UNIVERSIDAD DE MURCIA

CURSO DE ADMINISTRACIÓN ELECTRÓNICA

Tema 3 – Formatos de firma electrónica

Daniel Sánchez Martínez (danielsm@um.es)
Proyecto Administración Electrónica
Universidad de Murcia

Objetivos

- Clasificar las diferentes tipologías de firma electrónica.
- Comprender los diferentes formatos de firma electrónica más extendidos en la actualidad.
- Conocer las diferentes posibilidades para relacionar los datos de firma y el documento firmado.
- Entender la problemática de la firma electrónica avanzada y los estándares AdES.
- Introducir el formato de firma XAdES y sus diferentes perfiles.

UNIVERSIDAD DE MURCIA

Tipos de firma

- Según el tipo de certificado
- Según su formato
  - CMS
  - XML
  - PDF
- Según la relación entre los datos y la firma
- Según el número de firmantes

Tipos de Firma

- Según el certificado:
  - Firma de usuario
    - Perfil ‘persona física’
    - Perfil ‘persona jurídica’
    - Perfil ‘empleado público’
  - Firma de servidor
    - Sede electrónica y sello de órgano.
    - Servidores web → túnel SSL
    - Firma automática (sellado, registro, notificación…)
  - Firma de código
    - Componentes que se ejecutan en los clientes.

Tipos de Firma

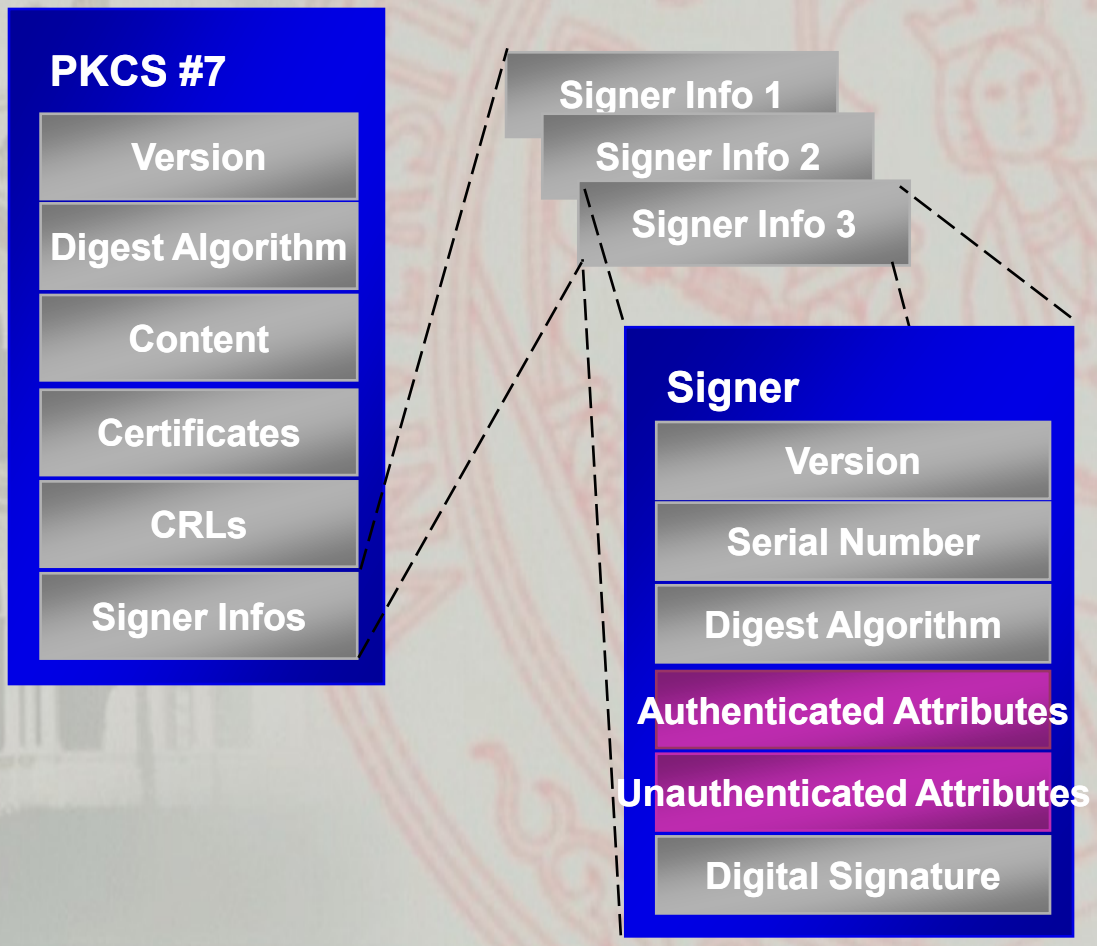
- Según el formato (firmas básicas):
  - CMS (Cryptographic Message Syntax) – PKCS#7
    - Codificación ASN.1-DER (RFC 3852)
    - Librerías
      - OpenSSL y CAPICOM ActiveX (Win32)
      - .NET Framework 2.0 (soporte nativo)
      - IAIK y BouncyCastle (Java)
  - XML Signature
    - Codificación XML (RFC 3075)
    - Librerías:
      - .NET Framework 2.0 (soporte nativo)
      - IAIK y Apache XML Security (Java)
      - JRE 1.6 (soporte nativo)
  - PDF
    - Soporta PKCS#7
    - Librerías:
      - iText (Java)

Tipos de Firma

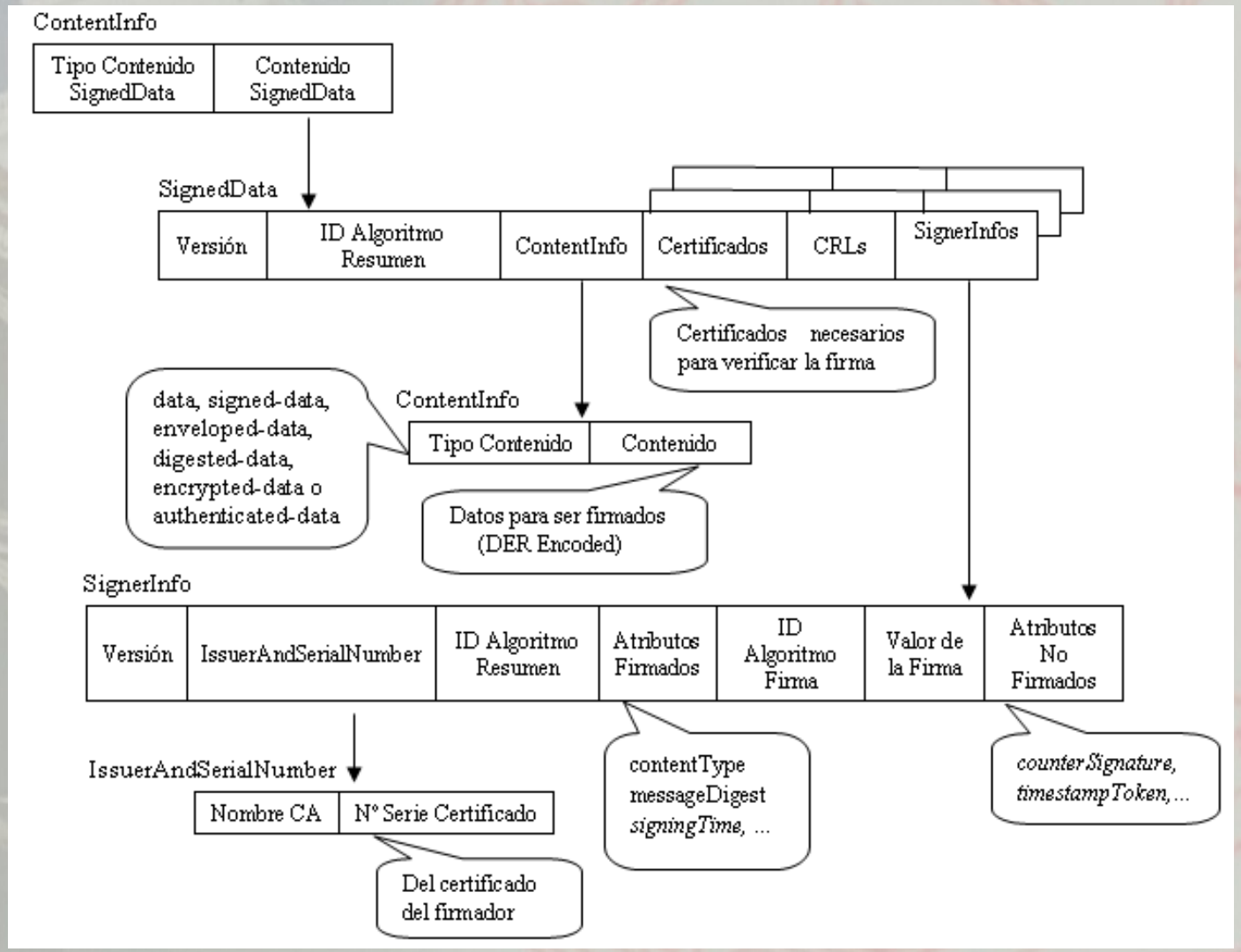
- Según la relación entre la propia firma y los datos que se firman:
  - Detached (CMS y XMLdsig)
    - La firma está separada del documento
  - Enveloping (CMS y XMLdsig)
    - La firma contiene el documento
  - Enveloped (XMLdsig y PDF)
    - La firma está incluida dentro del documento

