



**Agència Catalana
de Certificació**

Guia de sintaxi i formats de signatura
electrònica - Part 2: Signatura XML

Informació general

Control documental

Projecte:	N/A
Entitat de destinació:	Públic
Títol:	Guia de sintaxi i formats de signatura electrònica - Part 2: Signatura XML
Codi de referència:	ACC_Guia_002-2
Versió:	1.0
Data:	
Fitxer:	Guia formats XML v1r0.doc
Eina/es d'edició:	Word 2002
Autor/s:	Àrea d'assessorament i recerca de CATCert, amb la col·laboració de l'Institut de Dret i Tecnologia de la Universitat Autònoma de Barcelona
Resum:	

Estat formal

Preparat per:	Revisat per:	Aprovat per:
Nom: AiR/IDT	Nom: Director AiR	Nom: Director General

Control de versions

Versió	Parts que canvien	Descripció del canvi	Data
1.0	Tot	Creació del document	

Índex

1. Introducció	7
1.1 Objecte i abast	7
1.2 Contingut	7
1.3 Referències	7
2. La sintaxi XML de signatura electrònica	9
2.1 Introducció	9
2.2 La creació de la signatura XML	11
2.2.1 Generació de les referències.....	11
2.2.2 Generació de la signatura electrònica.....	11
2.3 La verificació de la signatura XML	12
2.3.1 Validació de les referències.....	12
2.3.2 Validació de la signatura electrònica	12
3. L'estructura de la signatura electrònica XML	13
3.1 La informació signada	13
3.1.1 El mètode de canonicalització.....	14
3.1.2 El mètode de signatura	16
3.1.3 Les referències als objectes signats	17
3.1.3.1 Els atributs de les referències.....	18
3.1.3.2 Les transformacions dels objectes a signar.....	19
3.1.3.3 El mètode de resum criptogràfic	20
3.1.3.4 El valor del resum criptogràfic	21
3.2 El valor de la signatura	21
3.3 La informació de les claus de signatura	21
3.3.1 El mètode de recuperació d'informació de claus	23
3.3.2 El certificat X.509	24
3.4 L'objecte signat	25
4. Els elements opcionals de la signatura electrònica XML	27
4.1 El manifest	27
4.2 Les propietats de la signatura	28
5. El elements addicionals de la signatura electrònica XML derivats de la Directiva europea (XAdES)	30
5.1 Les propietats de la signatura	30
5.1.1 Les propietats signades.....	32
5.1.1.1 Les propietats signades de la signatura.....	33

5.1.1.2	Les propietats signades de l'objecte de dades.....	34
5.1.2	Les propietats no signades.....	35
5.1.2.1	Les propietats no signades de la signatura.....	36
5.1.2.2	Les propietats no signades de l'objecte de dades.....	37
5.2	La data i hora de la signatura electrònica.....	38
5.3	La contrasignatura.....	38
5.3.1	Contrasignatures mitjançant referències.....	38
5.3.2	Contrasignatures mitjançant l'element contrasignatura.....	39
5.4	El certificat emprat per signar.....	39
5.5	L'identificador de la política de signatura electrònica.....	40
5.6	El format de l'objecte de dades signat.....	44
5.7	La indicació del tipus de compromís del signatari.....	45
5.8	El lloc de producció de la signatura.....	46
5.9	El rol del signatari.....	47
5.10	El segell de data i hora sobre tots els objectes de dades signats.....	48
5.11	El segell de data i hora sobre un objecte de dades individual signat.....	49
5.12	El segell de data i hora sobre la signatura.....	49
5.13	Les referències completes dels certificats.....	50
5.14	Les referències completes de la informació de revocació de certificats.....	50
5.15	Les referències completes dels certificats d'atributs.....	54
5.16	Les referències completes de la informació de revocació d'atributs.....	54
5.17	El segell de data i hora sobre la signatura completa.....	55
5.18	El segell de data i hora sobre les referències de certificats i revocacions.....	55
5.19	Els valors dels certificats.....	56
5.20	Els valors dels certificats d'autoritat d'atributs.....	57
5.21	Els valors de les revocacions.....	57
5.22	Els valors de les revocacions d'atributs.....	58
5.23	El segell de data i hora d'arxiu.....	59
6.	<i>Els formats de la signatura electrònica XML.....</i>	60
6.1	La signatura electrònica bàsica (XAdES-BES).....	60
6.2	La signatura electrònica amb política explícita (XAdES-EPES).....	61
6.3	La signatura electrònica amb segell de data i hora (XAdES-T).....	62

6.4	La signatura electrònica amb referències completes de dades de validació (XAdES-C)	63
6.5	La signatura electrònica amb referències completes de dades de validació i segellada (XAdES-X Type 1)	65
6.6	La signatura electrònica amb referències completes i segellades de dades de validació (XAdES-X Type 2)	66
6.7	La signatura electrònica amb dades completes de validació i segellada (XAdES-X Long Type 1)	68
6.8	La signatura electrònica amb dades completes i segellades de validació (XAdES-X Long Type 2).....	70
6.9	La signatura electrònica d'arxiu (XAdES-A)	72
	<i>Annex. La sintaxi de la signatura electrònica en XML.....</i>	<i>74</i>

1. Introducció

1.1 Objecte i abast

Aquesta guia té per objecte la presentació de la sintaxi XML de la signatura electrònica, així com els seus formats i propietats per a la producció de signatures electròniques amb valor legal.

1.2 Contingut

Aquesta Guia té els següents continguts:

1. Introducció (aquest secció).
2. La sintaxi XML de signatura electrònica.
3. L'estructura de la signatura electrònica XML.
4. Els elements opcionals de la signatura electrònica XML.
5. El elements addicionals de la signatura electrònica XML derivats de la Directiva europea (XAdES).
6. Els formats de la signatura electrònica XML.
7. Annex.

1.3 Referències

- Canonical XML Version 1.0, W3C Recommendation 15 March 2001.
- Directiva 99/93/CE, del Parlament Europeu i del Consell de 13 de desembre de 1999, per la que s'estableix un marc comunitari per a la signatura electrònica.
- ETSI TS 101903 v1.3.2, XML Advanced Electronic Signatures (XAdES), 2006-03.
- Exclusive XML Canonicalization Version 1.0, W3C Recommendation 18 July 2002.
- ITU-T Recommendation X.208, Specification of Abstract Syntax Notation One, 1988.
- ITU-T Recommendation X.209, Specification of Basic Encoding Rules for Abstract Syntax Notation One, 1988.
- ITU-T Recommendation X.509, The Directory – Authentication Framework, 1988.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002.



Agència Catalana
de Certificació

Guia de sintaxi i formats de signatura electrònica - Part 2: Signatura XML

-
- XML-Signature XPath Filter 2.0, W3C Recommendation 08 November 2002.

2. La sintaxi XML de signatura electrònica

2.1 Introducció

La sintaxi de signatura en XML (en general anomenada Signatura XML) és un mètode per associar l'ús d'una clau de signatura amb les dades signades a les que es refereix. En aquest sentit, cal dir que la signatura XML és molt versàtil, i que permet diversos tipus de claus, incloent-hi claus certificades (X.509v3) o claus sense certificar.

Un aspecte fonamental de la signatura XML és l'habilitat per signar únicament parts de l'arbre del document XML enloc del document sencer. Aquesta capacitat és rellevant quan un únic document té una història llarga en que els seus components són produïts en dates diferents per persones també diverses, cadascuna de les quals signa només els elements que els hi són aplicables.

Aquesta flexibilitat també és molt important en situacions en que és important garantir la integritat de certs parts del document XML, permetent que la resta del document pugui ser modificat. Un exemple seria un formulari enviat per ser completat pel seu destinatari: si la signatura fos produïda sobre tot el document, l'addició de les informacions al formulari invalidaria el propi formulari.

La signatura XML permet signar el formulari amb exclusió dels camps del formulari a omplir, i permet que l'usuari signi només les dades que omple, sense afectar a la validesa de la signatura original.

La Signatura XML ha estat definida pel Consorci W3C mitjançant un conjunt d'especificacions tècniques:

- XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002.
- Canonical XML Version 1.0, W3C Recommendation 15 March 2001.
- Exclusive XML Canonicalization Version 1.0, W3C Recommendation 18 July 2002.
- XML-Signature XPath Filter 2.0, W3C Recommendation 08 November 2002.

La signatura XML es pot aplicar a qualsevol contingut digital (objecte de dades), incloent-hi XML, podent referir-se a un o més recursos. En aquest sentit, la signatura XML es relaciona amb les dades objecte de signatura mitjançant identificadors uniformes de recurs (URIs).

En aquest sentit, la signatura XML pot ser emprada per signar més d'un tipus de recurs. Per exemple, una única signatura pot cobrir dades codificades en text, com HTML, dades binàries, com JPEG o dades codificades en XML.

En funció de la seva relació amb les dades objecte de signatura, les signatures XML poden ser:

- Signatures embolcallades o que embolcallen dades sobre el mateix document XML.

Dins d'un mateix document XML, la signatura es relaciona amb objectes de dades locals (del propi document) mitjançant identificadors de recurs fragmentaris (interns al propi document), de forma que aquests objectes de dades locals poden ser inclosos dins d'una signatura (embolcallant) o incloure una signatura (embolcallada).

- Signatures independents.

Les signatures independents es produeixen sobre recursos externs al document XML o sobre objectes de dades locals externs a la signatura; és a dir, objectes que no contenen la signatura ni són continguts per aquesta, sinó que es troben al mateix nivell¹.

La signatura XML és aplicada al contingut signat mitjançant una indirecció: el contingut es resumeix, el resum es col·locat en un element XML juntament a altres informacions i aquest element es resumeix i signat criptogràficament.

Aquesta característica de la signatura XML permet la realització d'operacions molt complexes de signatura electrònica sobre els diferents objectes d'un document XML, o de documents externs.

Per exemple, es pot controlar exactament què entra a formar part de la signatura, fins i tot elegint o exclouent-hi parts del document o dels elements que el formen.

A continuació es mostra de forma senzilla l'element XML que conté la signatura:

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

¹ L'objecte a signar i la signatura són "objectes germans" als efectes de la jerarquia de continguts.

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

La signatura XML no especifica com s'associen les claus de signatura amb persones o entitats, ni aporta cap semàntica sobre el significat de les dades signades. En aquest sentit, les aplicacions que facin ús d'aquesta sintaxi, han d'especificar requisits addicionals relatius a les claus, els algorismes, el processament i la representació/visualització de la signatura.

En aquest sentit, cal ja esmentar l'especificació ETSI TS 101903, que especifica requisits i condicions addicionals en relació amb l'ús de la signatura electrònica XML per produir signatures amb valor legal d'acord amb la Directiva europea de signatura electrònica.

2.2 La creació de la signatura XML

Per crear la signatura XML cal generar, en primer lloc, els elements `Reference` – en relació amb els objectes a signar – i posteriorment, el valor de la signatura sobre l'element `SignedInfo`, com es detalla a continuació.

2.2.1 Generació de les referències

Per a cada objecte de dades que ha de ser signat, cal fer el següent:

1. Aplicar a l'objecte les transformacions apropiades d'acord amb l'aplicació.
2. Calcular el valor del resum sobre l'objecte de dades transformat.
3. Crear un element `Reference`, incloent-hi la identificació – opcional – de l'objecte de dades, qualsevol element – també opcional – de transformació, l'algorisme de resum i el valor corresponent.

2.2.2 Generació de la signatura electrònica

Per a la generació de la signatura electrònica cal fer el següent:

1. Crear l'element `SignedInfo` incloent-hi el mètode de signatura, el mètode de canonicalització i la referència o referències.
2. Canonicalitzar i després calcular el valor de la signatura sobre l'element `SignedInfo`, emprant l'algorisme identificat al mètode de signatura.
3. Construir l'element `Signature`, incloent-hi l'element `SignedInfo`, els objectes signats, la informació de claus i el valor de la signatura.

2.3 La verificació de la signatura XML

Per verificar la signatura XML cal comprovar la validesa dels elements `Reference` i posteriorment la validació criptogràfica de la signatura sobre l'element `SignedInfo`.

2.3.1 Validació de les referències

Per a la validació de les referències cal fer el següent:

1. Canonicalitzar l'element `SignedInfo` amb l'algorisme indicat.
2. Per a cada referència:
 - a. Obtenir l'objecte de dades. Per exemple, l'aplicació pot obtenir l'objecte a partir de la URI i aplicar-li una o més transformacions indicades a l'element `Reference`, o bé obtenir-lo d'un dipòsit local).
 - b. Resumir l'objecte de dades resultant emprant l'algorisme indicat.
 - c. Comparar el resum obtingut amb el valor de resum contingut a la referència inclosa a l'element `SignedInfo`. Si la comparació no és correcta, la validació falla.

2.3.2 Validació de la signatura electrònica

Per a la validació de la signatura electrònica cal fer el següent:

1. Obtenir la informació de claus a partir de l'element `KeyInfo` o d'un altre lloc, com un dipòsit local.

Generalment s'obté un certificat digital de signatura electrònica X.509v3.

2. Obtenir la forma canònica del mètode de signatura emprant l'algorisme indicat i emprar el resultat obtingut, juntament amb la informació de claus, per confirmar el valor de la signatura.

En el cas de l'algorisme RSA, s'emprarà la clau pública obtinguda del certificat per validar la signatura digital continguda al `SignatureValue`, emprant el resum calculat del `SignedInfo`. Si la comparació no és correcta, la validació falla.

3. L'estructura de la signatura electrònica XML

L'element `Signature`, basat en el tipus `SignatureType`, conté l'estructura de la signatura electrònica XML.

Aquest element té la següent definició d'esquema:

```
<element name="Signature" type="ds:SignatureType"/>

<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

L'element `Signature` conté els següents elements:

- La informació signada, que agrupa i representa les dades objectes de signatura.
- El valor de la signatura, corresponent a la informació signada.
- Opcionalment, la informació de les claus necessària per a la validació de la signatura.
- Opcionalment, un o més objectes signats².

3.1 La informació signada

L'element `SignedInfo`, basat en el tipus `SignedInfoType`, conté les dades que són signades.

Aquest element té la següent definició d'esquema:

```
<element name="SignedInfo" type="ds:SignedInfoType"/>
```

² Els objectes queden embolcallats dins de la signatura, en aquest cas.

```
<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

L'element `SignedInfo` conté els següents elements:

- El mètode de canonicalització de la informació signada.
- El mètode de signatura electrònica.
- Una o més referències³ amb els resums dels objectes signats.
- Opcionalment, un atribut per identificar la signatura de forma que pugui ser referida des d'altres signatures o altres objectes.

Aquest element no conté propietats explícites de la signatura o del resum com per exemple el moment en que es varen calcular o el número de sèrie d'un dispositiu criptogràfic, tot i que resulta possible incloure aquestes – i altres informacions que es considerin adients – emprant l'element `Propietats de la Signatura` (`SignatureProperties`), que es pot trobar dins de l'element `Objecte` (`Object`)

3.1.1 El mètode de canonicalització

L'element `CanonicalizationMethod`, basat en el tipus `CanonicalizationMethodType`, és un element obligatori que especifica l'algorisme de canonicalització aplicat a l'element `SignedInfo` abans de realitzar els càlculs criptogràfics (el resum i la signatura posterior).

Per "canonicalització" s'entén el procés de produir una representació física única d'un document XML, referida a l'estructura de les entitats que el componen, de l'ordenació dels seus atributs i de la codificació del conjunt de caràcters emprat.

