esteja verificando, por exemplo, a assinatura de uma certidão, após a verificação da assinatura, deve verificar a autoridade do signatário. Para isso, deve já ter estabelecido seu contexto de segurança: os certificados raiz da ICP-Brasil e as fontes de autoridade dos privilégios, neste caso o Poder Judiciário para o privilégio de Oficial de Registro de Imóveis.

8 Referências

[1] ETSI TS 101 733 v1.8.1. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), Technical Specification, Nov. 2009.

[2] ETSI TS 101 903 v1.4.1. Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[3] ETSI TS 102 778-1 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 1: PAdES Overview: a framework document for PAdES. ETSI. 20p. July, 2009.

[4] ETSI TS 102 778-2 v1.2.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 2: PAdES Basic: CMS profile based on ISO 32.000-1. ETSI. 12p. 2009.

[5] ETSI TS 102 778-3 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles. ETSI. 20p. July, 2009.

[6] ETSI TS 102 778-4 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 4: PAdES Long Term – PAdES-LTV Profile. ETSI. 20p. July, 2009.

[7] ETSI TS 102 778-4 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 5: PAdES for XML Content – Profiles for XAdES signatures. ETSI. 20p. July, 2009.

[8] RSA LABORATORIES. PKCS#7: Crypographic message syntax standard. RSA. Version 1.4. Laboratories Technical Note. 1993.

[9] RSA LABORATORIES. RFC 2315: PKCS#7 - Cryptographic message syntax (CMS) - version 1.5. March 1998. March 1998. (disponível em http://www.ietf.org/rfc/rfc2315.txt).

[10] HOUSLEY, R. RFC 2630: Cryptographic message syntax (CMS). Internet Engineering Task Force (IETF). June 1999. (disponível em http://www.ietf.org/rfc/rfc2630.txt).

[11] HOUSLEY, R. RFC 3369: Cryptographic message syntax (CMS). Internet Engineering Task Force (IETF). August 2002. (disponível em http://www.ietf.org/rfc/rfc3369.txt).

[12] HOUSLEY, R. RFC 3852: Cryptographic message syntax (CMS). Internet Engineering Task Force (IETF), July 2004. (disponível em http://www.ietf.org/rfc/rfc3852.txt).

[13] HOUSLEY, R. RFC 5652: Cryptographic message syntax (CMS). Internet Engineering Task Force (IETF), Sep. 2009. (disponível em http://www.ietf.org/rfc/rfc5652.txt).

[14] EASTLAKE 3rd, D.; REAGLE, J.; SOLO, D. RFC 3275. (Extensible Markup Language) XML-Signature Syntax and Processing. IETF, mar. 2002.

[15] BARTEL, M; et. All. XML Signature Syntax and Processing. Second edition. World Wide Web Consortium (W3C). June, 2008.

[16] ISO 32000-1:2008 – Document management: portable document format (PDF 1.7). 748p. 2008.

[17] The AdES family of standards: CAdES, XAdES and PAdES: implementation guidance for using electronic signatures in the European Union. Adobe Systems Inc. 2009.

[18] ITU-T. ITU-T Recommendation X.690, Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>. Acesso em: 19 mar. 2010.

[19] ICP-Brasil. DOC-ICP-15: Visão geral sobre assinaturas digitais na ICP-Brasil. ICP-Brasil. Versão 2.0. Abril. 2010.