Tipos de Firma. Firma CMS

- CMS o PKCS#7

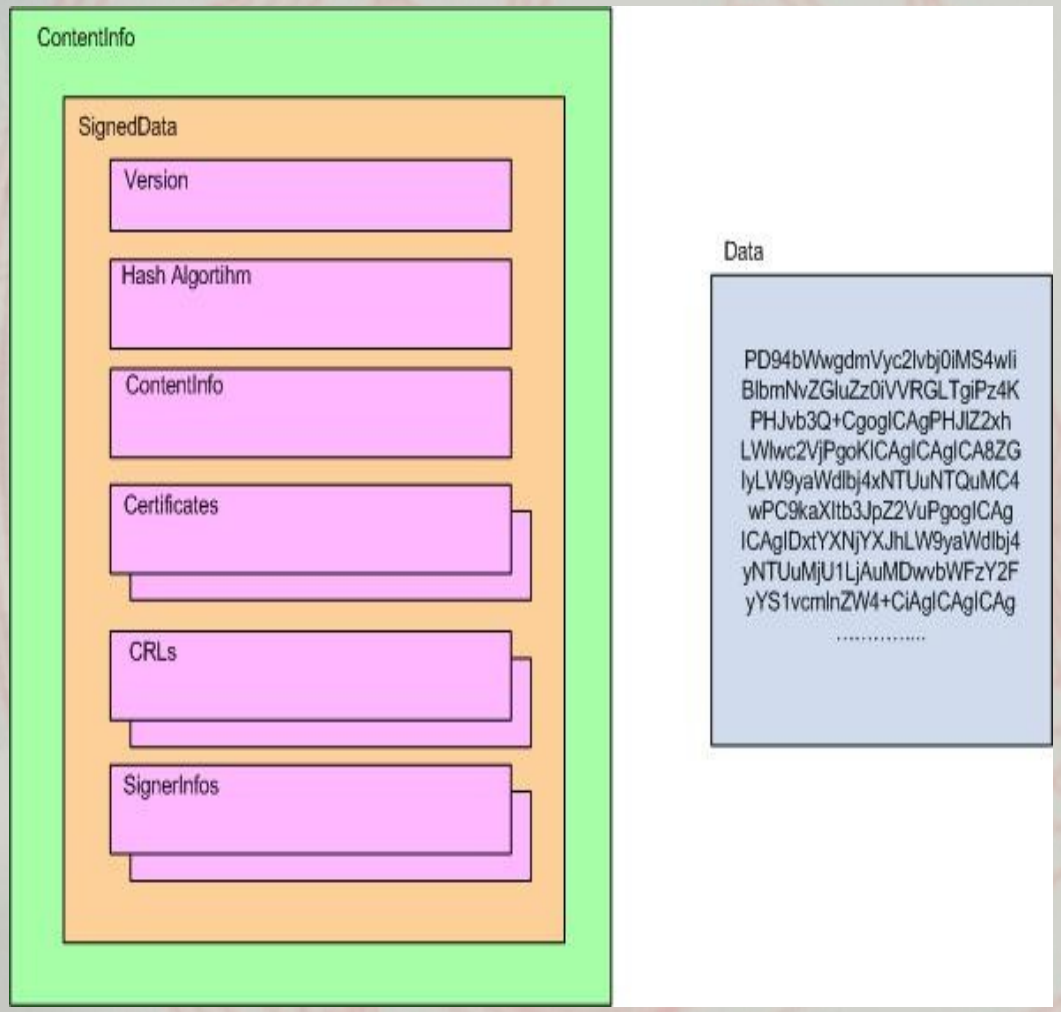


Tipos de Firma. Firma CMS



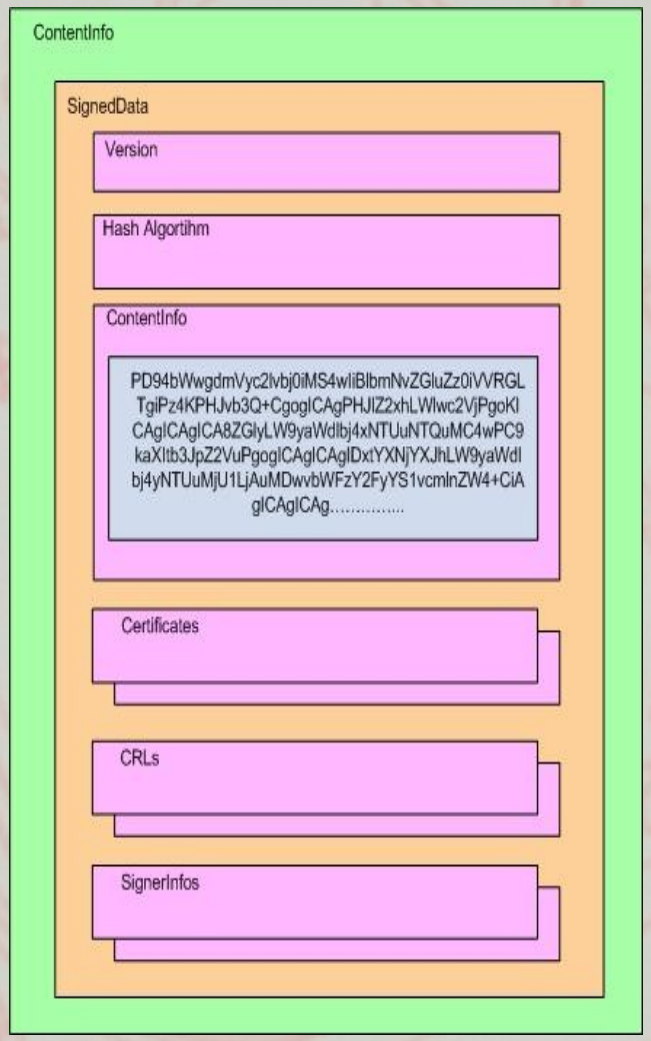
Tipos de Firma. Firma CMS

- Firma Detached



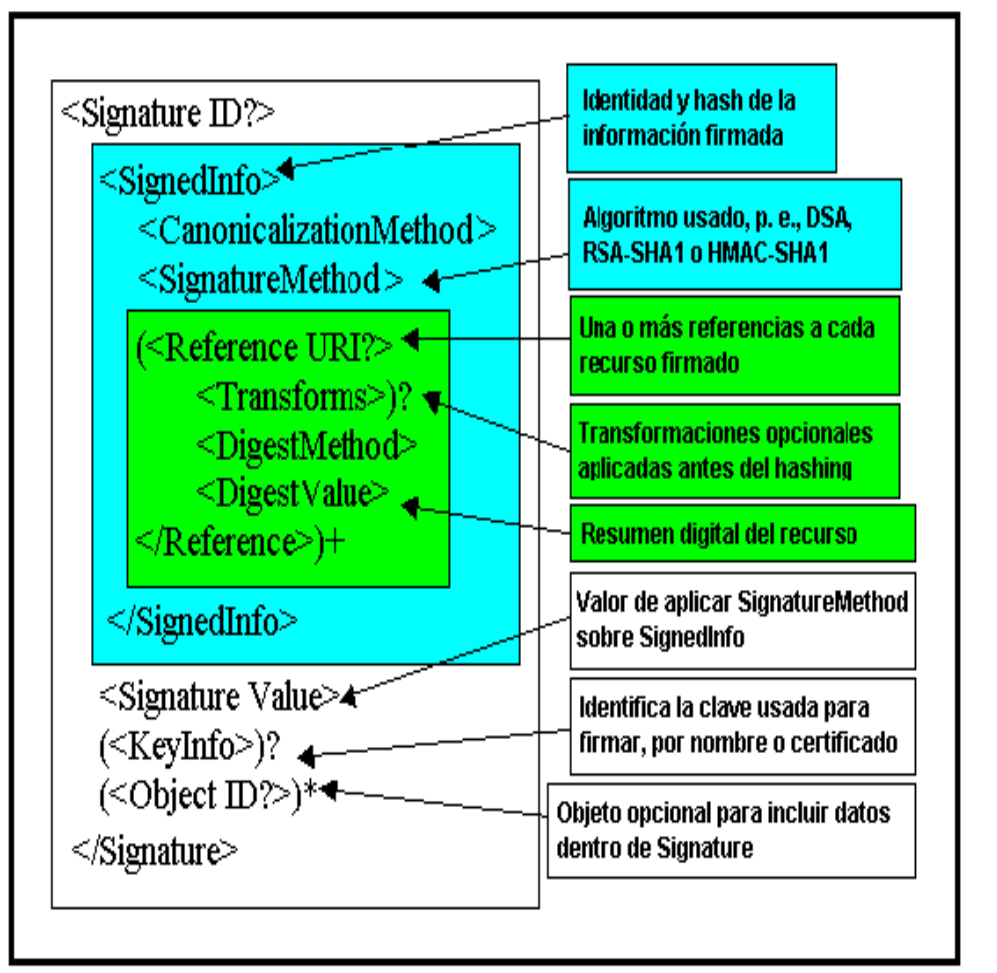
Tipos de Firma. Firma CMS

- Firma Enveloping



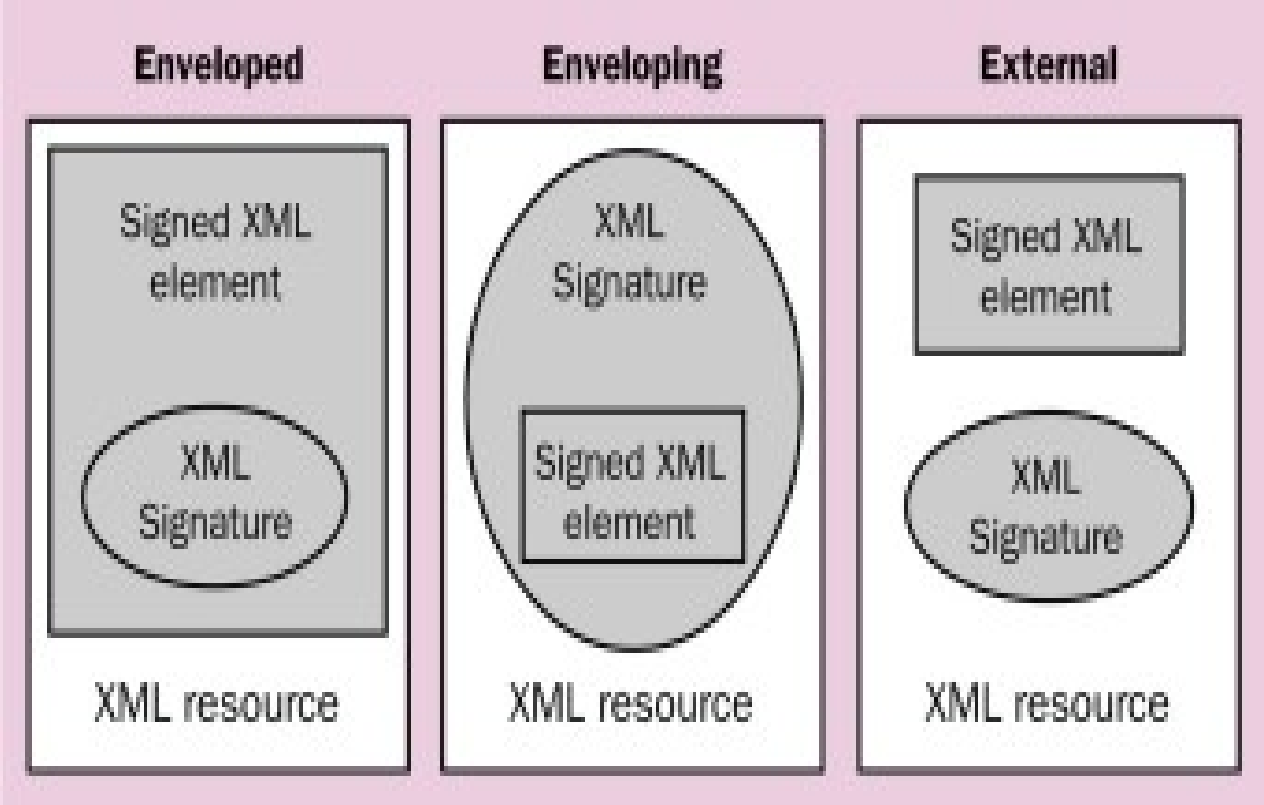
Tipos de Firma. Firma XML

- XML Signature

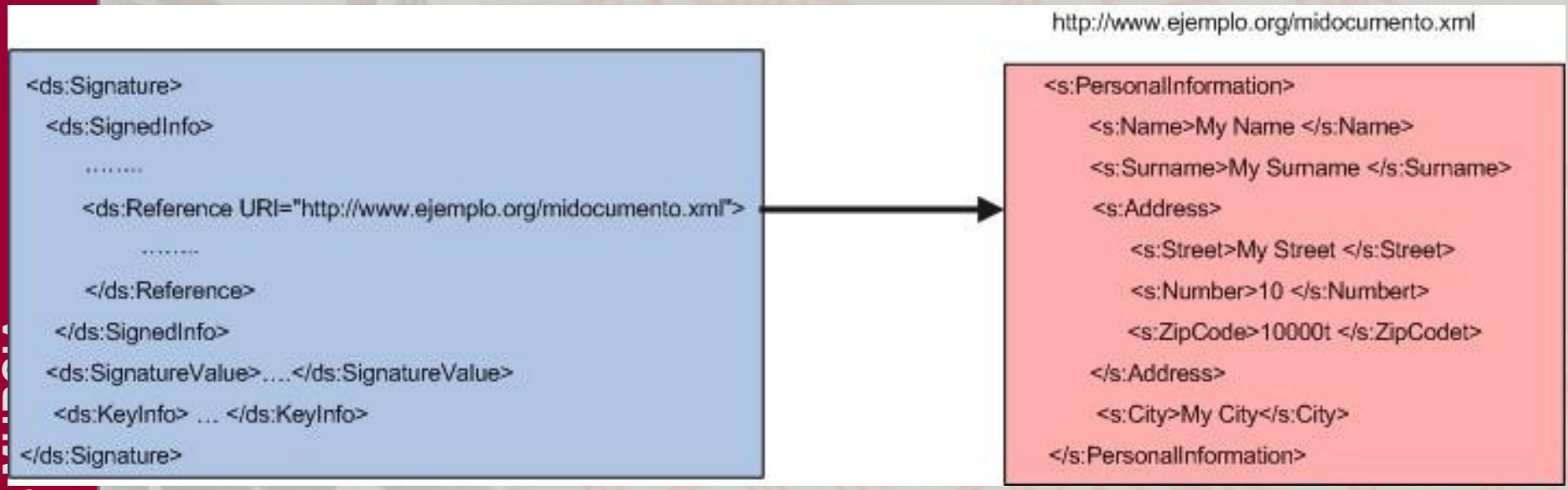


Tipos de Firma. Firma XML

- Tipos de Firma XML



XML detached



XML detached

```
<Signature Id="˝MiFirmaDetached˝" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                    c14n-20010315"></CanonicalizationMethod>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                sha1"></SignatureMethod>
        <Referente URI="http://www.ejemplo.org/midocumento.html">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-
                        xml-c14n-20010315#WithComments"></Transform>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                <DigestValue>vo7Aa…fwJ8=</DigestValue>
        </Reference>
    </SignedInfo>
    <SignatureValue>BwUwA…2OLtBQ=</SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509Certificate>MIIB9jCC…wZgyg=</X509Certificate>
        </X509Data>
        <KeyValue>
            <RSAKeyValue>
                <Modulus>Pkkl…TP7U=</Modulus>
                <Exponent>AQAB</Exponent>
            </RSAKeyValue>
        </KeyValue>
    </KeyInfo>
</Signature>
```

XML enveloping

```
<ds:Signature>
  <ds:SignedInfo>
      ……..
     <ds:Reference URI="#midocumento.xml">
          ……..
      </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>….</ds:SignatureValue>
  <ds:KeyInfo> … </ds:KeyInfo>
  <ds:Object Id="midocumento">
      <s:PersonalInformation>
          <s:Name>My Name </s:Name>
          <s:Surname>My Surname </s:Surname>
                  ……..
       </s:PersonalInformation>
  </ds:Object>
</ds:Signature>
```

XML enveloping

```
<Signature Id="“MiFirmaEnveloping”" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                        c14n-20010315"></CanonicalizationMethod>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                    sha1"></SignatureMethod>
        <Referente URI="#MiDocumento">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-
                        xml-c14n-20010315#WithComments"></Transform>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                <DigestValue>vo7Aa…fwJ8=</DigestValue>
        </Reference>
    </SignedInfo>
    <SignatureValue>BwUwA…2OLtBQ=</SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509Certificate>MIIB9jCC…wZgyg=</X509Certificate>
        </X509Data>