Aquesta necessitat neix del fet que poden existir documents XML considerats lògicament equivalents tot i no disposar d'una mateixa representació física, per exemple perquè contenen els mateixos elements, però ordenats de forma diferent.

³ L'ús dels elements de tipus `Reference` mostra la indirecció en la generació de la signatura XML, ja que aquests elements contenen els resums criptogràfics dels objectes signats, amb les seves transformacions.

Aquests documents, interpretats per una aplicació XML, es poden considerar idèntics, ja que l'ordre o la codificació no resulta essencial per a l'aplicació.

En aquest sentit, donat que les recomanacions del W3C que especifiquen el llenguatge XML i els esquemes de noms XML defineixen diverses mètodes sintàctics per expressar la mateixa informació, les aplicacions XML es prenen molta llibertat a l'hora de modificar el format o la representació física dels elements XML, sempre que no s'afecti a la informació continguda als mateixos.

La canonicalització serveix perquè una aplicació pugui determinar els canvis que s'hagin pogut produir en un document XML, mitjançant la comparació de la forma canònica del document abans i després d'un determinat processament.

De fet, la problemàtica en relació amb la signatura electrònica rau en aspectes com que el document XML pot ser posteriorment modificat, amb l'addició de nous elements, fins i tot dins dels elements que han estat objecte de signatura, o poden ser representants físicament de forma diferent⁴, el que pot suposar que la signatura es verifiqui incorrectament, tot i ser vàlida.

Per evitar aquests problemes, les dades que han de ser signades són canonicalitzades abans de produir el resum criptogràfic, de forma que encara que el posterior processament del document XML canviï l'aspecte dels elements a partir dels quals es va formar la signatura electrònica, sempre es pugui reconstruir posteriorment i validar la signatura electrònica.

Aquest element té la següent definició d'esquema:

```
<element name="CanonicalizationMethod"
  type="ds:CanonicalizationMethodType"/>

<complexType name="CanonicalizationMethodType" mixed="true">
  <sequence>
    <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
    <!-- (0,unbounded) elements from (1,1) namespace -->
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

Els algorismes de canonicalització es representen mitjançant URIs indicades com atributs de l'element que els utilitza. Els productes que implementen la signatura XML han d'emprar el següents algorismes de canonicalització:

⁴ Per exemple, perquè l'aplicació XML afegixi espais en blanc.

-
- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315> (obligatori)
 - <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments> (opcional)

El següent és un exemple d'element de canonicalització XML:

```
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-  
c14n-20010315"/>
```

L'especificació normativa de XML Canònic és "Exclusive XML Canonicalization Version 1.0, W3C Recommendation 18 July 2002", generalment coneguda amb l'acrònim C14N.

L'algorisme C14N és capaç de tractar com entrada una cadena d'octets o un conjunt de nodes XPath, i produeix una cadena d'octets com a sortida. L'XML Canònic és fàcilment parametritzat, mitjançant una URI addicional per ometre o retindre els comentaris inclosos al document XML.

3.1.2 El mètode de signatura

L'element `SignatureMethod`, basat en el tipus `SignatureMethodType`, és un element obligatori que especifica l'algorisme emprat per a la generació i verificació de la signatura electrònica.

Aquest algorisme identifica totes les funcions criptogràfiques involucrades en l'operació de signatura (per exemple, resumit, signatura, autenticació, etc).

Aquest element té la següent definició d'esquema:

```
<element name="SignatureMethod" type="ds:SignatureMethodType"/>  
  
<complexType name="SignatureMethodType" mixed="true">  
  <sequence>  
    <element name="HMACOutputLength" minOccurs="0"  
      type="ds:HMACOutputLengthType"/>  
    <any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>  
    <!-- (0,unbounded) elements from (1,1) external namespace -->  
  </sequence>  
  <attribute name="Algorithm" type="anyURI" use="required"/>  
</complexType>
```

Els algorismes es representen mitjançant URIs indicades com atributs de l'element que els utilitza. Els productes que implementen la signatura XML han d'emprar el següents algorismes:

- Algorismes de resum
 - o <http://www.w3.org/2000/09/xmlsig#sha1> (obligatori)
- Algorismes de signatura
 - o <http://www.w3.org/2000/09/xmlsig#dsa-sha1> (obligatori)
 - o <http://www.w3.org/2000/09/xmlsig#rsa-sha1> (recomanat)

Els següents són exemples d'element d'algorismes:

```
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmlsig#rsa-
  sha1"/>
```

3.1.3 Les referències als objectes signats

L'element `Reference`, basat en el tipus `ReferenceType`, és un element que especifica un algorisme i un valor de resum criptogràfic, i opcionalment l'identificador de l'objecte signat, el tipus d'objecte i/o una llista de transformacions a aplicar a les dades abans de resumir-les i signar-les.

L'element pot aparèixer una o més vegades dins de l'element `SignedInfo`, en funció del nombre d'objectes a signar a que cal referir-se.

Aquest element té la següent definició d'esquema:

```
<element name="Reference" type="ds:ReferenceType"/>

<complexType name="ReferenceType">
  <sequence>
    <element ref="ds:Transforms" minOccurs="0"/>
    <element ref="ds:DigestMethod"/>
    <element ref="ds:DigestValue"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

```
<attribute name="URI" type="anyURI" use="optional"/>  
<attribute name="Type" type="anyURI" use="optional"/>  
</complexType>
```

3.1.3.1 Els atributs de les referències

L'atribut d'identificació de la referència (`Id`) permet que el camp referència sigui, a la seva vegada, referit des de qualsevol altre lloc.

L'atribut d'identificació de l'objecte signat (en forma d'URI), defineix sobre quin objecte va ser creat el contingut resumit, mitjançant una referència d'identificació uniforme de recursos, d'acord amb l'especificació IETF RFC 2396, mentre que les transformacions corresponents permeten determinar com va ser creat el contingut resumit.

Les aplicacions XML estan obligades a tractar la sintaxi URI, recomanant-se la resolució de les adreces d'acord amb el sistema HTTP (operació anomenada "desreferenciar").

Si un recurs es troba identificat per més d'una URI, aleshores cal emprar la més específica.

Quan aquest atribut s'omet, es suposa que l'aplicació destinatària coneix la identitat de l'objecte referit, per exemple, perquè aquesta informació es deriva del context de l'aplicació. En qualsevol cas, aquest atribut només es pot ometre, com a màxim, en una referència de les que formen part de l'element `SignedInfo` o de l'element `Manifest`.

L'atribut tipus (`Type`) facilita el processament de les dades referides, especialment quan es tracta de dades externes al document XML, ja que conté informació sobre el tipus d'objecte que es signa. El tipus d'objecte signat es identifica mitjançant una URI, com per exemple:

- <http://www.w3.org/2000/09/xmldsig#Object> es refereix a un objecte de dades que es signa.
- <http://www.w3.org/2000/09/xmldsig#Manifest> es refereix a un manifest que agrupa referències a objectes.
- <http://uri.etsi.org/01903#SignedProperties> es refereix a les propietats signades de la signatura o dels objectes signats.

Cal indicar que aquest atribut es refereix al tipus d'objecte assenyalat, no al seu contingut. Per exemple, un element `Object` que conté un element `SignatureProperties` és sempre referit com tipus `#Object`, no com allò que conté. A més, tot i que l'atribut aporta una informació que és aconsellable seguir, l'especificació de signatura XML no imposa cap validació de la informació del tipus.

3.1.3.2 Les transformacions dels objectes a signar

L'element opcional `Transforms`, basat en el tipus `TransformsType`, conté una llista ordenada d'elements de transformació, que descriuen com el signatari va obtenir l'objecte de dades que va ser resumida.

L'entrada del primer element de transformació és el resultat de desreferenciar l'atribut URI de l'element `Reference`. La sortida de cada element de transformació serveix d'entrada per a la següent transformació. La sortida del darrer element de transformació és l'entrada per l'algorisme de resum.

És important tenir en compte que quan s'apliquen transformacions sobre els objectes de dades, el signatari no està realment signant les dades originals, sinó els objectes transformats, el que ha de ser valorat des de la perspectiva de seguretat tècnica, però especialment des del punt de vista legal.

Cada transformació consisteix en un algorisme amb els seus paràmetres corresponents, quan resulta aplicable.

Alguns exemples de transformacions són la decodificació base64, la canonicalització, el filtrat XPath o les transformacions de fulls d'estil.

La definició genèrica de l'element `Transform` permet l'ús d'algorismes específics d'aplicacions concretes, cosa que no es recomana en els casos en que la signatura electrònica ha de ser verificada fora del domini específic de l'aplicació.

Aquests elements tenen la següent definició d'esquema:

```
<element name="Transforms" type="ds:TransformsType"/>

<complexType name="TransformsType">
  <sequence>
    <element ref="ds:Transform" maxOccurs="unbounded"/>
  </sequence>
</complexType>

<element name="Transform" type="ds:TransformType"/>

<complexType name="TransformType" mixed="true">
  <choice minOccurs="0" maxOccurs="unbounded">
    <any namespace="##other" processContents="lax"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </choice>
</complexType>
```

```
<element name="XPath" type="string"/>
</choice>
<attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

Els algorismes de transformació recomanats són els següents:

- Els algorismes de canonicalització indicats anteriorment.
- Base64: <http://www.w3.org/2000/09/xmlsig#base64>
- Filtrat XPath: <http://www.w3.org/TR/1999/REC-xpath-19991116>
- XSLT: <http://www.w3.org/TR/1999/REC-xslt-19991116>
- Signatura embolcallada: <http://www.w3.org/2000/09/xmlsig#enveloped-signature>

3.1.3.3 El mètode de resum criptogràfic

L'element `DigestMethod`, basat en el tipus `DigestMethodType`, és un element obligatori que identifica l'algorisme de resum a aplicar a l'objecte signat, una vegada ha estat transformat i convertit a una cadena d'octets.

Aquest element té la següent definició d'esquema:

```
<element name="DigestMethod" type="ds:DigestMethodType"/>
<complexType name="DigestMethodType" mixed="true">
  <sequence>
    <any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

Els algorismes es representen mitjançant URIs indicades com atributs de l'element que els utilitza. Els productes que implementen la signatura XML han d'emprar el següents algorismes de resum:

- <http://www.w3.org/2000/09/xmlsig#sha1> (obligatori)

3.1.3.4 El valor del resum criptogràfic

L'element `DigestValue`, basat en el tipus `DigestValueType`, és un element obligatori que conté el valor del resum criptogràfic codificat, d'acord amb l'algorisme corresponent.

Aquest element té la següent definició d'esquema:

```
<element name="DigestValue" type="ds:DigestValueType"/>

<simpleType name="DigestValueType">
  <restriction base="base64Binary"/>
</simpleType>
```

3.2 El valor de la signatura

L'element `SignatureValue`, basat en el tipus `SignatureValueType`, conté el valor concret d'una signatura digital, codificada en base64.

Aquest element té la següent definició d'esquema:

```
<element name="SignatureValue" type="ds:SignatureValueType"/>

<complexType name="SignatureValueType">
  <simpleContent>
    <extension base="base64Binary">
      <attribute name="Id" type="ID" use="optional"/>
    </extension>
  </simpleContent>
</complexType>
```

3.3 La informació de les claus de signatura

L'element `KeyInfo`, basat en el tipus `KeyInfoType`, és un element opcional que permet el/s destinatari/s del document signat obtenir les claus necessàries per validar la signatura electrònica.

Aquest element pot contenir claus, noms, certificats i altres informacions de gestió de claus públiques, com per exemple dades d'intercanvi o de distribució de claus. En tot cas, els aspectes de confiança relatius a les claus no són definits per l'especificació

de la signatura XML, sinó que han de ser establerts de forma externa, com per exemple pel context de l'aplicació.

Si l'element `KeyInfo` s'omet, cal suposar que el destinatari del document signat serà capaç d'identificar la clau mitjançant el context de l'aplicació.

Múltiples declaracions dins de l'element es poden referir a la mateixa clau, essent necessari per a les aplicacions que compleixin l'especificació implantar com a mínim l'element `KeyValue`. Així mateix, es recomana que les aplicacions implantin l'element `RetrievalMethod`.

Aquest element té la següent definició d'esquema:

```
<element name="KeyInfo" type="ds:KeyInfoType" />

<complexType name="KeyInfoType" mixed="true">
  <choice maxOccurs="unbounded">
    <element ref="ds:KeyName" />
    <element ref="ds:KeyValue" />
    <element ref="ds:RetrievalMethod" />
    <element ref="ds:X509Data" />
    <element ref="ds:PGPData" />
    <element ref="ds:SPKIData" />
    <element ref="ds:MgmtData" />
    <any processContents="lax" namespace="##other" />
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </choice>
  <attribute name="Id" type="ID" use="optional" />
</complexType>
```

Les opcions per representar informació de claus de signatura són les següents:

- Nom i valor de clau (`KeyName` i `KeyValue`), que identifica la clau de signatura emprada.
- Mètode de recuperació (`RetrievalMethod`), que permet referir informació de claus externa a la signatura.
- Certificat de clau pública X.509 (`X509Data`), que identifica el certificat de tipus X.509 emprat, així com la informació de revocació relacionada.
- Claus PGP (`PGPData`), que identifica la clau PGP emprada.

- Certificat de clau pública SPKI (SPKIData), que identifica el certificat de tipus SPKI emprat.
- Dades de gestió de claus (MgmtData), que identifica mecanismes de distribució o negociació de claus.

En aquesta guia analitzem únicament les opcions d'informació de claus relacionades amb l'ús de certificats de clau pública, que són necessaris per a la signatura electrònica reconeguda.

3.3.1 El mètode de recuperació d'informació de claus

L'element `RetrievalMethod`, basat en el tipus `RetrievalInfoType`, és un element que conté una referència a informació de claus (`KeyInfo`) emmagatzemada a una localització remota, externa a la signatura.

Per exemple, diverses signatures d'un document poden emprar una clau verificada mitjançant una cadena de certificats X.509v3 que apareix una única vegada al document signat, o que es troba emmagatzemada a un dipòsit d'informació local enlloc del document. En aquesta cadena, cada element `KeyInfo` pot referir-se a aquesta cadena emporant un element `RetrievalMethod` enlloc d'haver d'incloure la cadena de certificats sencera a cada signatura electrònica.

L'especificació de signatura XML inclou una llista de tipus de `KeyInfo` que es poden emprar per descriure claus de signatura remotes.

- <http://www.w3.org/2000/09/xmldsig#DSAKeyValue>
- <http://www.w3.org/2000/09/xmldsig#RSAKeyValue>
- <http://www.w3.org/2000/09/xmldsig#X509Data>
- <http://www.w3.org/2000/09/xmldsig#PGPData>
- <http://www.w3.org/2000/09/xmldsig#SPKIData>
- <http://www.w3.org/2000/09/xmldsig#MgmtData>
- <http://www.w3.org/2000/09/xmldsig#rawX509Certificate>⁵

Aquest element té la següent definició d'esquema:

```
<element name="RetrievalMethod" type="ds:RetrievalMethodType" />
```

```
<complexType name="RetrievalMethodType">
```

⁵ Es tracta d'un certificat X.509 binary (ASN.1 DER).

```
<sequence>
  <element ref="ds:Transforms" minOccurs="0"/>
</sequence>
<attribute name="URI" type="anyURI"/>
<attribute name="Type" type="anyURI" use="optional"/>
</complexType>
```

3.3.2 El certificat X.509

L'element X509Data, basat en el tipus X509DataType, és un element que conté un o més identificadors de certificats i altra informació relacionada amb claus certificades, com la identificació del subscriptor del certificat o la informació de revocació.