        <KeyValue>
            <RSAKeyValue>
                <Modulus>Pkkl…TP7U=</Modulus>
                <Exponent>AQAB</Exponent>
            </RSAKeyValue>
        </KeyValue>
    </KeyInfo>
    <Object Id=" MiDocumento">
        <m:mydocument xmlns:m="urn:myschema">
            <m:name>name</m:name>
            <m:lastname>lastname</m:lastname>
        </m:mydocument>
    </Object>
</Signature>
```

XML enveloped

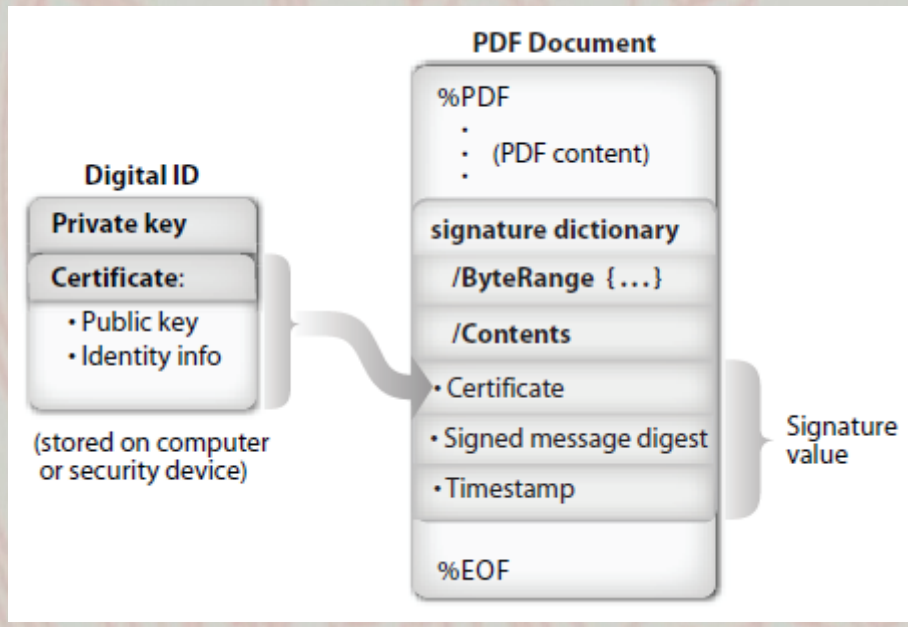
```
<s:PersonalInformation Id="midocumento">
    <s:Name>My Name </s:Name>
    <s:Surname>My Surname </s:Surname>
        <ds:Signature>
          <ds:SignedInfo>
              ……..
            <ds:Reference URI="#midocumento">
                <ds:Transforms>
                    <ds:Transform
                        Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                    </ds:Transform>
                </ds:Transforms>
                  ……..
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>….</ds:SignatureValue>
          <ds:KeyInfo> … </ds:KeyInfo>
        </ds:Signature>
    <s:Address>
        <s:Street>My Street </s:Street>
        <s:Number>10 </s:Numbert>
        <s:ZipCode>10000t </s:ZipCodet>
    </s:Address>
    <s:City>My City</s:City>
</s:PersonalInformation>
```

XML enveloped

```
<m:mydocument Id="“MiDocumento”" xmlns:m="urn:myschema">
    <m:name>name</m:name>
    <m:lastname>lastname</m:lastname>
    <Signature Id="“MiFirmaEnveloping”" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                        c14n-20010315"></CanonicalizationMethod>
            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                        sha1"></SignatureMethod>
            <Referente URI="#MiDocumento">
                        <Transforms>
                            <Transform Algorithm="http://www.w3.org/2000/09/
                            xmldsig#enveloped-signature"></Transform>
                            <Transform Algorithm="http://www.w3.org/TR/2001/REC-
                            xml-c14n-20010315#WithComments"></Transform>
                        </Transforms>
                        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                        <DigestValue>vo7Aa…fwJ8=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>BwUwA…2OLtBQ=</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIB9j…wZgyg=</X509Certificate>
            </X509Data>
            <KeyValue>
                <RSAKeyValue>
                    <Modulus>Pkkl…TP7U=</Modulus>
                    <Exponent>AQAB</Exponent>
                </RSAKeyValue>
            </KeyValue>
        </KeyInfo>
    </Signature>
</m:mydocument>
```

Tipos de firma. Firma PDF

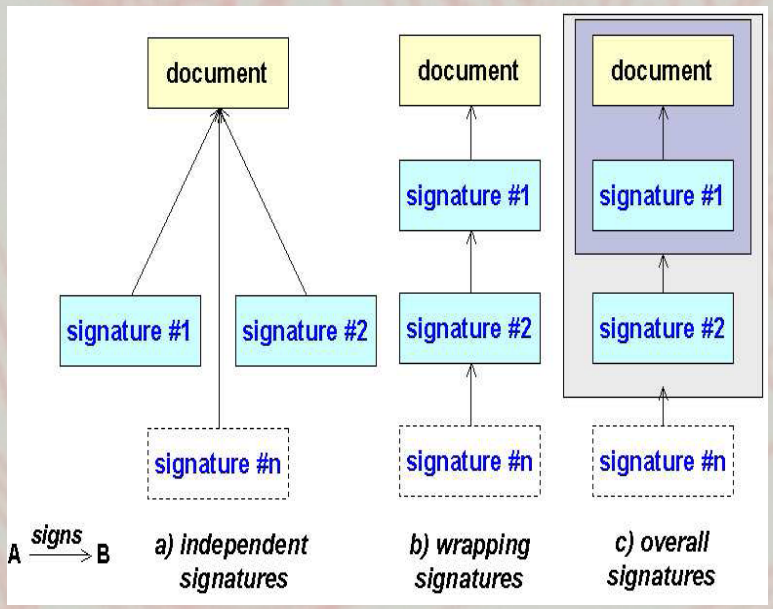
- Utiliza una estructura CMS Enveloping modificada en un objeto interno.
  - En 'ContentInfo' sólo se introduce el hash del documento PDF.
- Dos clasificaciones de firma.
  - Firma de certificación → sólo 1 por documento.
  - Firma de aprobación → múltiples firmantes.
- Puede incluir timestamp, pero se agrega en el instante previo a la firma.
- No cumple los estándares AdES.



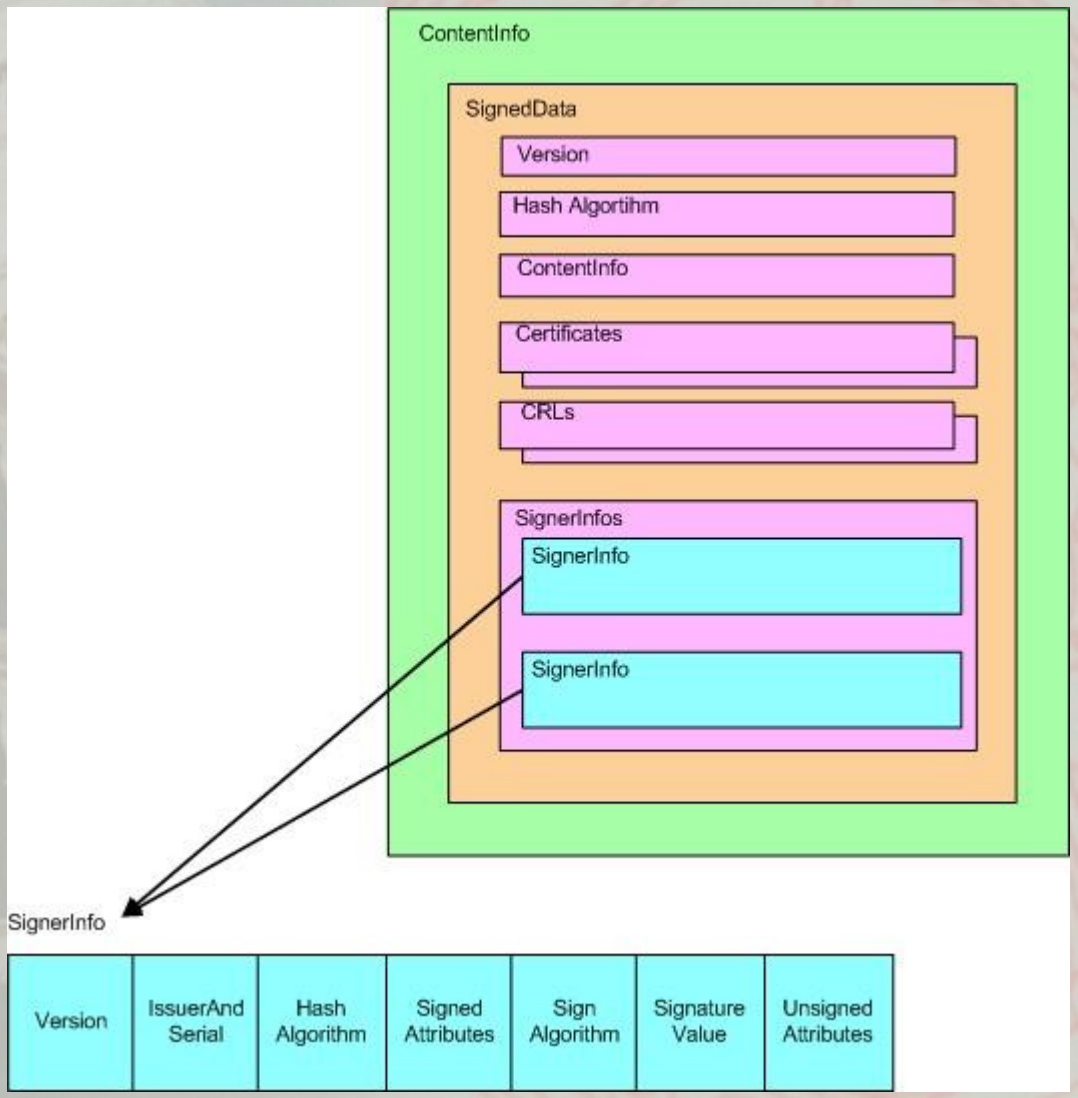
Icon	Status	Certificate and document status
	Certified & Valid	**Certificate status**: Valid. The signer used the certification process, and the signature was the first signature in the document. For details, see "Signing With a Certification Signature" on page 74. and **Document integrity status**: The document has not changed since it was signed or has only changed in ways specifically permitted by the certifier.
	Valid	**Certificate status**: Valid. and **Document integrity status**: The document has not changed since it was signed or only contains changes allowed by a previous signer, if any.
	Valid: Changed view	**Certificate status**: Valid. This icon may appear in a certified document, but it only appears on approval document signatures and not certification signatures. and **Document integrity status**: The document has changed since it was signed. The current view of the document is not the same as that which was signed. View the signed version to see what was signed. For details, see "Viewing and Comparing Changes and Versions" on page 105
	Unknown	**Certificate status**: Unknown: The certificate has not been trusted (and is not untrusted), the revocation check could not complete, a chain could not be built to trust anchor, and so on. and **Document integrity status**: The document has changed since it was signed. The document the user is viewing is not the signed version.
	Unknown	**Certificate status**: Unknown: The certificate or any certificate in the chain up to the issuing root certificate has not been trusted (trust must exist for one certificate in the chain), the revocation check could not complete, a chain could not be built to trust anchor, the certificate has been trusted for signing but not for certifying. and **Document integrity status**: The document has not changed since it was signed.
	Unknown	**Certificate status**: Unverified. The certificate validation check has not executed or could not complete due to bad revocation information, and non-responding server, no network connection, etc. and **Document integrity status**: Unverified. The document integrity check has not executed or could not complete.
	Invalid	**Certificate status**: The signer's certificate was invalid. or **Document integrity status**: Illegal changes have been made to the document.

Tipos de Firma

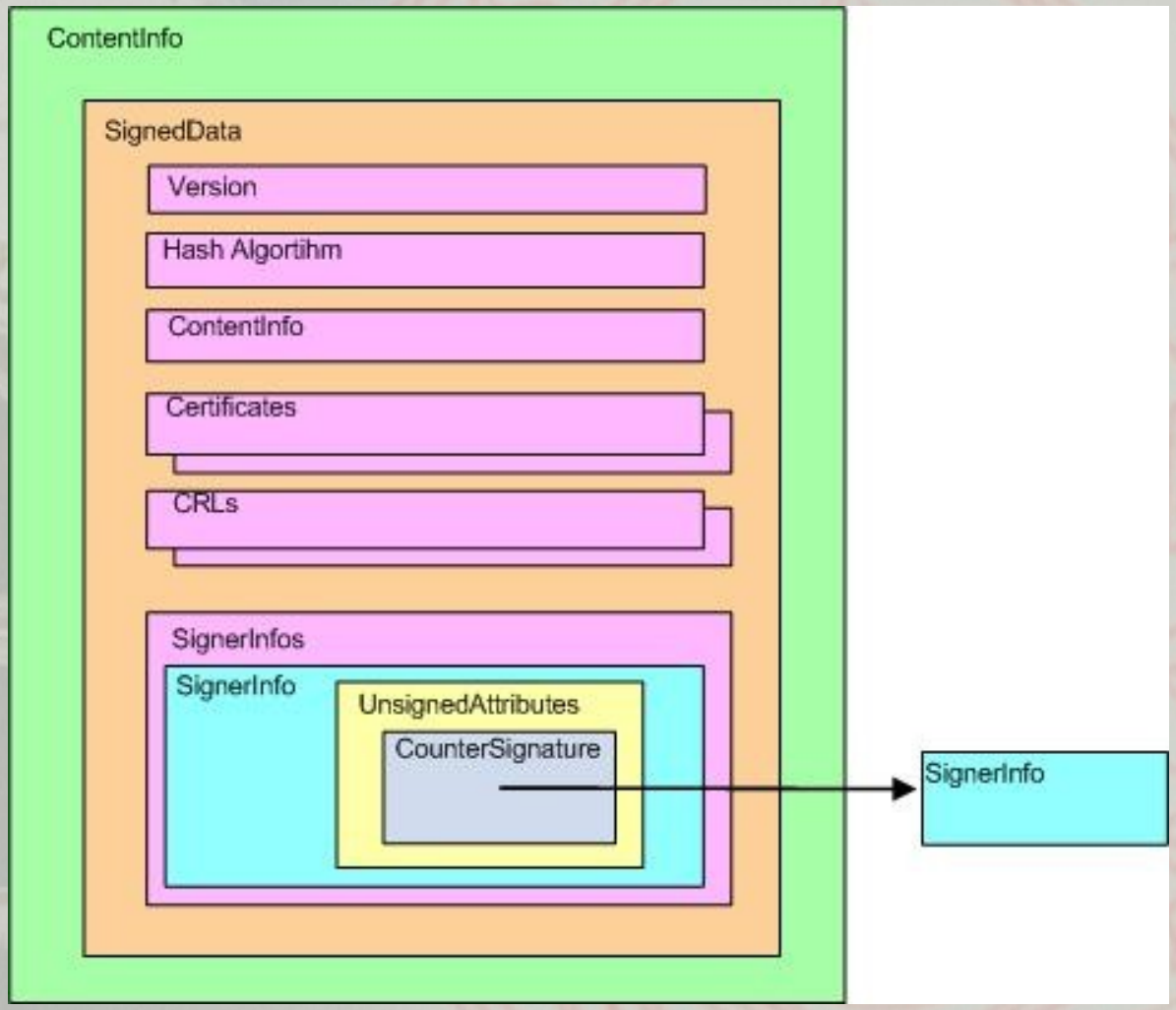
- Según el número de firmantes:
  - Firma única
  - Firma múltiple
    - Cofirma con firmas independientes
    - Cofirma en serie, contatenadas o envolventes
    - Cofirma total