Aquests elements tenen la següent definició d'esquema:

```
<element name="X509Data" type="ds:X509DataType"/>

<complexType name="X509DataType">
  <sequence maxOccurs="unbounded">
    <choice>
      <element name="X509IssuerSerial" type="ds:X509IssuerSerialType"/>
      <element name="X509SKI" type="base64Binary"/>
      <element name="X509SubjectName" type="string"/>
      <element name="X509Certificate" type="base64Binary"/>
      <element name="X509CRL" type="base64Binary"/>
      <any namespace="##other" processContents="lax"/>
    </choice>
  </sequence>
</complexType>

<complexType name="X509IssuerSerialType">
  <sequence>
    <element name="X509IssuerName" type="string"/>
    <element name="X509SerialNumber" type="integer"/>
  </sequence>
</complexType>
```

Resulta obligatori que aparegui un dels continguts mínims següents. En cas que apareguin diversos elements, s'ha de considerar que tots els elements es refereixen al mateix certificat:

- L'element `X509IssuerSerial`, basat en el tipus `X509IssuerSerialType`, que conté el nom d'una Entitat de Certificat i un número de sèrie que identifiquen un certificat X509.
- L'element `X509SubjectName`, que conté un nom de subscriptor d'un certificat X.509.
- L'element `X509SKI`, que conté el valor de l'extensió `SubjectKeyIdentifier` d'un certificat X.509v3, codificat en base64.
- L'element `X509Certificate`, que conté un certificat X.509 codificat en base64.
- L'element `X509CRL`, que conté una llista de revocació de certificats codificada en base64.
- Altres elements complementaris, que es poden definir en altres esquemes de nom.

Els elements `X509IssuerSerial`, `X509SKI` i `X509SubjectName` han de referir-se al certificat o als certificats que contenen la clau de validació de signatura. Els elements que es refereixen un mateix certificat han de ser agrupats dins d'un únic element `X509Data`, juntament amb el certificat referit, quan s'indiqui.

Els elements `X509IssuerSerial`, `X509SKI` i `X509SubjectName` relatius a la mateixa clau de signatura però que es troben referits a diferents certificats – com per exemple succeeix amb una cadena de certificació – han de ser agrupats en un únic element `KeyInfo`, però poden aparèixer a diferents elements `X509Data`. Un d'aquests certificats ha de contenir la clau de validació de la signatura electrònica.

L'ordre en que apareixen els anteriors elements no és significatiu, i no permet inferir com és la cadena de certificació.

3.4 L'objecte signat

L'element opcional `Object`, basat en el tipus `ObjectType`, que pot aparèixer una o més vegades, conté qualsevol tipus de dada que ha de ser signada. L'element s'utilitza per crear signatures que embolcallen els objectes signats (també anomenades signatures embolcallants).

Aquest element té la següent definició d'esquema:

```
<element name="Object" type="ds:ObjectType"/>
```

```
<complexType name="ObjectType" mixed="true">
  <sequence minOccurs="0" maxOccurs="unbounded">
    <any namespace="##any" processContents="lax"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
  <attribute name="MimeType" type="string" use="optional"/>
  <attribute name="Encoding" type="anyURI" use="optional"/>
</complexType>
```

L'identificador de l'objecte (`Id`) s'utilitza per referir-se a aquest objecte des d'un element `Reference` d'una signatura electrònica, o des d'un element `Manifest`.

L'atribut opcional `MimeType` descriu d'acord amb l'especificació MIME, les dades dins de l'objecte, de forma independent de la seva codificació. Per exemple, en el cas d'un fitxer gràfic PNG aquest atribut contindria el valor "image/png". A més, tot i que l'atribut aporta una informació que és aconsellable seguir, l'especificació de signatura XML no imposa cap validació de la informació del tipus MIME.

Les aplicacions que requereixen d'informació normativa sobre tipus i codificació d'objectes per a la validació de la signatura electrònica haurien d'aplicar les transformacions necessàries per obtenir resultats amb tipus i codificacions correctes.

L'atribut `Encoding` es pot emprar per incloure una URI que identifica el mètode de codificació de l'objecte, com per exemple un fitxer binary.

4. Els elements opcionals de la signatura electrònica XML

L'especificació de la signatura XML estableix dos elements opcionals, el Manifest i les Propietats de la signatura.

4.1 El manifest

L'element `Manifest`, basat en el tipus `ManifestType`, conté una llista de referències a objectes que es signen.

Pot aparèixer a qualsevol lloc d'un document XML, i, si apareix dins d'un element `Signature`, ha de trobar-se contingut dins de l'element `Object`.

A diferència de la llista continguda a l'element `SignedInfo`, és l'aplicació la que defineix quins dels resums criptogràfics dels documents són comprovats, i quin és el processament a realitzar en cas que l'objecte sigui innaccessible o si falla la comprovació del resum corresponent.

En cas que l'element `Manifest` sigui referit des d'un element `SignedInfo`⁶, es calcula i verifica el resum criptogràfic del manifest sencer, però no necessàriament dels objectes inclosos a les referències incloses al manifest⁷. Quelcom semblant succeeix quan el manifest es referit des d'un altre manifest.

Aquest element té la següent definició d'esquema:

```
<element name="Manifest" type="ds:ManifestType"/>

<complexType name="ManifestType">
  <sequence>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

L'element resulta útil en diverses situacions:

⁶ Una referència continguda a l'element `SignedInfo` pot referir una URI a un manifest.

⁷ Com s'ha dit, aquest processament addicional l'haurà de fer l'aplicació.

- Quan no es desitja aplicar el comportament habitual de validació dels resums criptogràfics de les referències per a la validació de la signatura electrònica, sinó que l'aplicació controli el tractament d'aquesta validació.

Per exemple, imaginem un cas en què la signatura conté diverses referències: si una d'elles falla, la validació de la signatura falla; però és possible que en el context d'una aplicació tingui sentit considerar que la signatura electrònica resulta vàlida encara que alguna de les referències no es validi correctament. Per aconseguir aquest comportament, cal incloure aquestes referències en un manifest i tractar-lo específicament.

- Quan cal aplicar moltes signatures diferents a molts documents diferents, resulta més eficient crear les referències dins d'un manifest i referir-se al mateix des dels diferents elements `SignedInfo`.

4.2 Les propietats de la signatura

L'element opcional `SignatureProperties`, basat en el tipus `SignaturePropertiesType`, conté una o més dades addicionals relatives a la generació de la signatura, com per exemple un segell de data i hora.

Pot apareixer a qualsevol lloc d'un document XML, i, si apareix dins d'un element `Signature`, ha de trobar-se contingut dins de l'element `Object`.

Cada dada addicional es tracta dins d'un element `SignatureProperty`, basat en el tipus `SignaturePropertyType`.

Aquests elements tenen la següent definició d'esquema:

```
<element name="SignatureProperties" type="ds:SignaturePropertiesType"/>
```

```
<complexType name="SignaturePropertiesType">  
  <sequence>  
    <element ref="ds:SignatureProperty" maxOccurs="unbounded"/>  
  </sequence>  
  <attribute name="Id" type="ID" use="optional"/>  
</complexType>
```

```
<element name="SignatureProperty" type="ds:SignaturePropertyType"/>
```

```
<complexType name="SignaturePropertyType" mixed="true">  
  <choice maxOccurs="unbounded">  
    <any namespace="##other" processContents="lax"/>  
  </choice>  
</complexType>
```

```
<!-- (1,1) elements from (1,unbounded) namespaces -->
</choice>
<attribute name="Target" type="anyURI" use="required"/>
<attribute name="Id" type="ID" use="optional"/>
</complexType>
```

5. El elements addicionals de la signatura electrònica XML derivats de la Directiva europea (XAdES)

Addicionalment als elements i continguts de la signatura electrònica que ja hem presentat, resulta necessari presentar l'especificació de l'ETSI TS 101903, que determina els formats de signatura electrònica d'acord amb la Directiva europea de signatura electrònica.

Aquesta especificació, que s'inscriu dins del mandat de normalització tècnica de la signatura electrònica realitzada per la Comissió Europea als organismes de normalització europeus, sota la direcció i supervisió de la Iniciativa Europea de Normalització de la Signatura Electrònica (EESSI), descriu configuracions específiques i elements addicionals de la signatura electrònica, amb els següents objectius:

1. Assegurar el compliment dels requisits jurídics de la signatura electrònica avançada i, en el seu cas, de la signatura electrònica reconeguda.
2. Garantir la possibilitat de validar legalment la signatura electrònica, fins i tot durant llargs terminis temporals.
3. Especificar els casos d'ús del segellament de data i hora dels continguts signats, les signatures electròniques i la informació amb valor d'evidència associada a les mateixes.

5.1 Les propietats de la signatura

Per assolir els objectius esmentats anteriorment, l'especificació ETSI TS 101 903 especifica una sèrie d'elements addicionals que es refereixen a propietats de la signatura o a propietats del o dels objectes de dades signats.

Els elements específics continguts a l'esmentada especificació es poden incloure en la signatura electrònica de dues formes:

- Mitjançant la seva incorporació directa a la signatura electrònica, dins d'un element `QualifyingProperties` dins de l'element `Object` signat.
- Mitjançant la seva incorporació indirecta a la signatura, dins d'un o més elements `QualifyingPropertiesReference` dins de l'element `Object` signat. En aquest segon cas, les propietats resideixen en un lloc extern a la signatura.

L'element `QualifyingProperties` té la següent definició d'esquema:

```
<xsd:element name="QualifyingProperties"
  type="QualifyingPropertiesType"/>

<xsd:complexType name="QualifyingPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedProperties" type="SignedPropertiesType"
      minOccurs="0"/>
    <xsd:element name="UnsignedProperties" type="UnsignedPropertiesType"
      minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Target" type="xsd:anyURI" use="required"/>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Les propietats que qualifiquen la signatura, siguin incorporades o no directament a la signatura, poden ser dos tipus:

- Propietats vinculades criptogràficament pel signatari a la signatura XML, perquè formen part de la signatura electrònica mitjançant la seva inclusió a un element `Reference` de la informació signada. Aquestes propietats s'anomenen Propietats signades.
- Propietats no vinculades criptogràficament pel signatari a la signatura XML, anomenades Propietats no signades.

L'atribut `Target` identifica la signatura XML amb la qual es relacionen les propietats. El valor ha de trobar-se buit quan l'element `QualifyingProperties` està embolcallat per la signatura XML a que es refereix, i ha de contenir una URI assenyalant a la signatura XML.

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

Per la seva banda, l'element `QualifyingPropertiesReference` té la següent definició d'esquema:

```
<xsd:element name="QualifyingPropertiesReference"
  type="QualifyingPropertiesReferenceType"/>
```

```
<xsd:complexType name="QualifyingPropertiesReferenceType">
  <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

L'atribut URI conté una referència a un element `QualifyingProperties` extern a la signatura.

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

5.1.1 Les propietats signades

L'element `SignedProperties` conté un nombre de propietats que són signades i formen part de la signatura XML, de forma col·lectiva.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SignedProperties" type="SignedPropertiesType" />

<xsd:complexType name="SignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedSignatureProperties"
      type="SignedSignaturePropertiesType" />
    <xsd:element name="SignedDataObjectProperties"
      type="SignedDataObjectPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

L'element ha de contenir una o més propietats que qualifiquen al signatari o a la pròpia signatura electrònica, agrupades dins de l'element `SignedSignatureProperties`.

També pot contenir una o més propietats que qualifiquen alguns dels objectes de dades signats, agrupats dins de l'element `SignedDataObjectProperties`.

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

5.1.1.1 Les propietats signades de la signatura

L'element `SignedSignatureProperties` agrupa les propietats signades associades amb la signatura referida a l'atribut `Target` de l'element `QualifyingProperties`.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SignedSignatureProperties"
  type="SignedSignaturePropertiesType" />

<xsd:complexType name="SignedSignaturePropertiesType">
  <xsd:sequence>
    <xsd:element name="SigningTime" type="xsd:dateTime"
      minOccurs="0"/>
    <xsd:element name="SigningCertificate" type="CertIDListType"
      minOccurs="0"/>
    <xsd:element name="SignaturePolicyIdentifier"
      type="SignaturePolicyIdentifierType" minOccurs="0"/>
    <xsd:element name="SignatureProductionPlace"
      type="SignatureProductionPlaceType" minOccurs="0"/>
    <xsd:element name="SignerRole" type="SignerRoleType"
      minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Les propietats de la signatura que es poden signar són les següents:

- La data i hora de la signatura electrònica (`SigningTime`).
- El certificat emprat per signar (`SigningCertificate`).
- L'identificador de la política de signatura electrònica (`SignaturePolicyIdentifier`).
- El lloc de producció de la signatura electrònica (`SignatureProductionPlace`).
- El rol del signatari (`SignerRole`).

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

Amb la finalitat de protegir les propietats amb la signatura XML, cal afegir-li un element `Reference` que calculi el resum criptogràfic del contingut de l'element `SignedProperties` i l'afegeixi al càlcul del valor del càlcul de la signatura digital

La referència ha d'identificar les propietats signades amb el tipus <http://uri.etsi.org/01903#SignedProperties>.

5.1.1.2 Les propietats signades de l'objecte de dades

L'element `SignedDataObjectProperties` agrupa les propietats signades associades amb un o més objectes de dades signats per la signatura referida a l'atribut `Target` de l'element `QualifyingProperties`.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SignedDataObjectProperties"
  type="SignedDataObjectPropertiesType"/>

<xsd:complexType name="SignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="DataObjectFormat" type="DataObjectFormatType"
      minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="CommitmentTypeIndication"
      type="CommitmentTypeIndicationType" minOccurs="0"
      maxOccurs="unbounded"/>
    <xsd:element name="AllDataObjectsTimeStamp"
      type="XAdESTimeStampType"
      minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="IndividualDataObjectsTimeStamp"
      type="XAdESTimeStampType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Les propietats de l'objecte de dades signat que es poden signar són les següents:

- El format de l'objecte de dades (`DataObjectFormat`).

- La indicació del tipus de compromís del signatari (CommitmentTypeIndication).
- El segell de data i hora sobre tots els objectes de dades signats (AllDataObjectsTimeStamp).
- El segell de data i hora sobre un objecte de dades individual signat (IndividualDataObjectsTimeStamp).

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

5.1.2 Les propietats no signades

L'element `UnsignedProperties` conté una o més propietats que no són signades i, per tant, no formen part de la signatura XML.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="UnsignedProperties" type="UnsignedPropertiesType" />

<xsd:complexType name="UnsignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedSignatureProperties"
      type="UnsignedSignaturePropertiesType" minOccurs="0"/>
    <xsd:element name="UnsignedDataObjectProperties"
      type="UnsignedDataObjectPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

L'element pot contenir una o més propietats que qualifiquen al signatari o a la pròpia signatura electrònica, agrupades dins de l'element `UnsignedSignatureProperties`.

També pot contenir una o més propietats que qualifiquen alguns dels objectes de dades signats, agrupats dins de l'element `UnsignedDataObjectProperties`.

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

5.1.2.1 Les propietats no signades de la signatura

L'element `UnsignedDataObjectProperties` agrupa les propietats no signades associades amb una signatura referida a l'atribut `Target` de l'element `QualifyingProperties`.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="UnsignedSignatureProperties"
  type="UnsignedSignaturePropertiesType"/>

<xsd:complexType name="UnsignedSignaturePropertiesType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="CounterSignature" type="CounterSignatureType" />
    <xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>
    <xsd:element name="CompleteCertificateRefs"
      type="CompleteCertificateRefsType"/>
    <xsd:element name="CompleteRevocationRefs"
      type="CompleteRevocationRefsType"/>
    <xsd:element name="AttributeCertificateRefs"
      type="CompleteCertificateRefsType"/>
    <xsd:element name="AttributeRevocationRefs"
      type="CompleteRevocationRefsType"/>
    <xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
    <xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>
    <xsd:element name="CertificateValues" type="CertificateValuesType"/>
    <xsd:element name="RevocationValues" type="RevocationValuesType"/>
    <xsd:element name="AttrAuthoritiesCertValues"
      type="CertificateValuesType"/>
    <xsd:element name="AttributeRevocationValues"
      type="RevocationValuesType"/>
    <xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>
    <xsd:any namespace="##other" />
  </xsd:choice>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Les propietats de la signatura que es poden incloure sense signar són les següents:

- La contrasignatura (`CounterSignature`).
- El segell de data i hora sobre la signatura (`SignatureTimeStamp`).
- Les referències completes dels certificats (`CompleteCertificateRefs`).
- Les referències completes de la informació de revocació dels certificats (`CompleteRevocationRefs`).
- Les referències completes dels certificats d'atributs (`AttributeCertificateRefs`).
- Les referències completes de la informació de revocació d'atributs (`AttributeRevocationRefs`).
- El segell de data i hora sobre la signatura completa (`SigAndRefsTimeStamp`).
- El segell de data i hora sobre les referències de certificats i revocacions (`RefsOnlyTimeStamp`).
- Els valors dels certificats (`CertificateValues`).
- Els valors de les revocacions (`RevocationValues`).
- Els valors dels certificats d'autoritat d'atributs (`AttrAuthoritiesCertValues`).
- Els valors de les revocacions d'atributs (`AttributeRevocationValues`).
- El segell de data i hora d'arxiu (`ArchiveTimeStamp`).
- Altres propietats (`Any`), que permet la futura addició de propietats.

L'atribut opcional `Id` permet referir-se a aquest element des de qualsevol altre lloc del document XML.

5.1.2.2 Les propietats no signades de l'objecte de dades

L'element `UnsignedDataObjectProperties` agrupa les propietats no signades associades amb un o més objectes de dades signats per la signatura referida a l'atribut `Target` de l'element `QualifyingProperties`.

Aquest element, de moment, no s'utilitza, i només s'indica a efectes de futures extensions per aplicacions.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="UnsignedDataObjectProperties"  
  type="UnsignedDataObjectPropertiesType" />
```

```
<xsd:complexType name="UnsignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedDataObjectProperty" type="AnyType"
      minOccurs="0" maxOccurs="unbounded" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
```