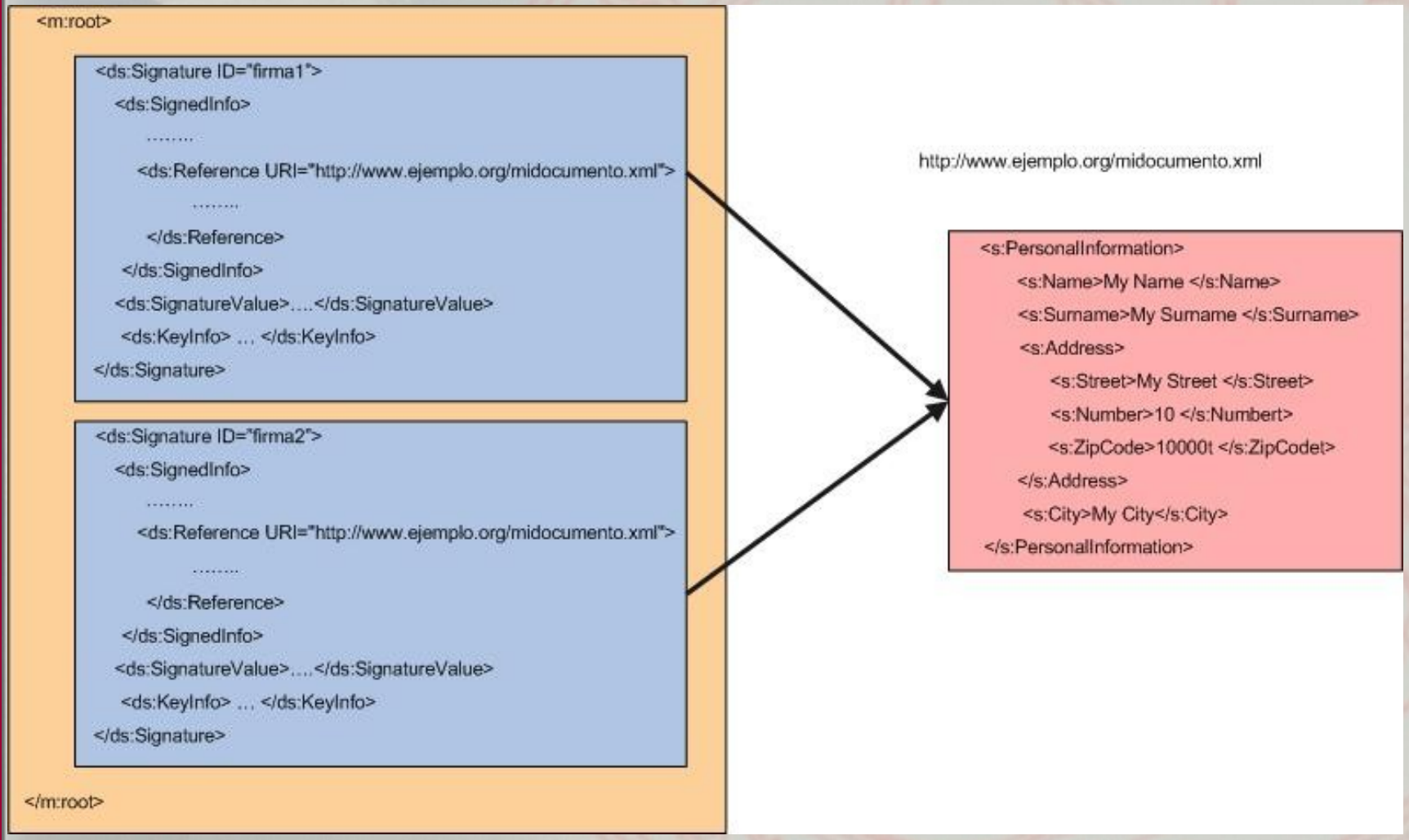
Firmas independientes CMS



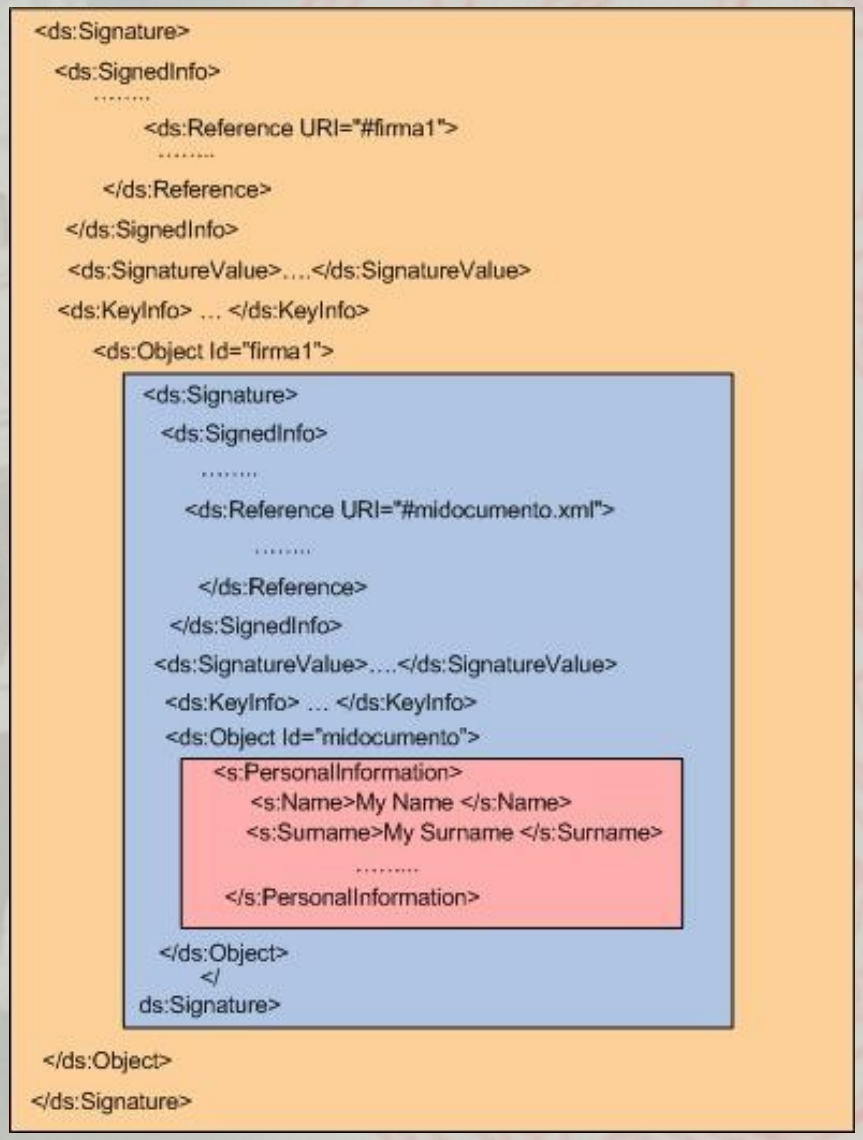
Firmas envueltas CMS



Firmas independientes XML



Firmas envueltas XML



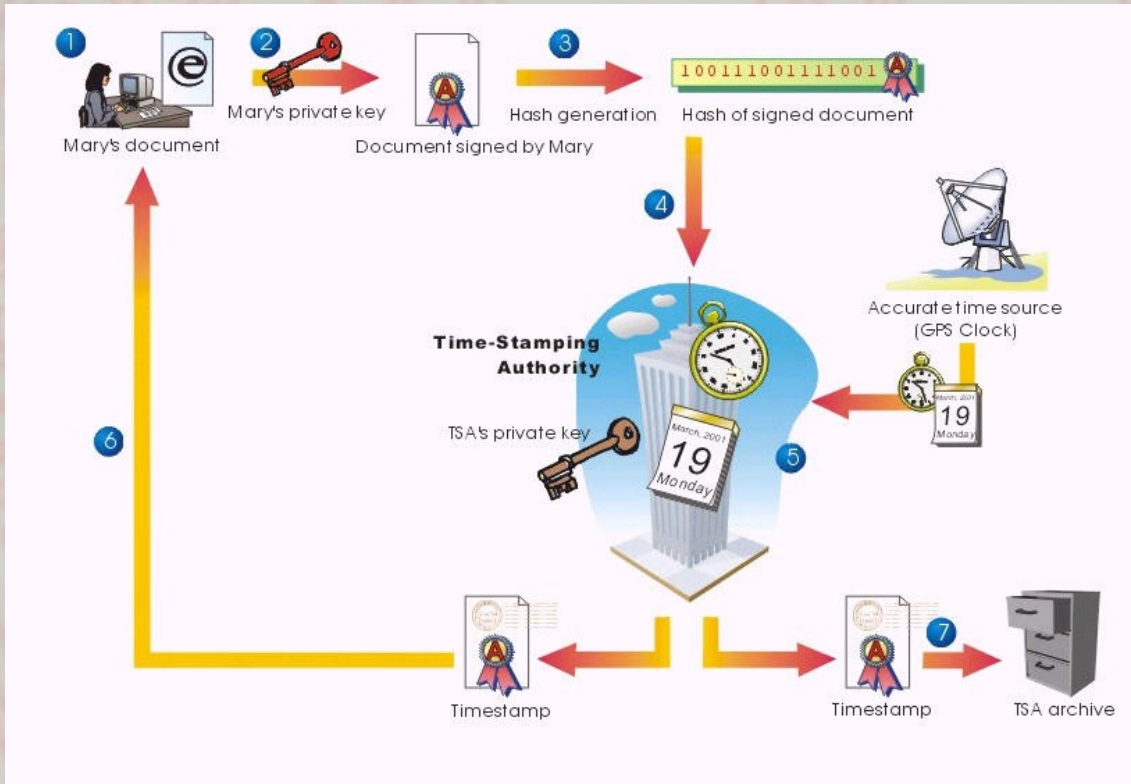
Sellado de tiempo

RFC 3161
XML Timestamp Token
Autoridades de sellado

Sellado de tiempo

- Permite vincular un documento o transacción electrónica a una fecha y hora fiables.