5.2 La data i hora de la signatura electrònica

L'element `SigningTime` especifica el moment en què, suposadament, el signatari ha realitzat el procés de signar.

Ha de ser sempre una propietat signada, només pot apareixer una vegada i qualifica tota la signatura.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SigningTime" type="xsd:dateTime" />
```

5.3 La contrasignatura

Una contrasignatura és una signatura sobre una signatura anterior, que es pot realitzar de dues formes:

- Mitjançant l'ús de referències.
- Mitjançant l'ús de l'element específic `Contrasignatura`.

5.3.1 Contrasignatures mitjançant referències

En aquest cas, el que es fa és incloure, dins d'una signatura XML un element `Reference` amb tipus <http://uri.etsi.org/01903#CountersignedSignature>, que assenyala a la contrasignatura.

La referència s'ha de construir de forma que signi el valor `SignatureValue` de la signatura contrasignada, d'acord amb les normes de processament de referències de la signatura XML.

5.3.2 Contrasignatures mitjançant l'element contrasignatura

En aquest segon cas, s'utilitza l'element `CounterSignature`, que és una propietat no signada que qualifica a la signatura que l'incorpora, contenint una o més contrasignatures.

El contingut d'aquest element és una signatura; el seu element `SignedInfo` ha de contenir un element `Reference` assenyalant l'element `SignatureValue` de la signatura contrasignada, degudament codificada en base64 i canonicalitzada.

És a dir, la contrasignatura es troba embolcallada dins de la signatura contrasignada.

A la seva vegada, la contrasignatura pot ser contrasignada, construint cadenes de signatures, representant explícitament fluxes de procés signat.

L'element té la següent definició d'esquema:

```
<xsd:element name="CounterSignature" type="CounterSignatureType" />

<xsd:complexType name="CounterSignatureType">
  <xsd:sequence>
    <xsd:element ref="ds:Signature"/>
  </xsd:sequence>
</xsd:complexType>
```

5.4 El certificat emprat per signar

L'element `SigningCertificate` ha estat dissenyat per prevenir atacs de substitució i reexpedició de certificats, així com per permetre l'ús en la verificació de la signatura electrònica d'un conjunt restringit de certificats d'autorització.

Ha de ser sempre una propietat signada, només pot apareixer una vegada i qualifica tota la signatura.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SigningCertificate" type="CertIDListType" />

<xsd:complexType name="CertIDListType">
  <xsd:sequence>
    <xsd:element name="Cert" type="CertIDType" maxOccurs="unbounded" />
  </xsd:sequence>
</xsd:complexType>
```

```
<xsd:complexType name="CertIDType">
  <xsd:sequence>
    <xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
    <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="DigestAlgAndValueType">
  <xsd:sequence>
    <xsd:element ref="ds:DigestMethod"/>
    <xsd:element ref="ds:DigestValue"/>
  </xsd:sequence>
</xsd:complexType>
```

L'element conté la seqüència o llista d'identificadors de certificats i els seus resums criptogràfics (en forma d'elements `Certs`).

L'element `IssuerSerial` conté la identificació de cadascun dels certificats continguts dins la llista anteriorment indicada. En cas que l'element `X509IssuerSerial` sigui emprat dins de la signatura, com hem vist anteriorment, per referir-se al mateix certificat, el seu valor ha de ser el mateix que el de d'aquest element `IssuerSerial`.

L'element `CertDigest` conté el resum de cadascun dels certificats continguts dins la llista anteriorment indicada. Està format per dos elements:

- `DigestMethod` indica l'algorisme de resum emprats.
- `DigestValue` indica el valor del resum criptogràfic calculat sobre el certificat.

L'atribut opcional `URI` indica el lloc on es pot trobar el certificat referit.

5.5 L'identificador de la política de signatura electrònica

Com veurem posteriorment, algunes signatures electròniques identifiquen de forma explícita la política d'acord amb la qual han estat creades o cal que siguin verificades.

Existeixen dues formes per identificar la política de signatura:

- La signatura electrònica pot contenir un identificador explícit i unívoc de la política aplicable, juntament amb el valor del resum criptogràfic de la política de signatura, de forma que resulta verificable que la política de signatura electrònica indicada pel signatari és la mateixa que la política emprada pel verificador de la signatura.

Aquest indicador explícit de política té una referència única global, que, en aquest cas, es vinculada pel signatari a la signatura. En aquest cas, ha d'existir una especificació de política codificada, pel seu tractament automàtic per part de l'aplicació. Es tracta d'una manifestació explícita sobre l'aplicació també explícita de la política.

Finalment, cal dir que aquest tipus d'identificador de política de signatura electrònica pot ser qualificada amb informació addicional, com veurem posteriorment.

- Alternativament, la signatura electrònica pot prescindir d'incloure l'identificador i resum criptogràfic abans esmentats. Això resulta possible quan la política de signatura pot ser derivada unívocament de la semàntica del tipus d'objectes de dades signats, així com d'altres informacions, com per exemple la llei o un contracte privat, que mencionin que una política de signatura ha de ser emprada de forma obligatòria per signar el contingut especificat.
- En aquest cas, la signatura contindrà específicament un element buit indicant que s'utilitza aquesta forma implícita per identificar la política aplicable. Es tracta d'una manifestació explícita sobre l'aplicació implícita de la política.

Ha de ser sempre una propietat signada, només pot apareixer una vegada i qualifica tota la signatura.

Aquest element té la següent definició d'esquema:

```
<xsd:element name="SignaturePolicyIdentifier"
  type="SignaturePolicyIdentifierType"/>

<xsd:complexType name="SignaturePolicyIdentifierType">
  <xsd:choice>
    <xsd:element name="SignaturePolicyId" type="SignaturePolicyIdType"/>
    <xsd:element name="SignaturePolicyImplied"/>
  </xsd:choice>
</xsd:complexType>

<xsd:complexType name="SignaturePolicyIdType">
  <xsd:sequence>
```

```
<xsd:element name="SigPolicyId" type="ObjectIdentifierType"/>
<xsd:element ref="ds:Transforms" minOccurs="0"/>
<xsd:element name="SigPolicyHash" type="DigestAlgAndValueType"/>
<xsd:element name="SigPolicyQualifiers"
  type="SigPolicyQualifiersListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SigPolicyQualifiersListType">
  <xsd:sequence>
    <xsd:element name="SigPolicyQualifier" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

L'element `SignaturePolicyId` apareix quan la política de signatura s'identifica de forma explícita, d'acord amb la primera alternativa.

L'element `SigPolicyId` conté un identificador unívoc per aquesta versió de la política, mentre que l'element `SigPolicyHash` conté el valor del resum criptogràfic de la política de signatura.

L'element opcional `Transforms` permet tractar les transformacions necessàries sobre el document de política de signatura abans d'obtenir-ne el resum criptogràfic.

L'element `SigPolicyQualifier` pot contenir informació addicional que qualifica la política de signatura electrònica.

Per una altra banda, d'acord amb la segona alternativa indicada anteriorment, es pot emprar l'element `SignaturePolicyImplied`, que és l'element buit que indica que els objectes de dades signats i altres dades externes determinen la política implícita a aplicar.

Respecte a les informacions que poden qualificar l'identificador de política de signatura, s'han establert dues:

- Una URL a la qual es pot obtenir el document de política de signatura electrònica.
- Un avís a l'usuari que s'hauria de mostrar quan la signatura es verifica.

Els anteriors elements tenen la següent definició d'esquema:

```
<xsd:element name="SPURI" type="xsd:anyURI" />

<xsd:element name="SPUserNotice" type="SPUserNoticeType" />

<xsd:complexType name="SPUserNoticeType">
  <xsd:sequence>
    <xsd:element name="NoticeRef" type="NoticeReferenceType"
      minOccurs="0" />
    <xsd:element name="ExplicitText" type="xsd:string"
      minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NoticeReferenceType">
  <xsd:sequence>
    <xsd:element name="Organization" type="xsd:string" />
    <xsd:element name="NoticeNumbers" type="IntegerListType" />
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IntegerListType">
  <xsd:sequence>
    <xsd:element name="int" type="xsd:integer" minOccurs="0"
      maxOccurs="unbounded" />
  </xsd:sequence>
</xsd:complexType>
```

L'element `SPUserNotice` agrupa les formes de referir-se als avisos d'usuari.

L'element `ExplicitText` conté un text de fins a 200 caràcters a mostrar quan la signatura es verificada, mentre que l'element `NoticeRef` identifica numèricament els avisos d'una organització concreta, de forma que una aplicació els pugui obtenir i tractar a partir d'un fitxer.

5.6 El format de l'objecte de dades signat

L'element `DataObjectFormat` conté informació sobre el format de l'objecte de dades signat. S'hauria d'incloure quan les dades signades han de ser presentades a usuaris humans en la verificació si el format de presentació no es pot determinar implícitament a partir de les dades signades.

És una propietat signada que qualifica un objecte de dades signat específic, i per tant, pot aparèixer tantes vegades a una signatura com els objectes de dades signats.

L'element té la següent definició d'esquema:

```
<xsd:element name="DataObjectFormat" type="DataObjectFormatType"/>

<xsd:complexType name="DataObjectFormatType">
  <xsd:sequence>
    <xsd:element name="Description" type="xsd:string" minOccurs="0"/>
    <xsd:element name="ObjectIdentifier" type="ObjectIdentifierType"
      minOccurs="0"/>
    <xsd:element name="MimeType" type="xsd:string" minOccurs="0"/>
    <xsd:element name="Encoding" type="xsd:anyURI" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="ObjectReference" type="xsd:anyURI"
    use="required"/>
</xsd:complexType>
```

L'atribut obligatori `ObjectReference` ha de referir-se a l'element `Reference` de la signatura que assenjala a l'objecte de dades qualificat.

L'element ha de contenir un⁸ o més dels següents elements opcionals:

- Informació textual relativa a l'objecte de dades signat, a l'element `Description`.
- Un identificador indicant el tipus d'objecte de dades signat, a l'element `ObjectIdentifier`, que permet identificadors de tipus URI i de tipus OID.
- Una identificació del tipus MIME corresponent a l'objecte de dades signat, a l'element `MimeType`.
- Una indicació del format de codificació de l'objecte de dades signat, a l'element `Encoding`.

⁸ Amb excepció de l'element `Encoding`, que no té perquè aparèixer en cap cas.

5.7 La indicació del tipus de compromís del signatari

L'element `CommitmentTypeIndication` permet a un signatari explicitar a un verificador que, signant les dades, mostra un tipus de compromís del signatari. La indicació del tipus de compromís pot ser qualificada amb informació addicional.

Aquesta indicació es pot produir mitjançant l'ús d'un atribut específic, que en aquest cas ha de ser un atribut signat, o mitjançant la seva inclusió dins d'una política de signatura electrònica.

És una propietat signada que qualifica un objecte de dades signat específic, i per tant, pot aparèixer tantes vegades a una signatura com els objectes de dades signats.

L'element té la següent definició d'esquema:

```
<xsd:element name="CommitmentTypeIndication"
  type="CommitmentTypeIndicationType"/>

<xsd:complexType name="CommitmentTypeIndicationType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeId" type="ObjectIdentifierType"/>
    <xsd:choice>
      <xsd:element name="ObjectReference"
        type="xsd:anyURI" maxOccurs="unbounded"/>
      <xsd:element name="AllSignedDataObjects"/>
    </xsd:choice>
    <xsd:element name="CommitmentTypeQualifiers"
      type="CommitmentTypeQualifiersListType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CommitmentTypeQualifiersListType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeQualifier"
      type="AnyType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Els tipus de compromís definits són els següents:

- Prova d'origen (*proof of origin*) indica que el signatari reconeix haver creat, aprovat i enviat el missatge. La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfOrigin>.
- Prova de recepció (*proof of reception*) indica que el signatari reconeix haver rebut el contingut del missatge. La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfReceipt>.
- Prova de lliurament (*proof of delivery*) indica que el signatari⁹ que inclou aquesta indicació ha lliurat el missatge en un magatzem local accessible pel receptor del missatge. La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfDelivery>.
- Prova d'enviament (*proof of sender*) indica que el signatari ha enviat el missatge (però no necessàriament que l'ha creat). La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfSender>.
- Prova d'aprovació (*proof of approval*) indica que el signatari ha aprovat el contingut del missatge. La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfApproval>.
- Prova de creació (*proof of creation*) indica que el signatari ha creat el missatge (però no necessàriament que l'ha aprovat o enviat). La URI que identifica el tipus de contingut és <http://uri.etsi.org/01093/v1.2.2#ProofOfCreation>.

Cada element `ObjectReference` es refereix a un element `Reference` que assenyala, dins de la signatura, un objecte de dades signat qualificat per la indicació del tipus de compromís del signatari amb respecte a l'objecte en qüestió.

En cas que el tipus de compromís sigui el mateix per a tots els objectes de dades signats, cal incloure l'element buit `AllSignedDataObjects`.

L'element `CommitmentTypeQualifiers` permet afegir dades addicionals sobre el tipus de compromís del signatari.

5.8 El lloc de producció de la signatura

L'element `SignatureProductionPlace` especifica una adreça associada amb el signatari, que es troba a una localització geogràfica particular, com per exemple una ciutat.

És una propietat signada que qualifica al signatari, i no pot aparèixer més d'una vegada a la signatura.

L'element té la següent definició d'esquema:

⁹ Típicament es tracta d'un intermediari, com per exemple un proveïdor de correu electrònic.

```
<xsd:element name="SignatureProductionPlace"
  type="SignatureProductionPlaceType"/>

<xsd:complexType name="SignatureProductionPlaceType">
  <xsd:sequence>
    <xsd:element name="City" type="xsd:string" minOccurs="0"/>
    <xsd:element name="StateOrProvince" type="xsd:string"
      minOccurs="0"/>
    <xsd:element name="PostalCode" type="xsd:string" minOccurs="0"/>
    <xsd:element name="CountryName" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

5.9 El rol del signatari

L'element `SignerRole` especifica els rols en que actua el signatari, que poden ser de dos tipus¹⁰:

- Rols al·legats pel signatari.
- Rols del signatari certificats.

És una propietat signada que qualifica al signatari, i no pot aparèixer més d'una vegada a la signatura.

L'element té la següent definició d'esquema:

```
<xsd:element name="SignerRole" type="SignerRoleType"/>

<xsd:complexType name="SignerRoleType">
  <xsd:sequence>
    <xsd:element name="ClaimedRoles" type="ClaimedRolesListType"
      minOccurs="0"/>
    <xsd:element name="CertifiedRoles" type="CertifiedRolesListType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

¹⁰ Al menys una de les dues opcions ha d'aparèixer dins l'element, podent-hi constar les dues a la vegada, en relació amb rols diferents.

```
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ClaimedRolesListType">
  <xsd:sequence>
    <xsd:element name="ClaimedRole" type="AnyType"
      maxOccurs="unbounded" />
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CertifiedRolesListType">
  <xsd:sequence>
    <xsd:element name="CertifiedRole" type="EncapsulatedPKIDataType"
      maxOccurs="unbounded" />
  </xsd:sequence>
</xsd:complexType>
```

L'element `ClaimedRoles` conté una seqüència de rols al·legats pel signatari. Poden venir especificats mitjançant cadenes de text o bé mitjançant qualsevol altre tipus de dades, si bé resulta aleshores necessari definir-los en el context o domini d'aplicació¹¹.

L'element `CertifiedRoles` conté un o més certificats d'atributs codificats en DER i embolcallats dins del tipus `EncapsulatedPKIDataType`.

5.10 El segell de data i hora sobre tots els objectes de dades signats

L'element `AllDataObjectsTimeStamp` conté el segell de data i hora, calculat abans de la creació de la signatura, sobre la llista ordenada¹² tots els elements `Reference` continguts dins de la signatura que assenyalen els objectes a signar, amb excepció de l'element `SignedProperties`.

És una propietat signada que qualifica els objectes de dades signats, que pot aparèixer una o més vegades, de diferents Entitats de Segellament de Data i Hora.

¹¹ Mitjançant el corresponent esquema de noms si es tracta d'un tipus definit XML, identificat dins d'un espai de noms propi.

¹² La llista es produeix a partir del processament de les diferents referències, aplicant els mètodes de canonicalització que s'escaiguin.

L'element té la següent definició d'esquema:

```
<xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType"/>
```

5.11 El segell de data i hora sobre un objecte de dades individual signat

L'element `IndividualDataObjectsTimeStamp` conté el segell de data i hora, calcular abans de la creació de la signatura, sobre la llista ordenada¹³ d'alguns elements `Reference` continguts dins de la signatura que assenyalen objectes a signar, amb excepció de l'element `SignedProperties`.

És una propietat signada que qualifica els objectes de dades signats, que pot aparèixer una o més vegades, de diferents Entitats de Segellament de Data i Hora.

L'element té la següent definició d'esquema:

```
<xsd:element name="IndividualDataObjectsTimeStamp"  
  type="XAdESTimeStampType"/>
```

Aquesta propietat utilitza el mecanisme `Include`, de forma que les aplicacions que la generin han de compondre els elements `Include` necessaris per referir-se als elements `Reference` en relació amb els quals es genera el segell de data i hora.

5.12 El segell de data i hora sobre la signatura

L'element `SignatureTimeStampToken` conté el segellament de la data i l'hora del valor de la signatura (d'un signatari concret), demostrant que la signatura existia en un moment concret del temps.

És una propietat no signada¹⁴ que qualifica la signatura, que pot aparèixer una o més vegades, de diferents Entitats de Segellament de Data i Hora.

L'element té la següent definició d'esquema:

```
<xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>
```

¹³ La llista es produeix a partir del processament de les diferents referències, aplicant els mètodes de canonicalització que s'escaiguin.

¹⁴ Lògicament, ja que la signatura ja ha estat creada.

5.13 Les referències completes dels certificats

L'element `CompleteCertificateRefs` conté les referències al conjunt dels certificats d'Entitat de Certificació que han estat emprats per validar una signatura electrònica¹⁵.

És una propietat no signada, que qualifica la signatura, i que només pot aparèixer una vegada.

L'element té la següent definició d'esquema:

```
<xsd:element name="CompleteCertificateRefs"
  type="CompleteCertificateRefsType"/>

<xsd:complexType name="CompleteCertificateRefsType">
  <xsd:sequence>
    <xsd:element name="CertRefs" type="CertIDListType" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

L'element `CertRefs` conté una llista d'elements `Cert`, que incorporen la identificació i el resum criptogràfic de cada certificat.

5.14 Les referències completes de la informació de revocació de certificats

L'element `CompleteRevocationRefs` conté les referències a les informacions de revocació dels certificats del signatari i de les Entitats de Certificació, que han estat emprats per validar una signatura electrònica¹⁶, principalment Llistes de Revocació de Certificats (CRLs) i OCSP.

Aquesta propietat es pot emprar per demostrar que el verificador de la signatura electrònica ha aplicat la diligència deguda en relació amb la comprovació de la signatura electrònica, i que serà capaç de recuperar aquesta informació des del lloc en que es trobi emmagatzemada.

¹⁵ També es podria emprar per referir-se als certificats que formen una cadena de certificats que permet validar un segell criptogràfic de data i hora.

¹⁶ També es podria emprar per referir-se a les informacions de revocació de certificats que permet validar un segell criptogràfic de data i hora.

És una propietat no signada, que qualifica la signatura, i que només pot aparèixer una vegada.

L'element té la següent definició d'esquema:

```
<xsd:element name="CompleteRevocationRefs"
  type="CompleteRevocationRefsType"/>

<xsd:complexType name="CompleteRevocationRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRefs" type="CRLRefsType" minOccurs="0"/>
    <xsd:element name="OCSPRefs" type="OCSPRefsType" minOccurs="0"/>
    <xsd:element name="OtherRefs" type="OtherCertStatusRefsType"
      minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<xsd:complexType name="CRLRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRef" type="CRLRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLRefType">
  <xsd:sequence>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"/>
    <xsd:element name="CRLIdentifier" type="CRLIdentifierType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLIdentifierType">
  <xsd:sequence>
    <xsd:element name="Issuer" type="xsd:string"/>
    <xsd:element name="IssueTime" type="xsd:dateTime" />
    <xsd:element name="Number" type="xsd:integer" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

```
</xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="OCSPRefsType">
  <xsd:sequence>
    <xsd:element name="OCSPRef" type="OCSPRefType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OCSPRefType">
  <xsd:sequence>
    <xsd:element name="OCSPIdentifier" type="OCSPIdentifierType"/>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ResponderIDType">
  <xsd:choice>
    <xsd:element name="ByName" type="xsd:string"/>
    <xsd:element name="ByKey" type="xsd:base64Binary"/>
  </xsd:choice>
</xsd:complexType>

<xsd:complexType name="OCSPIdentifierType">
  <xsd:sequence>
    <xsd:element name="ResponderID" type="ResponderIDType"/>
    <xsd:element name="ProducedAt" type="xsd:dateTime"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="OtherCertStatusRefsType">
  <xsd:sequence>
```

```
<xsd:element name="OtherRef" type="AnyType" maxOccurs="unbounded" />  
</xsd:sequence>  
</xsd:complexType>
```

L'element pot contenir:

- Seqüències de referències a Llistes de Revocació de Certificats, mitjançant l'element `CRLRefs`.
- Seqüències de referències a Respostes OCSP¹⁷, mitjançant l'element `OCSPRefs`.
- Seqüències de referències a altres informacions d'estat de revocació, com per exemple respostes de serveis de validació específics, com el servei d'Autoritat de Validació Semàntica de la plataforma PSIS de CATCert.

Cada element dins de la llista `CRLRefs` conté:

- El resum criptogràfic de la CRL, codificada en DER (element `DigestAlgAndValue`).
- Un conjunt d'informacions que identifiquen la CRL (element `CRLIdentifier`), incloent-hi el nom del seu emissor (element `Issuer`), el moment de la seva emissió (element `IssueTime`); opcionalment, el número de CRL (element `Number`), i finalment, un atribut opcional `URI` que permet recuperar la CRL d'un dipòsit en que es trobi emmagatzemada.

Cada element de la llista `OCSPRefs` conté:

- Un conjunt d'informacions que identifica cada resposta OCSP (`OCSPIdentifier`) mitjançant el nom del seu emissor (element `ResponderID`) i el seu moment d'emissió (element `ProducedAt`), que ha de correspondre amb el moment indicat al camp `producedAt` de la resposta OCSP corresponent; i finalment, un atribut opcional `URI` que permet recuperar la Resposta OCSP d'un dipòsit en que es trobi emmagatzemada.
- Opcionalment, el resum criptogràfic de la Resposta OCSP, codificada en DER (element `DigestAlgAndValue`), ja que pot resultar necessari distingir entre dues respostes OCSP rebudes dins del mateix segon.

¹⁷ Tal i com es defineixen a l'especificació tècnica IETF RFC 2560.

5.15 Les referències completes dels certificats d'atributs

L'element `AttributeCertificateRefs` conté les referències al conjunt dels certificats d'Entitat d'Atributs que han estat emprats per validar un certificat d'atributs del signatari; és a dir, indica la cadena de certificats considerar vàlida per verificar l'atribut certificat.

Aquest element s'utilitza, conseqüentment, únicament quan la signatura electrònica conté certificats d'atributs, per exemple, en un element `CertifiedRole`.

És una propietat no signada, que qualifica la signatura, i que només pot aparèixer una vegada.

L'element té la següent definició d'esquema:

```
<xsd:element name="AttributeCertificateRefs"  
  type="CompleteCertificateRefsType"/>
```

5.16 Les referències completes de la informació de revocació d'atributs

L'element `AttributeRevocationRefs` conté referències del conjunt de llistes de revocació de certificats o de respostes OCSP que ha estat emprat en la validació dels certificats d'atributs del signatari.

Aquest atribut es pot emprar per demostrar que el verificador de la signatura electrònica ha aplicat la diligència deguda en relació amb la comprovació dels certificats d'atributs, i que serà capaç de recuperar aquesta informació des del lloc en que es trobi emmagatzemada.

Aquest atribut s'utilitza, conseqüentment, únicament quan la signatura electrònica conté certificats d'atributs, per exemple, en un camp `CertifiedRole`, i només en cas que els certificats d'atributs siguin revocables¹⁸.

És una propietat no signada, que qualifica la signatura, i que només pot aparèixer una vegada.

L'element té la següent definició d'esquema:

```
<xsd:element name="AttributeRevocationRefs"  
  type="CompleteRevocationRefsType"/>
```

¹⁸ Algunes Entitats d'Atributs emeten certificats d'atributs que no són revocables, ja que el seu termini de vigència és breu.

5.17 El segell de data i hora sobre la signatura completa

L'element `SigAndRefsTimeStamp` conté el segellament de data i hora de la signatura electrònica completa, per protegir-la d'un possible compromís de la clau de l'Entitat de Certificació.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

```
<xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
```

Els objectes protegits pel segell de data i hora sobre la signatura completa són:

- Valor de la signatura.
- Tots els segells de data i hora sobre la signatura.
- Les referències completes de certificats.
- Les referències completes de la informació de revocació.
- Les referències completes de certificats d'atributs.
- Les referències completes de la informació de revocació d'atributs.

5.18 El segell de data i hora sobre les referències de certificats i revocacions

L'element `RefsOnlyTimeStamp` conté el segellament de data i hora de les referències de certificats i informació de revocació, tant sobre certificats de clau pública com sobre certificats d'atributs, que conté la signatura electrònica, per protegir-la d'un possible compromís de la clau de l'Entitat de Certificació.

L'ús d'aquest tipus de segellament resulta eficient quan es vol aplicar a sèries llargues de signatures basades en els mateixos certificats i informacions de revocació.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

```
<xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>
```

Els objectes protegits pel segell de data i hora sobre la signatura completa són:

-
- Les referències completes de certificats.
 - Les referències completes de la informació de revocació.
 - Les referències completes de certificats d'atributs.
 - Les referències completes de la informació de revocació d'atributs.

5.19 Els valors dels certificats

L'element `CertificateValues` conté els valors dels certificats¹⁹ a que es refereix l'atribut `CompleteCertificateRefs`, amb excepció dels valors dels certificats d'atributs, que s'inclouen a l'atribut `AttrAuthoritiesCertValues`.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

```
<xsd:element name="CertificateValues" type="CertificateValuesType"/>

<xsd:complexType name="CertificateValuesType">
  <xsd:choice minOccurs="0" maxOccurs="unbounded">
    <xsd:element name="EncapsulatedX509Certificate"
      type="EncapsulatedPKIDataType"/>
    <xsd:element name="OtherCertificate" type="AnyType"/>
  </xsd:choice>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

L'element `EncapsulatedX509Certificate` conté un certificat X.509 codificat en DER i posteriorment en base64.

L'element `OtherCertificate` permet afegir futurs formats de certificats.

Aquesta propietat pot incloure la informació dels certificats corresponents a una Entitat de Segellament de Data i Hora que ha subministrat segells de data i hora criptogràfics, quan aquests certificats no han estat inclosos dins de la signatura del segell de data i hora. En aquest cas, cas l'atribut serà afegit al segell de data i hora corresponent.

¹⁹ Els certificats també poden aparèixer al camp `KeyInfo` de la signatura, i en aquest cas no cal que es tornin a incloure en aquesta propietat.

5.20 Els valors dels certificats d'autoritat d'atributs

L'element `AttrAuthoritiesCertsValues` conté els valors dels certificats d'atributs²⁰ a que es refereix l'atribut `AttributeCertificateRefs`.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

```
<xsd:element name="AttrAuthoritiesCertValues"  
  type="CertificateValuesType"/>
```

5.21 Els valors de les revocacions

L'element `RevocationValues` conté els valors de les llistes de revocació de certificats i de les respostes OCSP a que es refereix l'atribut `CompleteRevocationReferences`.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

```
<xsd:element name="RevocationValues" type="RevocationValuesType"/>  
  
<xsd:complexType name="RevocationValuesType">  
  <xsd:sequence>  
    <xsd:element name="CRLValues" type="CRLValuesType"  
      minOccurs="0"/>  
    <xsd:element name="OCSPValues" type="OCSPValuesType" minOccurs="0"/>  
    <xsd:element name="OtherValues" type="OtherCertStatusValuesType"  
      minOccurs="0"/>  
  </xsd:sequence>  
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>  
</xsd:complexType>  
  
<xsd:complexType name="CRLValuesType">
```

²⁰ Els certificats també poden aparèixer a l'element `CertificateValues` anteriorment vist, i en aquest cas no cal que es tornin a incloure en aquesta propietat.