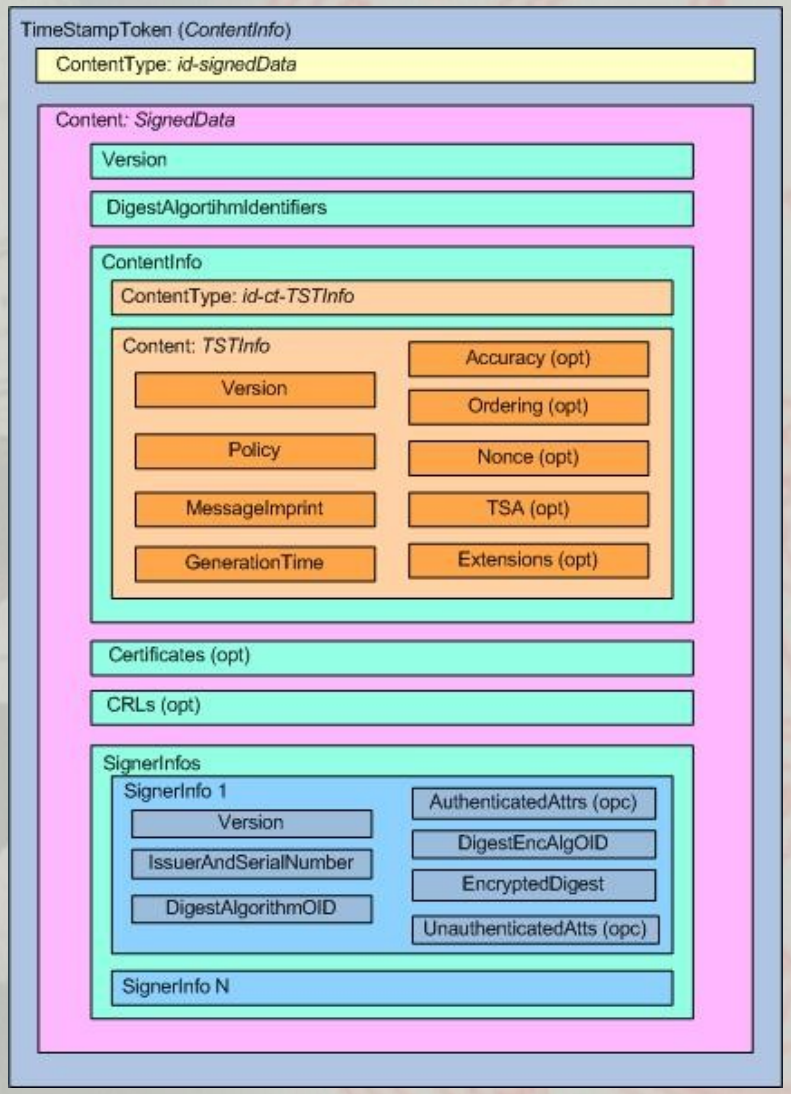
- El sello lo genera una TSA (Time Stamping Authority) utilizando una fuente de tiempo fiable.



RFC 3161

- Describe el formato de solicitud/respuesta de un timestamp token a una TSA, así como la estructura del mismo codificada en DER.
- *TSTInfo:*
  - *version:* versión del timestamp token.
  - *policy*: indica la política bajo la que se ha producido la respuesta.
  - *messageImprint:* debe tener el mismo valor que en la solicitud.
  - *serialNumber:* entero único asignado por la TSA a cada token.
  - *genTime:* fecha en la que la TSA creó el timestamp token.
  - *accuracy* (opcional): precisión en la fecha de producción del timestamp token.
  - *ordering* (opcional): indica si cada timestamp token producido por la misma TSA puede ordenarse en base a la fecha de generación.
  - *nonce* (opcional): este campo debe aparecer si se incluyó en la solicitud y debe tener el mismo valor que el indicado en la misma.
  - *tsa* (opcional): uno de los “subject names” incluidos en el certificado utilizado para verificar el token.
  - *extensions* (opcional): para añadir información adicional en el futuro.

RFC 3161

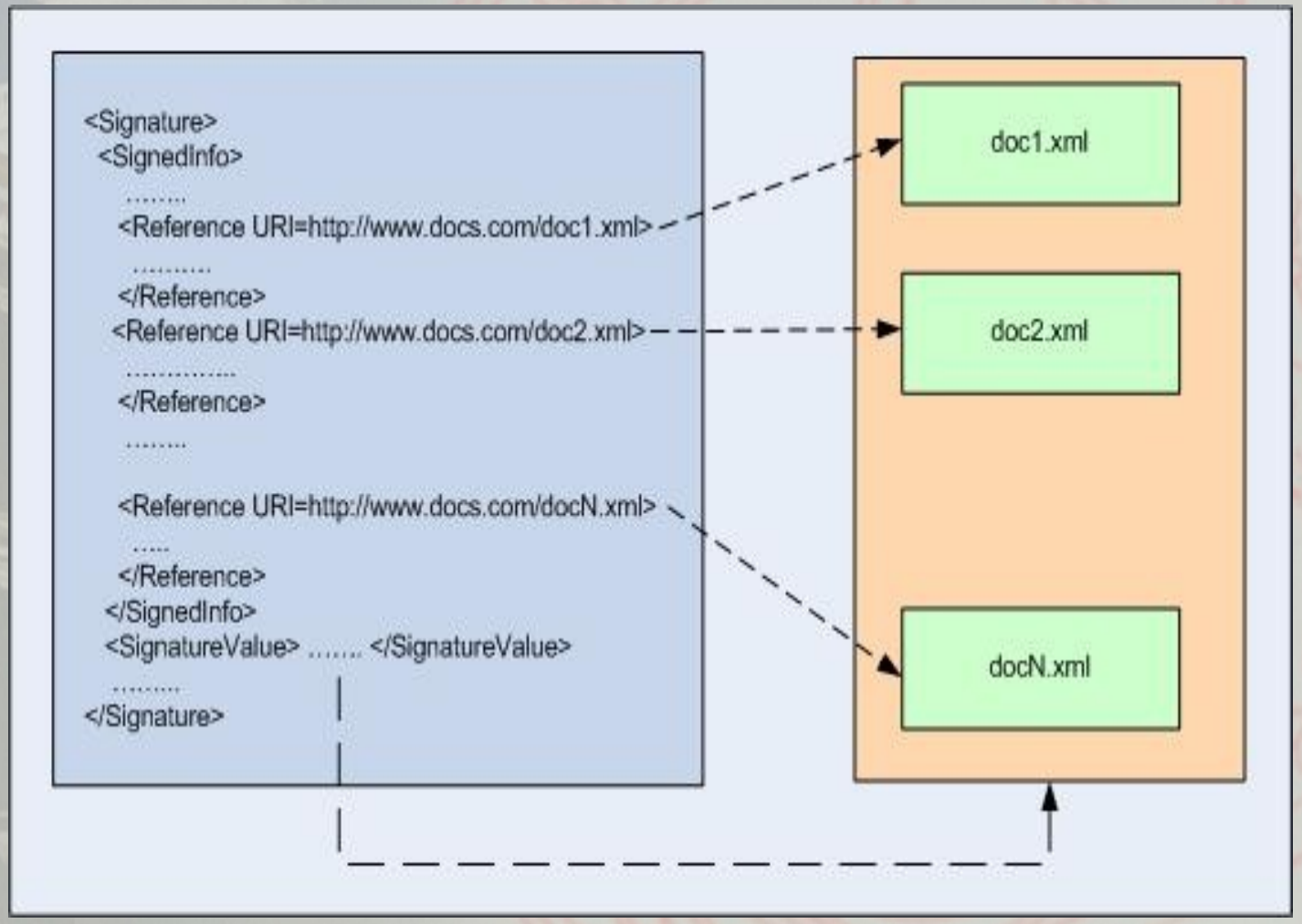

TimeStampToken (ContentInfo)
ContentType: id-signedData
Content: SignedData
Version
DigestAlgortihmIdentifiers
ContentInfo
ContentType: id-ct-TSTInfo
Content: TSTInfo
Version
Policy
MessageImprint
GenerationTime
Accuracy (opt)
Ordering (opt)
Nonce (opt)
TSA (opt)
Extensions (opt)
Certificates (opt)
CRLs (opt)
SignerInfos
SignerInfo 1
Version
IssuerAndSerialNumber
DigestAlgorithmOID
AuthenticatedAttrs (opc)
DigestEncAlgOID
EncryptedDigest
UnauthenticatedAtts (opc)
SignerInfo N

XML TimestampToken

- Definido por OASIS en la especificación OASIS DSS (Digital Signature Service).
- Su estructura es similar a la del RFC 3161, pero codificada en XML.
- Se integra en OASIS DSS, y en concreto en el perfil 'XML Timestamping Profile for DSS', que define el formato de solicitud/respuesta de tokens.
- Ventaja frente a RFC 3161 → integrado en un servicio permite "sellar" varios documentos a la vez.

```
<xs:element name="TstInfo">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="SerialNumber" type="xs:integer"/>
            <xs:element name="CreationTime" type="xs:dateTime"/>
            <xs:element name="Policy" type="xs:anyURI" minOccurs="0"/>
            <xs:element name="ErrorBound" type="xs:duration"
                        minOccurs="0"/>
            <xs:element name="Ordered" type="xs:boolean"
                        default="false" minOccurs="0"/>
            <xs:element name="TSA" type="saml:NameIdentifierType"
                        minOccurs="0"/>
        <xs:sequence>
    </xs:complexType>
</xs:element>
```