```
<xsd:sequence>
  <xsd:element name="EncapsulatedCRLValue"
    type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OCSPValuesType">
  <xsd:sequence>
    <xsd:element name="EncapsulatedOCSPValue"
      type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OtherCertStatusValuesType">
  <xsd:sequence>
    <xsd:element name="OtherValue" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Aquesta propietat pot incloure la informació dels certificats corresponents a una Entitat de Segellament de Data i Hora que ha subministrat segells de data i hora criptogràfics, quan aquests certificats no han estat inclosos dins de la signatura del segell de data i hora. En aquest cas, cas l'atribut serà afegit al segell de data i hora corresponent.

5.22 Els valors de les revocacions d'atributs

L'element `AttributeRevocationValues` conté els valors²¹ de les llistes de revocació de certificats i de les respostes OCSP a que es refereix l'atribut `AttributeRevocationRefs`.

És una propietat no signada, que qualifica la signatura, i que pot aparèixer una o més vegades.

L'element té la següent definició d'esquema:

²¹ Aquests valors de revocació també poden aparèixer a l'element `RevocationValues` anteriorment vist, i en aquest cas no cal que es tornin a incloure en aquesta propietat.

```
<xsd:element name="AttributeRevocationValues"  
  type="RevocationValuesType"/>
```

5.23 El segell de data i hora d'arxiu

L'element `ArchiveTimestampToken` conté el segellament de data i hora de diversos camps del `SignedData`. Si els atributs `CertificateValues` i `RevocationValues` no es troben presents, aleshores caldrà afegir-los abans de calcular el segell de data i hora d'arxiu.

Poden existir diverses instàncies d'aquest element dins de la signatura electrònica, i de fet el nombre d'aparicions d'aquest atribut es trobarà lligat a la durada de la signatura electrònica, ja que caldrà re-segellar la signatura per garantir-ne la validesa criptogràfica al llarg del temps.

```
<xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>
```

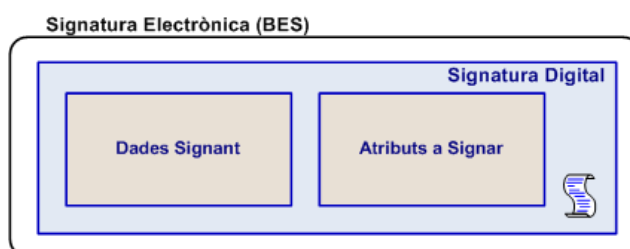
6. Els formats de la signatura electrònica XML

La signatura electrònica és un objecte digital que, com hem vist en les seccions anteriors, presenta moltes opcions de configuració diferents: en funció de les diferents necessitats identificades.

6.1 La signatura electrònica bàsica (XAdES-BES)

La signatura electrònica bàsica és el format de signatura electrònica que compleix els mínims exigits per la normativa legal de signatura electrònica derivada de la Directiva europea.

El següent gràfic mostra l'estructura de la signatura electrònica bàsica:



La signatura electrònica bàsica, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut:	Opcional

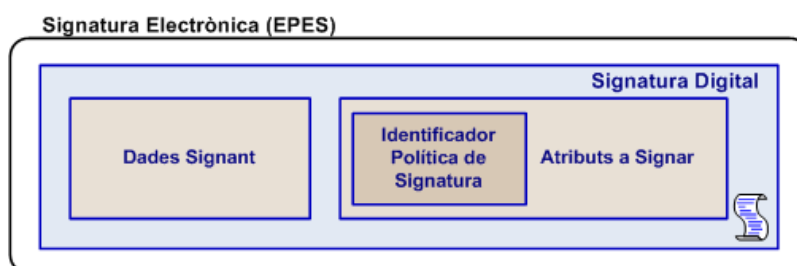
AllDataObjectsTimeStamp 0 IndividualDataObjectsTimeStamp	
9. La contrasignatura: Reference 0 CounterSignature	Opcional

6.2 La signatura electrònica amb política explícita (XAdES-EPES)

La signatura electrònica amb política explícita afegeix, a la política bàsica, la indicació explícita de la política de signatura electrònica que resulta aplicable a la creació i verificació de la signatura electrònica.

En aquest cas resulta obligatori aplicar les normes indicades a la política per considerar una signatura vàlidament creada o verificada.

El següent gràfic mostra l'estructura de la signatura electrònica amb política explícita:



La signatura electrònica amb política explícita, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: Signature	Obligatori
2. El certificat emprat per signar: SigningCertificate 0 KeyInfo:X509Data	Obligatori
3. La data i hora al·legada de la signatura: SigningTime	Opcional
4. El format de l'objecte de dades signat: DataObjectFormat	Opcional
5. La indicació del tipus de compromís: CommitmentTypeIndication	Opcional
6. El lloc de producció de la signatura: SignatureProductionPlace	Opcional
7. El rol del signatari: SignerRole	Opcional

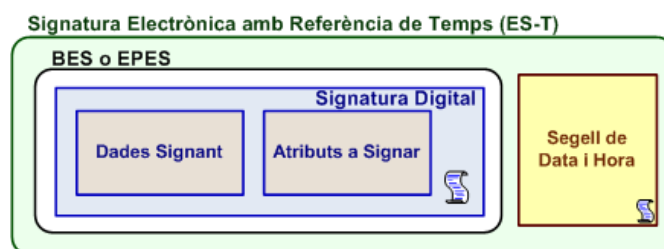
8. El segell de data i hora sobre el contingut: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp	Opcional
9. La contrasignatura: Reference o CounterSignature	Opcional
10. Identificació de la política de signatura: SignaturePolicyIdentifier	Obligatori

6.3 La signatura electrònica amb segell de data i hora (XAdES-T)

La signatura electrònica amb segell de data i hora afegeix a una signatura electrònica un segell de data i hora, amb la finalitat de garantir l'existència de la signatura abans de la data i hora corresponent.

Aquesta garantia de data i hora es pot aportar mitjançant un element addicional a la signatura, corresponent a un segell criptogràfic de data i hora, o mitjançant una marca de data i hora, que es gestiona a banda de la signatura.

El següent gràfic mostra l'estructura de la signatura electrònica amb segell de data i hora:



La signatura electrònica amb segell de data i hora, representada en sintaxi XML, es troba formada pels següents elements:

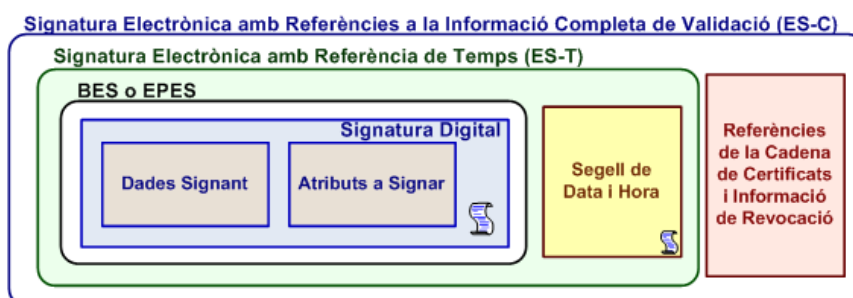
1. La signatura electrònica XML: Signature	Obligatori
2. El certificat emprat per signar: SigningCertificate o KeyInfo:X509Data	Obligatori
3. La data i hora al·legada de la signatura: SigningTime	Opcional
4. El format de l'objecte de dades signat: DataObjectFormat	Opcional
5. La indicació del tipus de compromís:	Opcional

CommitmentTypeIndication	
6. El lloc de producció de la signatura: SignatureProductionPlace	Opcional
7. El rol del signatari: SignerRole	Opcional
8. El segell de data i hora sobre el contingut: AllDataObjectsTimeStamp 0 IndividualDataObjectsTimeStamp	Opcional
9. La contrasignatura: Reference 0 CounterSignature	Opcional
10. Identificació de la política de signatura: SignaturePolicyIdentifier	Opcional ²²
11. Segell de data i hora de la signatura: SignatureTimeStamp	Obligatori ²³

6.4 La signatura electrònica amb referències completes de dades de validació (XAdES-C)

La signatura electrònica amb referències completes de dades de validació – també anomenada signatura electrònica completa – afegeix a una signatura electrònica les referències a les dades necessàries per validar la signatura, tot i que, de fet, no inclou les pròpies informacions de certificats ni de revocació.

El següent gràfic mostra l'estructura de la signatura electrònica amb referències completes de dades de validació:



La signatura electrònica amb referències completes de dades de validació, representada en sintaxi XML, es troba formada pels següents elements:

²² Depèn del tipus de signatura segellada.

²³ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut: <i>AllDataObjectsTimeStamp</i> o <i>IndividualDataObjectsTimeStamp</i>	Opcional
9. La contrasignatura: <i>Reference</i> o <i>CounterSignature</i>	Opcional
10. Identificació de la política de signatura: <i>SignaturePolicyIdentifier</i>	Opcional ²⁴
11. Segell de data i hora de la signatura: <i>SignatureTimeStamp</i>	Obligatori ²⁵
12. Referències completes de certificats: <i>CompleteCertificateRefs</i>	Obligatori
13. Referències completes de revocació: <i>CompleteRevocationRefs</i>	Obligatori
14. Referències completes de certificats d'atributs: <i>AttributeCertificateRefs</i>	Obligatori ²⁶
15. Referències completes de revocació d'atributs: <i>AttributeRevocationRefs</i>	Obligatori ²⁷

²⁴ Depèn del tipus de signatura segellada.

²⁵ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

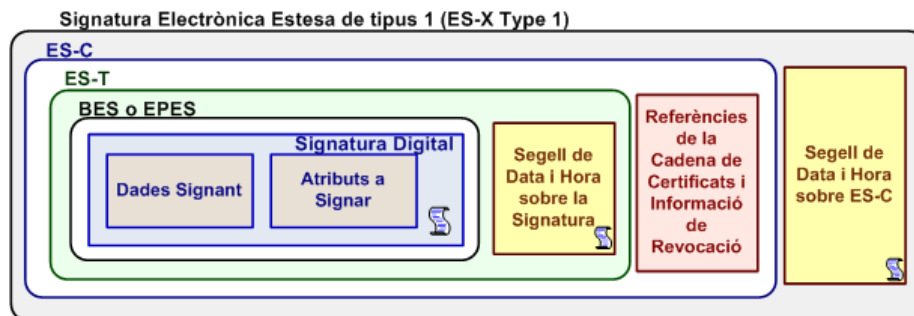
²⁶ Només és obligatori quan s'utilitzen certificats d'atributs.

²⁷ Només és obligatori quan s'utilitzen certificats d'atributs.

6.5 La signatura electrònica amb referències completes de dades de validació i segellada (XAdES-X Type 1)

La signatura electrònica amb referències completes de dades de validació i segellada – també anomenada signatura electrònica extensa de tipus 1 – afegeix a la signatura amb referències completes de dades de validació un segell de data i hora sobre aquesta, a l'objecte de protegir la integritat i garantir l'existència de les informacions de la signatura, en especial dels atributs no signats pel signatari.

El següent gràfic mostra l'estructura de la signatura electrònica amb referències completes de dades de validació i segellada:



La signatura electrònica amb referències completes de dades de validació i segellada, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut: <i>AllDataObjectsTimeStamp</i> o <i>IndividualDataObjectsTimeStamp</i>	Opcional

9. La contrasignatura: Reference o CounterSignature	Opcional
10. Identificació de la política de signatura: SignaturePolicyIdentifier	Opcional ²⁸
11. Segell de data i hora de la signatura: SignatureTimeStamp	Obligatori ²⁹
12. Referències completes de certificats: CompleteCertificateRefs	Obligatori
13. Referències completes de revocació: CompleteRevocationRefs	Obligatori
14. Referències completes de certificats d'atributs: AttributeCertificateRefs	Obligatori ³⁰
15. Referències completes de revocació d'atributs: AttributeRevocationRefs	Obligatori ³¹
16. Segell de data i hora sobre la signatura completa: SigAndRefsTimeStamp	Obligatori

6.6 La signatura electrònica amb referències completes i segellades de dades de validació (XAdES-X Type 2)

La signatura electrònica amb referències completes i segellades de dades de validació – també anomenada signatura electrònica extensa de tipus 2 – afegeix a la signatura amb referències completes de dades de validació un segell de data i hora sobre les referències de dades de validació, i no sobre la resta d'elements de la signatura, a l'objecte de protegir la integritat i garantir l'existència de d'aquestes referències.

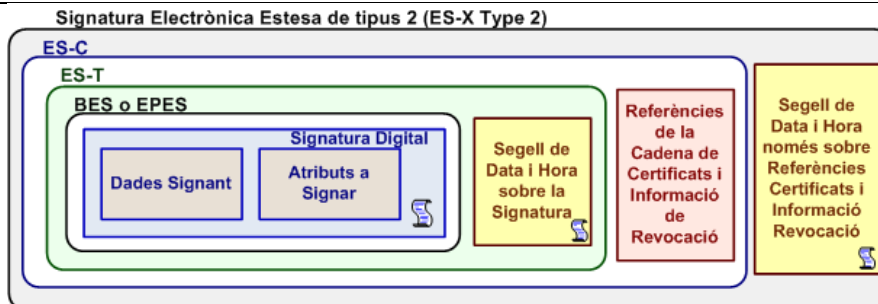
El següent gràfic mostra l'estructura de la signatura electrònica amb referències completes i segellades de dades de validació:

²⁸ Depèn del tipus de signatura segellada.

²⁹ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

³⁰ Només és obligatori quan s'utilitzen certificats d'atributs.

³¹ Només és obligatori quan s'utilitzen certificats d'atributs.



La signatura electrònica amb referències completes i segellades de dades de validació, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut: <i>AllDataObjectsTimeStamp</i> o <i>IndividualDataObjectsTimeStamp</i>	Opcional
9. La contrasignatura: <i>Reference</i> o <i>CounterSignature</i>	Opcional
10. Identificació de la política de signatura: <i>SignaturePolicyIdentifier</i>	Opcional ³²
11. Segell de data i hora de la signatura: <i>SignatureTimeStamp</i>	Obligatori ³³
12. Referències completes de certificats: <i>CompleteCertificateRefs</i>	Obligatori

³² Depèn del tipus de signatura segellada.

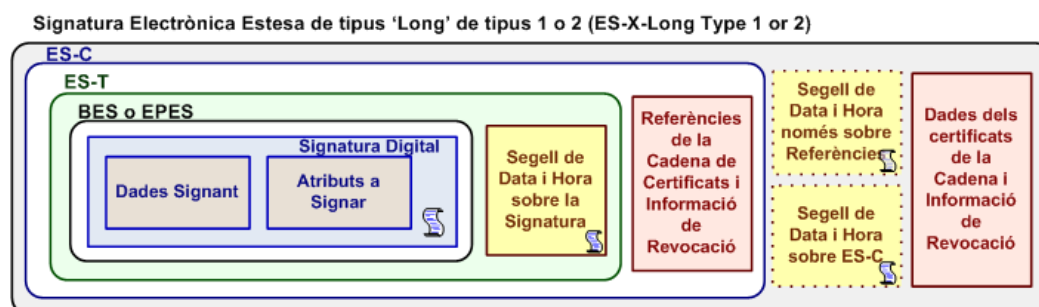
³³ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

13. Referències completes de revocació: CompleteRevocationRefs	Obligatori
14. Referències completes de certificats d'atributs: AttributeCertificateRefs	Obligatori ³⁴
15. Referències completes de revocació d'atributs: AttributeRevocationRefs	Obligatori ³⁵
16. Segell de data i hora sobre les referències de certificats i revocacions: RefsOnlyTimeStamp	Obligatori

6.7 La signatura electrònica amb dades completes de validació i segellada (XAdES-X Long Type 1)

La signatura electrònica amb dades completes de validació i segellada afegeix a la signatura amb dades completes de validació un segell de data i hora sobre aquesta, a l'objecte de protegir la integritat i garantir l'existència de les informacions de la signatura, en especial dels atributs no signats pel signatari.

El següent gràfic mostra l'estructura de la signatura electrònica amb dades completes de validació i segellades:



La signatura electrònica amb dades completes de validació i segellada, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: Signature	Obligatori
2. El certificat emprat per signar: SigningCertificate o KeyInfo:X509Data	Obligatori

³⁴ Només és obligatori quan s'utilitzen certificats d'atributs.

³⁵ Només és obligatori quan s'utilitzen certificats d'atributs.

3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut: <i>AllDataObjectsTimeStamp</i> o <i>IndividualDataObjectsTimeStamp</i>	Opcional
9. La contrasignatura: <i>Reference</i> o <i>CounterSignature</i>	Opcional
10. Identificació de la política de signatura: <i>SignaturePolicyIdentifier</i>	Opcional ³⁶
11. Segell de data i hora de la signatura: <i>SignatureTimeStamp</i>	Obligatori ³⁷
12. Referències completes de certificats: <i>CompleteCertificateRefs</i>	Obligatori
13. Referències completes de revocació: <i>CompleteRevocationRefs</i>	Obligatori
14. Referències completes de certificats d'atributs: <i>AttributeCertificateRefs</i>	Obligatori ³⁸
15. Referències completes de revocació d'atributs: <i>AttributeRevocationRefs</i>	Obligatori ³⁹
16. Segell de data i hora sobre la signatura completa: <i>SigAndRefsTimeStamp</i>	Obligatori
17. Valors de certificats: <i>CertificateValues</i>	Obligatori
18. Valors de revocació: <i>RevocationValues</i>	Obligatori
19. Valors de certificats d'atribut:	Obligatori ⁴⁰

³⁶ Depèn del tipus de signatura segellada.

³⁷ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

³⁸ Només és obligatori quan s'utilitzen certificats d'atributs.

³⁹ Només és obligatori quan s'utilitzen certificats d'atributs.

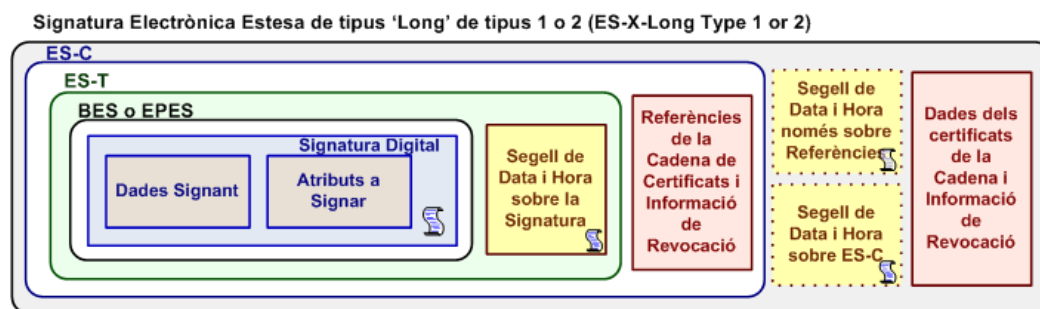
⁴⁰ Només és obligatori quan s'utilitzen certificats d'atributs.

AttrAuthoritiesCertsValues	
20. Valors de revocació de certificats d'atribut: AttributeRevocationValues	Obligatori ⁴¹

6.8 La signatura electrònica amb dades completes i segellades de validació (XAdES-X Long Type 2)

La signatura electrònica amb dades completes i segellades de validació afegeix a la signatura amb dades completes de validació un segell de data i hora sobre les referències de dades de validació, i no sobre la resta d'elements de la signatura, a l'objecte de protegir la integritat i garantir l'existència de d'aquestes referències.

El següent gràfic mostra l'estructura de la signatura electrònica amb dades completes i segellades de validació:



La signatura electrònica amb dades completes i segellades de validació, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura:	Opcional

⁴¹ Només és obligatori quan s'utilitzen certificats d'atributs.

SignatureProductionPlace	
7. El rol del signatari: SignerRole	Opcional
8. El segell de data i hora sobre el contingut: AllDataObjectsTimeStamp 0 IndividualDataObjectsTimeStamp	Opcional
9. La contrasignatura: Reference 0 CounterSignature	Opcional
10. Identificació de la política de signatura: SignaturePolicyIdentifier	Opcional ⁴²
11. Segell de data i hora de la signatura: SignatureTimeStamp	Obligatori ⁴³
12. Referències completes de certificats: CompleteCertificateRefs	Obligatori
13. Referències completes de revocació: CompleteRevocationRefs	Obligatori
14. Referències completes de certificats d'atributs: AttributeCertificateRefs	Obligatori ⁴⁴
15. Referències completes de revocació d'atributs: AttributeRevocationRefs	Obligatori ⁴⁵
16. Segell de data i hora sobre les referències de certificats i revocacions: RefsOnlyTimeStamp	Obligatori
17. Valors de certificats: CertificateValues	Obligatori
18. Valors de revocació: RevocationValues	Obligatori
19. Valors de certificats d'atribut: AttrAuthoritiesCertsValues	Obligatori ⁴⁶
20. Valors de revocació de certificats d'atribut: AttributeRevocationValues	Obligatori ⁴⁷

⁴² Depèn del tipus de signatura segellada.

⁴³ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

⁴⁴ Només és obligatori quan s'utilitzen certificats d'atributs.

⁴⁵ Només és obligatori quan s'utilitzen certificats d'atributs.

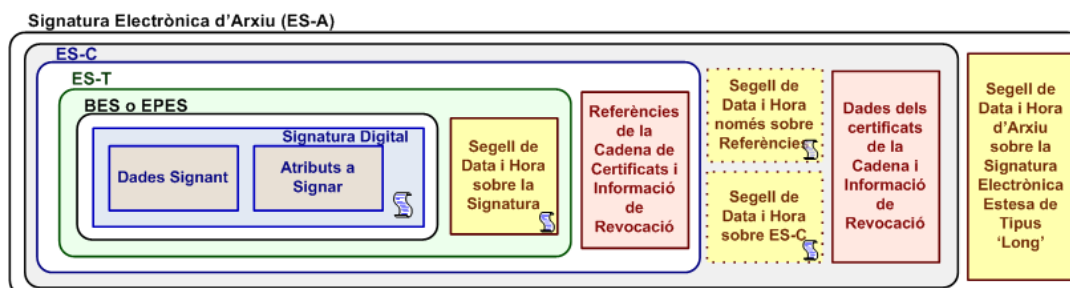
⁴⁶ Només és obligatori quan s'utilitzen certificats d'atributs.

⁴⁷ Només és obligatori quan s'utilitzen certificats d'atributs.

6.9 La signatura electrònica d'arxiu (XAdES-A)

La signatura electrònica d'arxiu afegeix a diversos formats de signatura electrònica extensa un segell de data i hora sobre la signatura.

El següent gràfic mostra l'estructura de la signatura electrònica d'arxiu:



La signatura electrònica d'arxiu, representada en sintaxi XML, es troba formada pels següents elements:

1. La signatura electrònica XML: <i>Signature</i>	Obligatori
2. El certificat emprat per signar: <i>SigningCertificate</i> o <i>KeyInfo:X509Data</i>	Obligatori
3. La data i hora al·legada de la signatura: <i>SigningTime</i>	Opcional
4. El format de l'objecte de dades signat: <i>DataObjectFormat</i>	Opcional
5. La indicació del tipus de compromís: <i>CommitmentTypeIndication</i>	Opcional
6. El lloc de producció de la signatura: <i>SignatureProductionPlace</i>	Opcional
7. El rol del signatari: <i>SignerRole</i>	Opcional
8. El segell de data i hora sobre el contingut: <i>AllDataObjectsTimeStamp</i> o <i>IndividualDataObjectsTimeStamp</i>	Opcional
9. La contrasignatura: <i>Reference</i> o <i>CounterSignature</i>	Opcional
10. Identificació de la política de signatura: <i>SignaturePolicyIdentifier</i>	Opcional ⁴⁸

⁴⁸ Depèn del tipus de signatura segellada.

11. Segell de data i hora de la signatura: SignatureTimeStamp	Obligatori ⁴⁹
12. Referències completes de certificats: CompleteCertificateRefs	Obligatori
13. Referències completes de revocació: CompleteRevocationRefs	Obligatori
14. Referències completes de certificats d'atributs: AttributeCertificateRefs	Obligatori ⁵⁰
15. Referències completes de revocació d'atributs: AttributeRevocationRefs	Obligatori ⁵¹
16. Segell de data i hora sobre la signatura completa: SigAndRefsTimeStamp	Obligatori ⁵²
17. Segell de data i hora sobre les referències de certificats i revocacions: RefsOnlyTimeStamp	Obligatori ⁵³
18. Valors de certificats: CertificateValues	Obligatori
19. Valors de revocació: RevocationValues	Obligatori
20. Valors de certificats d'atribut: AttrAuthoritiesCertsValues	Obligatori ⁵⁴
21. Valors de revocació de certificats d'atribut: AttributeRevocationValues	Obligatori ⁵⁵
22. Segell de data i hora d'arxiu: ArchiveTimeStamp	Obligatori

⁴⁹ Només és obligatori quan s'utilitza segellament criptogràfic de data i hora, enlloc de marcatge de data i hora.

⁵⁰ Només és obligatori quan s'utilitzen certificats d'atributs.

⁵¹ Només és obligatori quan s'utilitzen certificats d'atributs.

⁵² Només és obligatori quan la signatura electrònica d'arxiu es construeix sobre la signatura electrònica XAdES-X Long Type 1.

⁵³ Només és obligatori quan la signatura electrònica d'arxiu es construeix sobre la signatura electrònica XAdES-X Long Type 2.

⁵⁴ Només és obligatori quan s'utilitzen certificats d'atributs.

⁵⁵ Només és obligatori quan s'utilitzen certificats d'atributs.

Annex. La sintaxi de la signatura electrònica en XML

A continuació s'exposa la sintaxi XML completa, integrant els diferents elements de la normativa europea de signatura electrònica avançada.

Estructura de la signatura electrònica

```
<element name="Signature" type="ds:SignatureType"/>

<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Informació signada

```
<element name="SignedInfo" type="ds:SignedInfoType"/>

<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Mètode de canonicalització

```
<element name="CanonicalizationMethod"
```

```
type="ds:CanonicalizationMethodType"/>
```

```
<complexType name="CanonicalizationMethodType" mixed="true">
  <sequence>
    <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
    <!-- (0,unbounded) elements from (1,1) namespace -->
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

Mètode de signatura

```
<element name="SignatureMethod" type="ds:SignatureMethodType"/>

<complexType name="SignatureMethodType" mixed="true">
  <sequence>
    <element name="HMACOutputLength" minOccurs="0"
      type="ds:HMACOutputLengthType"/>
    <any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>
    <!-- (0,unbounded) elements from (1,1) external namespace -->
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

Referències als objectes signats

```
<element name="Reference" type="ds:ReferenceType"/>

<complexType name="ReferenceType">
  <sequence>
    <element ref="ds:Transforms" minOccurs="0"/>
    <element ref="ds:DigestMethod"/>
    <element ref="ds:DigestValue"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
  <attribute name="URI" type="anyURI" use="optional"/>
```

```
<attribute name="Type" type="anyURI" use="optional"/>
</complexType>

<element name="Transforms" type="ds:TransformsType"/>

<complexType name="TransformsType">
  <sequence>
    <element ref="ds:Transform" maxOccurs="unbounded"/>
  </sequence>
</complexType>

<element name="Transform" type="ds:TransformType"/>

<complexType name="TransformType" mixed="true">
  <choice minOccurs="0" maxOccurs="unbounded">
    <any namespace="##other" processContents="lax"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
    <element name="XPath" type="string"/>
  </choice>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>

<element name="DigestMethod" type="ds:DigestMethodType"/>

<complexType name="DigestMethodType" mixed="true">
  <sequence>
    <any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>

<element name="DigestValue" type="ds:DigestValueType"/>

<simpleType name="DigestValueType">
  <restriction base="base64Binary"/>
</simpleType>
```

```
</simpleType>
```

Valor de la signatura digital del signatari

```
<element name="SignatureValue" type="ds:SignatureValueType"/>

<complexType name="SignatureValueType">
  <simpleContent>
    <extension base="base64Binary">
      <attribute name="Id" type="ID" use="optional"/>
    </extension>
  </simpleContent>
</complexType>
```

Informació de claus de signatura

```
<element name="KeyInfo" type="ds:KeyInfoType"/>

<complexType name="KeyInfoType" mixed="true">
  <choice maxOccurs="unbounded">
    <element ref="ds:KeyName"/>
    <element ref="ds:KeyValue"/>
    <element ref="ds:RetrievalMethod"/>
    <element ref="ds:X509Data"/>
    <element ref="ds:PGPData"/>
    <element ref="ds:SPKIData"/>
    <element ref="ds:MgmtData"/>
    <any processContents="lax" namespace="##other"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </choice>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>

<element name="RetrievalMethod" type="ds:RetrievalMethodType"/>

<complexType name="RetrievalMethodType">
```

```
<sequence>
  <element ref="ds:Transforms" minOccurs="0"/>
</sequence>
<attribute name="URI" type="anyURI"/>
<attribute name="Type" type="anyURI" use="optional"/>
</complexType>

<element name="X509Data" type="ds:X509DataType"/>

<complexType name="X509DataType">
  <sequence maxOccurs="unbounded">
    <choice>
      <element name="X509IssuerSerial" type="ds:X509IssuerSerialType"/>
      <element name="X509SKI" type="base64Binary"/>
      <element name="X509SubjectName" type="string"/>
      <element name="X509Certificate" type="base64Binary"/>
      <element name="X509CRL" type="base64Binary"/>
      <any namespace="##other" processContents="lax"/>
    </choice>
  </sequence>
</complexType>

<complexType name="X509IssuerSerialType">
  <sequence>
    <element name="X509IssuerName" type="string"/>
    <element name="X509SerialNumber" type="integer"/>
  </sequence>
</complexType>
```