XML Timestamp Token



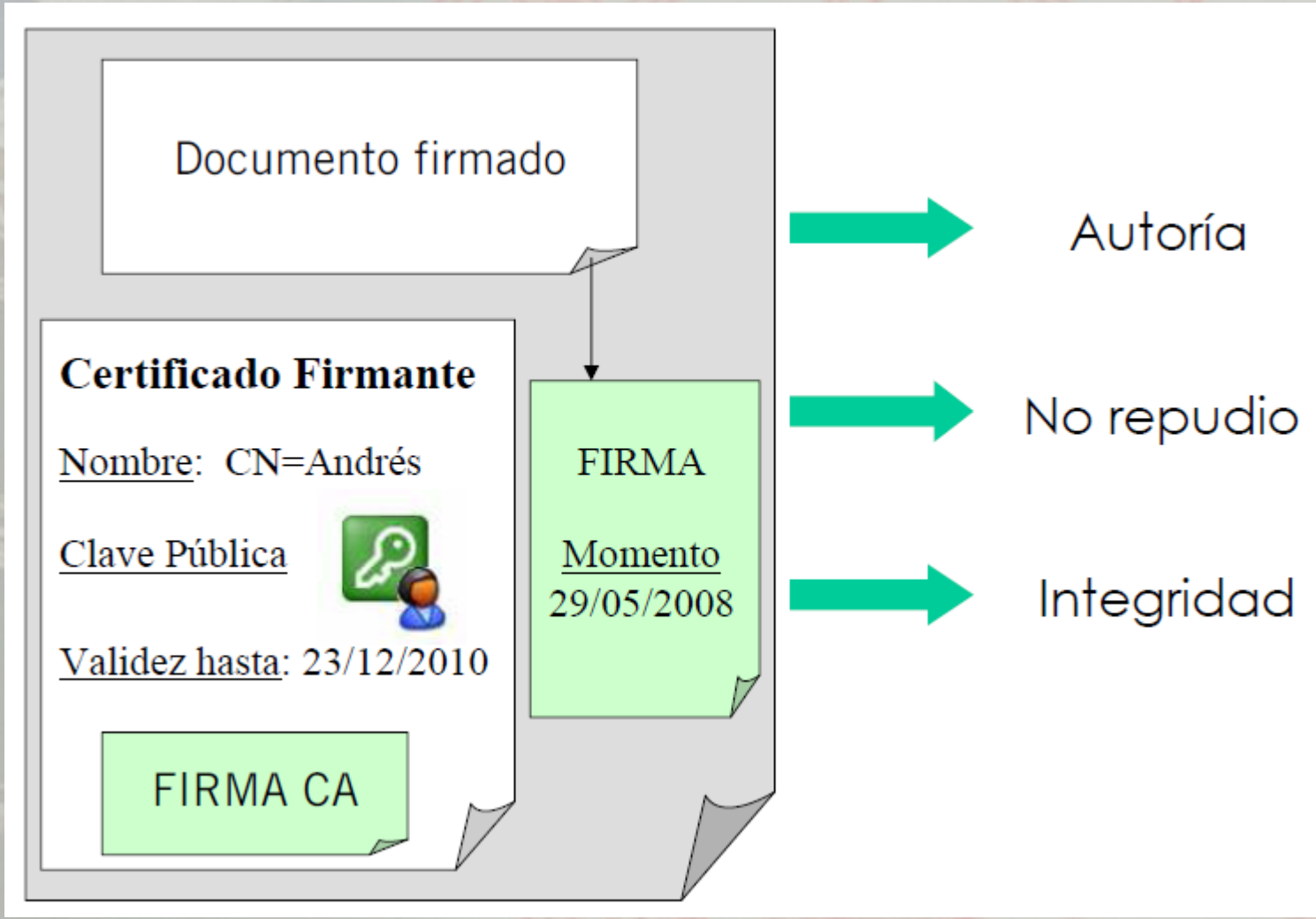
TSA

- Requisitos descritos en ETSI TS 102 023.
- Política de generación y gestión de los tokens de tiempo.
  - Módulo criptográfico para generar los tokens.
    - FIPS PUB 140-1
    - CEN Workshop Agreement 14167-2
  - Sincronización horaria UTC (relojes atómicos).
  - Procedimientos de seguridad definidos para el personal y las instalaciones físicas.
  - Verificación de los sellos a largo plazo.

Formatos AdES

Introducción
XAdES
Políticas de firma

Formatos AdES



Formatos AdES

- Problemas en el tiempo…
  - Caducidad de los certificados
  - Debilidad de los algoritmos criptográficos
  - Pérdida de información de revocación
  - Pérdida de certificados implicados
  - Incertidumbre sobre la fecha de existencia del documento
- Posibles soluciones…
  - Firmas periódicas (con nuevos certificados)
  - Firmas periódicas (más robustas)
  - Incluir información de revocación
  - Incluir todos los certificados implicados
  - Guardar información “temporal”

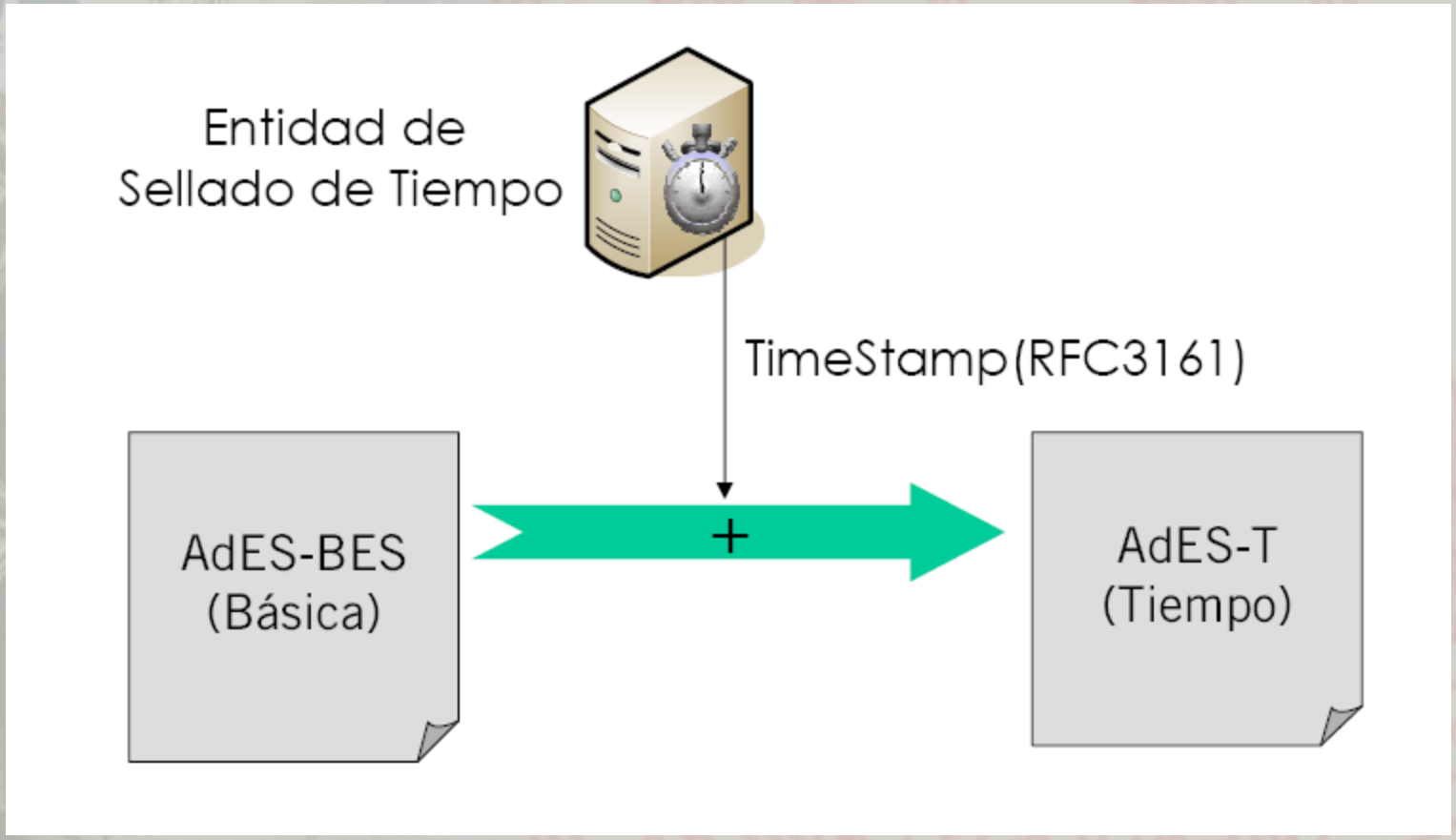
Formatos AdES

- **ETSI** define formatos de firma electrónica avanzada → AdES
- **Preservación de las firmas electrónicas**
  - Caducidad o revocación del certificado de firma → formato de firma fechada (AdES-T)
  - Desaparición o ausencia del prestador → formato de firma avanzado o extendido (AdES-C, X, XL)
    - Archivado de las evidencias de validación
      - Certificados
      - Sellos de tiempo
      - Respuestas de validación
  - Compromiso de los algoritmos de hash o firma (debilidad tecnológica) → formato archivado (AdES-A)
    - Hash o resumen digital proporciona integridad
    - Firma digital proporciona autenticidad y no repudio
    - Re-sellado de los documentos cada ciertos periodos de tiempo
      - Archivado de estos nuevos sellos de tiempo

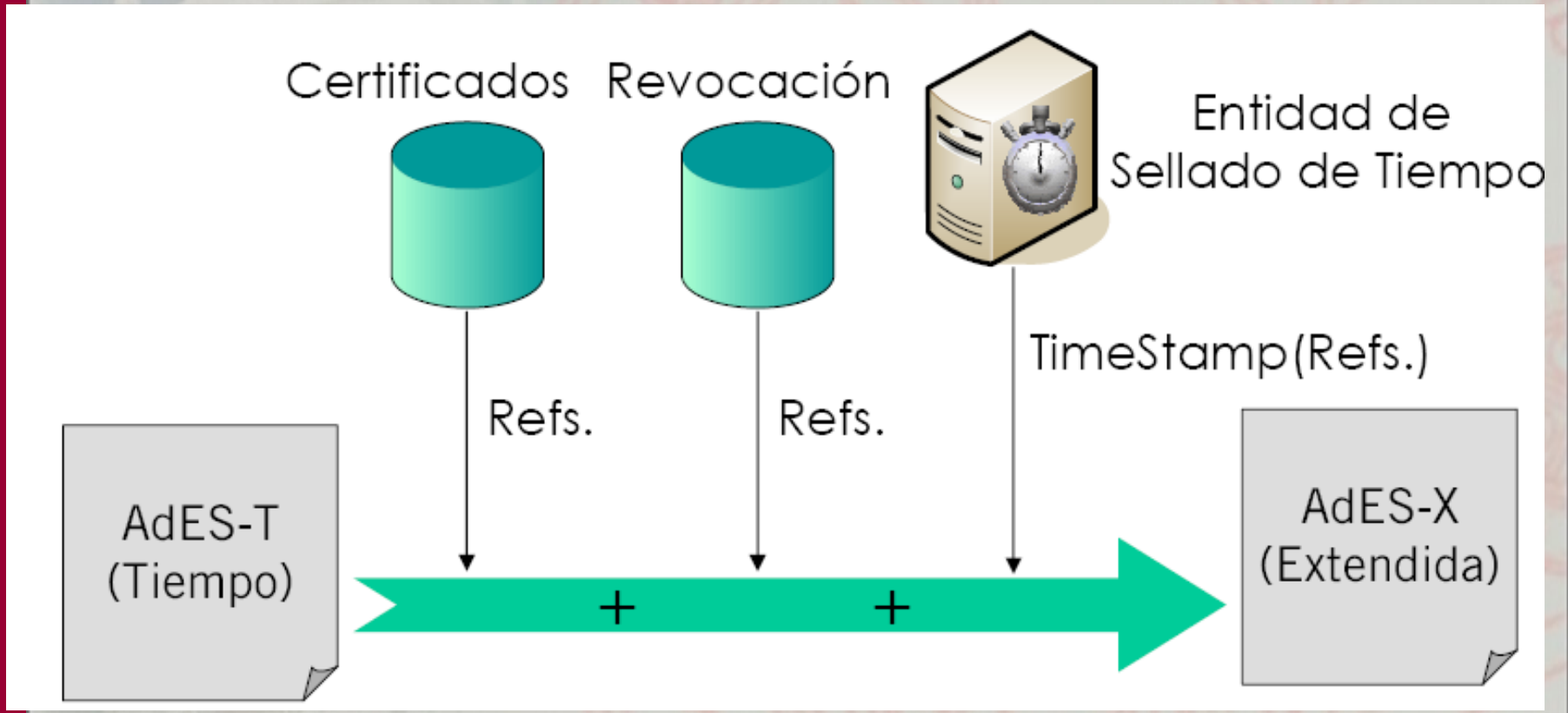
Formatos de Firma. XAdES

- XAdES
  - ETSI TS 101 903. Actualmente en la versión 1.3.2.
  - Conjunto de extensiones a XML-Dsig
    - Adecuadas para firma electrónica avanzada en el sentido marcado por la directiva 1999/93/EC de la Unión Europea.
  - Marco de interoperabilidad adoptado por el MAP y el resto de países miembros.
  - Diferentes perfiles en función del nivel de protección.
    - BES – EPES – T – C – X – XL – A

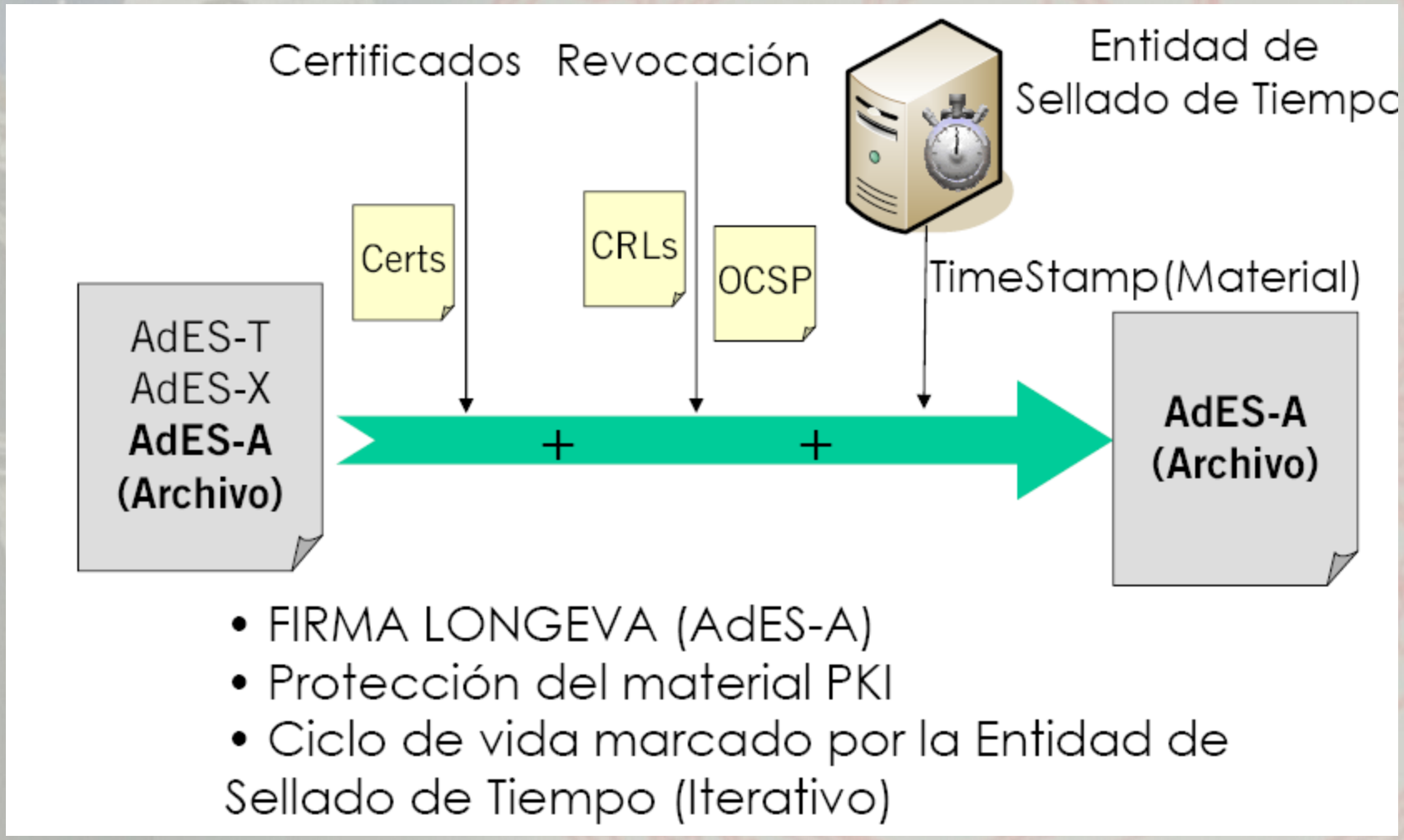
XAdES


Entidad de
Sellado de Tiempo
TimeStamp(RFC3161)
AdES-BES
(Básica)
+
AdES-T
(Tiempo)

XAdES


Certificados
Revocación
Entidad de Sellado de Tiempo
TimeStamp(Refs.)
Refs.
Refs.
AdES-T (Tiempo)
+
+
AdES-X (Extendida)

XAdES



- FIRMA LONGEVA (AdES-A)
- Protección del material PKI
- Ciclo de vida marcado por la Entidad de Sellado de Tiempo (Iterativo)

Políticas de firma

- Una política de firma es un conjunto de reglas concretas acerca de…
  - Cómo crear una firma
  - Cómo validar una firma
- Fomentan la interoperabilidad entre entidades y eliminan las inconsistencias.

Bibliografía

- Libro electrónico “Seguridad Informática”, Jorge Ramió Aguirre. 2007.
  - http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- “Criptografía y Seguridad en Computadores”. M. J. Lucena López
  - http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto
- “Curso básico de Criptografía para Principiantes”
  - http://www.wikilearning.com/curso_gratis/curso_de_criptografia_basica_para_principiantes/4306
- “Firma Electrónica”. Sociedad de la Información. Ministerio de Industria, Turismo y Comercio.
  - http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/
- “Firma Electrónica en Europa”. Página no oficial.
  - http://www.firma-electronica.eu/
- “An Introduction to Cryptography”, Network Associates.
  - http://www.pgpi.org/doc/guide/6.5/en/intro/
- “An Introduction to Cryptography and Digital Signatures”, Ian Curry
  - http://www.entrust.com/resources/pdf/cryptointro.pdf
- “Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats”. ETSI TS 101 733
  - http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010501p.pdf
- RFC 3852. Cyptrographic Message Syntax.
  - http://www.ietf.org/rfc/rfc3852.txt
- “XML Signature”. W3C.
  - http://www.w3.org/TR/xmldsig-core/
- RFC 3161. Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).
  - http://www.ietf.org/rfc/rfc3161.txt
- “OASIS Signature Services (DSS)”
  - http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html
- “Guía Breve Seguridad”. W3C
  - http://www.w3c.es/divulgacion/guiasbreves/Seguridad
- “Secure Electronic Commerce. Building the Infrastructure for Digital Signatures and Encryption”, Second Edition. W. Ford, M. Baum. Prentice Hall.
- “Seguridad y Comercio en el Web”, S. Garfinkel y G. Spafford. McGraw-Hill.
- “Understanding PKI: Concepts, Standards, and Deployment Considerations”, Second Edition. C. Adams, S. Lloyd. Addison Wesley.
- “PKI. Implementing and Managing E-Security”, A. Nash, W. Duane, C. Joseph, D. Brink. McGraw-Hill.

PREGUNTAS…