Objecte/s signat/s

```
<element name="Object" type="ds:ObjectType"/>

<complexType name="ObjectType" mixed="true">
  <sequence minOccurs="0" maxOccurs="unbounded">
    <any namespace="##any" processContents="lax"/>
  </sequence>
</complexType>
```

```
</sequence>
<attribute name="Id" type="ID" use="optional"/>
<attribute name="MimeType" type="string" use="optional"/>
<attribute name="Encoding" type="anyURI" use="optional"/>
</complexType>
```

Elements opcionals de la signatura XML

Manifest

```
<element name="Manifest" type="ds:ManifestType"/>

<complexType name="ManifestType">
  <sequence>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Propietats de signatura electrònica

```
<element name="SignatureProperties" type="ds:SignaturePropertiesType"/>

<complexType name="SignaturePropertiesType">
  <sequence>
    <element ref="ds:SignatureProperty" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>

<element name="SignatureProperty" type="ds:SignaturePropertyType"/>

<complexType name="SignaturePropertyType" mixed="true">
  <choice maxOccurs="unbounded">
    <any namespace="##other" processContents="lax"/>
    <!-- (1,1) elements from (1,unbounded) namespaces -->
```

```
</choice>
<attribute name="Target" type="anyURI" use="required"/>
<attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Elements addicionals de la signatura XML d'acord amb la Directiva europea

Propietats que qualifiquen la signatura

```
<xsd:element name="QualifyingProperties"
  type="QualifyingPropertiesType"/>

<xsd:complexType name="QualifyingPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedProperties" type="SignedPropertiesType"
      minOccurs="0"/>
    <xsd:element name="UnsignedProperties" type="UnsignedPropertiesType"
      minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Target" type="xsd:anyURI" use="required"/>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Propietats signades

```
<xsd:element name="SignedProperties" type="SignedPropertiesType" />

<xsd:complexType name="SignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedSignatureProperties"
      type="SignedSignaturePropertiesType"/>
    <xsd:element name="SignedDataObjectProperties"
      type="SignedDataObjectPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Propietats signades de signatura electrònica

```
<xsd:element name="SignedSignatureProperties"
  type="SignedSignaturePropertiesType" />

<xsd:complexType name="SignedSignaturePropertiesType">
  <xsd:sequence>
    <xsd:element name="SigningTime" type="xsd:dateTime"
      minOccurs="0"/>
    <xsd:element name="SigningCertificate" type="CertIDListType"
      minOccurs="0"/>
    <xsd:element name="SignaturePolicyIdentifer"
      type="SignaturePolicyIdentifierType" minOccurs="0"/>
    <xsd:element name="SignatureProductionPlace"
      type="SignatureProductionPlaceType" minOccurs="0"/>
    <xsd:element name="SignerRole" type="SignerRoleType"
      minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Propietats signades de l'objecte de dades

```
<xsd:element name="SignedDataObjectProperties"
  type="SignedDataObjectPropertiesType" />

<xsd:complexType name="SignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="DataObjectFormat" type="DataObjectFormatType"
      minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="CommitmentTypeIndication"
      type="CommitmentTypeIndicationType" minOccurs="0"
      maxOccurs="unbounded"/>
    <xsd:element name="AllDataObjectsTimeStamp"
      type="XAdESTimeStampType" />
  </xsd:sequence>
</xsd:complexType>
```

```
minOccurs="0" maxOccurs="unbounded" />
<xsd:element name="IndividualDataObjectsTimeStamp"
  type="XAdESTimeStampType" minOccurs="0" maxOccurs="unbounded" />
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
```

Propietats no signades

```
<xsd:element name="UnsignedProperties" type="UnsignedPropertiesType" />

<xsd:complexType name="UnsignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedSignatureProperties"
      type="UnsignedSignaturePropertiesType" minOccurs="0" />
    <xsd:element name="UnsignedDataObjectProperties"
      type="UnsignedDataObjectPropertiesType" minOccurs="0" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
```

Propietats no signades de signatura electrònica

```
<xsd:element name="UnsignedSignatureProperties"
  type="UnsignedSignaturePropertiesType" />

<xsd:complexType name="UnsignedSignaturePropertiesType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="CounterSignature" type="CounterSignatureType" />
    <xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType" />
    <xsd:element name="CompleteCertificateRefs"
      type="CompleteCertificateRefsType" />
    <xsd:element name="CompleteRevocationRefs"
      type="CompleteRevocationRefsType" />
    <xsd:element name="AttributeCertificateRefs"
      type="CompleteCertificateRefsType" />
```

```
<xsd:element name="AttributeRevocationRefs"
  type="CompleteRevocationRefsType" />
<xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType" />
<xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType" />
<xsd:element name="CertificateValues" type="CertificateValuesType" />
<xsd:element name="RevocationValues" type="RevocationValuesType" />
<xsd:element name="AttrAuthoritiesCertValues"
  type="CertificateValuesType" />
<xsd:element name="AttributeRevocationValues"
  type="RevocationValuesType" />
<xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType" />
<xsd:any namespace="##other" />
</xsd:choice>
<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
```

Propietats no signades de l'objecte de dades

```
<xsd:element name="UnsignedDataObjectProperties"
  type="UnsignedDataObjectPropertiesType" />

<xsd:complexType name="UnsignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedDataObjectProperty" type="AnyType"
      minOccurs="0" maxOccurs="unbounded" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
```

Referència a les propietats que qualifiquen la signatura

```
<xsd:element name="QualifyingPropertiesReference"
  type="QualifyingPropertiesReferenceType" />

<xsd:complexType name="QualifyingPropertiesReferenceType">
  <xsd:attribute name="URI" type="xsd:anyURI" use="required" />
```

```
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

Data i hora de la signatura electrònica

```
<xsd:element name="SigningTime" type="xsd:dateTime"/>
```

Contrasignatura

```
<xsd:element name="CounterSignature" type="CounterSignatureType" />
```

```
<xsd:complexType name="CounterSignatureType">
```

```
  <xsd:sequence>
```

```
    <xsd:element ref="ds:Signature"/>
```

```
  </xsd:sequence>
```

```
</xsd:complexType>
```

Certificat emprat per signar

```
<xsd:element name="SigningCertificate" type="CertIDListType"/>
```

```
<xsd:complexType name="CertIDListType">
```

```
  <xsd:sequence>
```

```
    <xsd:element name="Cert" type="CertIDType" maxOccurs="unbounded"/>
```

```
  </xsd:sequence>
```

```
</xsd:complexType>
```

```
<xsd:complexType name="CertIDType">
```

```
  <xsd:sequence>
```

```
    <xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
```

```
    <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
```

```
  </xsd:sequence>
```

```
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
```

```
</xsd:complexType>
```

```
<xsd:complexType name="DigestAlgAndValueType">
```

```
<xsd:sequence>
  <xsd:element ref="ds:DigestMethod"/>
  <xsd:element ref="ds:DigestValue"/>
</xsd:sequence>
</xsd:complexType>
```

Identificador de la política de signatura electrònica

```
<xsd:element name="SignaturePolicyIdentifier"
  type="SignaturePolicyIdentifierType"/>

<xsd:complexType name="SignaturePolicyIdentifierType">
  <xsd:choice>
    <xsd:element name="SignaturePolicyId" type="SignaturePolicyIdType"/>
    <xsd:element name="SignaturePolicyImplied"/>
  </xsd:choice>
</xsd:complexType>

<xsd:complexType name="SignaturePolicyIdType">
  <xsd:sequence>
    <xsd:element name="SigPolicyId" type="ObjectIdentifierType"/>
    <xsd:element ref="ds:Transforms" minOccurs="0"/>
    <xsd:element name="SigPolicyHash" type="DigestAlgAndValueType"/>
    <xsd:element name="SigPolicyQualifiers"
      type="SigPolicyQualifiersListType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SigPolicyQualifiersListType">
  <xsd:sequence>
    <xsd:element name="SigPolicyQualifier" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:element name="SPURI" type="xsd:anyURI"/>
```

```
<xsd:element name="SPUserNotice" type="SPUserNoticeType"/>

<xsd:complexType name="SPUserNoticeType">
  <xsd:sequence>
    <xsd:element name="NoticeRef" type="NoticeReferenceType"
      minOccurs="0"/>
    <xsd:element name="ExplicitText" type="xsd:string"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NoticeReferenceType">
  <xsd:sequence>
    <xsd:element name="Organization" type="xsd:string"/>
    <xsd:element name="NoticeNumbers" type="IntegerListType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IntegerListType">
  <xsd:sequence>
    <xsd:element name="int" type="xsd:integer" minOccurs="0"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Format de l'objecte de dades signat

```
<xsd:element name="DataObjectFormat" type="DataObjectFormatType"/>

<xsd:complexType name="DataObjectFormatType">
  <xsd:sequence>
    <xsd:element name="Description" type="xsd:string" minOccurs="0"/>
    <xsd:element name="ObjectIdentifier" type="ObjectIdentifierType"
      minOccurs="0"/>
    <xsd:element name="MimeType" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

```
<xsd:element name="Encoding" type="xsd:anyURI" minOccurs="0"/>
</xsd:sequence>
<xsd:attribute name="ObjectReference" type="xsd:anyURI"
  use="required"/>
</xsd:complexType>
```

Indicació del tipus de compromís del signatari

```
<xsd:element name="CommitmentTypeIndication"
  type="CommitmentTypeIndicationType"/>

<xsd:complexType name="CommitmentTypeIndicationType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeId" type="ObjectIdentifierType"/>
    <xsd:choice>
      <xsd:element name="ObjectReference" ObjectReference"
        type="xsd:anyURI" maxOccurs="unbounded"/>
      <xsd:element name="AllSignedDataObjects"/>
    </xsd:choice>
    <xsd:element name="CommitmentTypeQualifiers"
      type="CommitmentTypeQualifiersListType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CommitmentTypeQualifiersListType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeQualifier"
      type="AnyType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Lloc de producció de la signatura

```
<xsd:element name="SignatureProductionPlace"
  type="SignatureProductionPlaceType"/>
```

```
<xsd:complexType name="SignatureProductionPlaceType">
  <xsd:sequence>
    <xsd:element name="City" type="xsd:string" minOccurs="0"/>
    <xsd:element name="StateOrProvince" type="xsd:string"
      minOccurs="0"/>
    <xsd:element name="PostalCode" type="xsd:string" minOccurs="0"/>
    <xsd:element name="CountryName" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

Rol del signatari

```
<xsd:element name="SignerRole" type="SignerRoleType"/>

<xsd:complexType name="SignerRoleType">
  <xsd:sequence>
    <xsd:element name="ClaimedRoles" type="ClaimedRolesListType"
      minOccurs="0"/>
    <xsd:element name="CertifiedRoles" type="CertifiedRolesListType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ClaimedRolesListType">
  <xsd:sequence>
    <xsd:element name="ClaimedRole" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CertifiedRolesListType">
  <xsd:sequence>
    <xsd:element name="CertifiedRole" type="EncapsulatedPKIDataType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Segell de data i hora sobre tots els objectes de dades signats

```
<xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType"/>
```

Segell de data i hora sobre un objecte de dades individual signat

```
<xsd:element name="IndividualDataObjectsTimeStamp"  
  type="XAdESTimeStampType"/>
```

Segell de data i hora sobre la signatura

```
<xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>
```

Referències completes dels certificats

```
<xsd:element name="CompleteCertificateRefs"  
  type="CompleteCertificateRefsType"/>  
  
<xsd:complexType name="CompleteCertificateRefsType">  
  <xsd:sequence>  
    <xsd:element name="CertRefs" type="CertIDListType" />  
  </xsd:sequence>  
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>  
</xsd:complexType>
```

Referències completes a la informació de revocació de certificats

```
<xsd:element name="CompleteRevocationRefs"  
  type="CompleteRevocationRefsType"/>  
  
<xsd:complexType name="CompleteRevocationRefsType">  
  <xsd:sequence>  
    <xsd:element name="CRLRefs" type="CRLRefsType" minOccurs="0"/>  
    <xsd:element name="OCSPRefs" type="OCSPRefsType" minOccurs="0"/>  
    <xsd:element name="OtherRefs" type="OtherCertStatusRefsType"
```

```
minOccurs="0"/>
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<xsd:complexType name="CRLRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRef" type="CRLRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLRefType">
  <xsd:sequence>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"/>
    <xsd:element name="CRLIdentifier" type="CRLIdentifierType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLIdentifierType">
  <xsd:sequence>
    <xsd:element name="Issuer" type="xsd:string"/>
    <xsd:element name="IssueTime" type="xsd:dateTime" />
    <xsd:element name="Number" type="xsd:integer" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="OCSPRefsType">
  <xsd:sequence>
    <xsd:element name="OCSPRef" type="OCSPRefType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OCSPRefType">
```

```
<xsd:sequence>
  <xsd:element name="OCSPIdentifier" type="OCSPIdentifierType"/>
  <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"
    minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

```
<xsd:complexType name="ResponderIDType">
  <xsd:choice>
    <xsd:element name="ByName" type="xsd:string"/>
    <xsd:element name="ByKey" type="xsd:base64Binary"/>
  </xsd:choice>
</xsd:complexType>
```

```
<xsd:complexType name="OCSPIdentifierType">
  <xsd:sequence>
    <xsd:element name="ResponderID" type="ResponderIDType"/>
    <xsd:element name="ProducedAt" type="xsd:dateTime"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>
```

```
<xsd:complexType name="OtherCertStatusRefsType">
  <xsd:sequence>
    <xsd:element name="OtherRef" type="AnyType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Referències completes dels certificats d'atributs

```
<xsd:element name="AttributeCertificateRefs"
  type="CompleteCertificateRefsType"/>
```

Referències completes de la informació de revocació d'atributs

```
<xsd:element name="AttributeRevocationRefs"
```

```
type="CompleteRevocationRefsType"/>
```

Segell de data i hora sobre la signatura completa

```
<xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
```

Segell de data i hora sobre les referències de certificats i revocacions

```
<xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>
```

Valors dels certificats

```
<xsd:element name="CertificateValues" type="CertificateValuesType"/>
```

```
<xsd:complexType name="CertificateValuesType">
```

```
  <xsd:choice minOccurs="0" maxOccurs="unbounded">
```

```
    <xsd:element name="EncapsulatedX509Certificate"
```

```
      type="EncapsulatedPKIDataType"/>
```

```
    <xsd:element name="OtherCertificate" type="AnyType"/>
```

```
  </xsd:choice>
```

```
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
```

```
</xsd:complexType>
```

Valors de certificats d'atributs

```
<xsd:element name="AttrAuthoritiesCertValues"
```

```
  type="CertificateValuesType"/>
```

Valors de les revocacions

```
<xsd:element name="RevocationValues" type="RevocationValuesType"/>
```

```
<xsd:complexType name="RevocationValuesType">
```

```
  <xsd:sequence>
```

```
    <xsd:element name="CRLValues" type="CRLValuesType"
```

```
      minOccurs="0"/>
```

```
<xsd:element name="OCSPValues" type="OCSPValuesType" minOccurs="0"/>
<xsd:element name="OtherValues" type="OtherCertStatusValuesType"
  minOccurs="0"/>
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<xsd:complexType name="CRLValuesType">
  <xsd:sequence>
    <xsd:element name="EncapsulatedCRLValue"
      type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OCSPValuesType">
  <xsd:sequence>
    <xsd:element name="EncapsulatedOCSPValue"
      type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OtherCertStatusValuesType">
  <xsd:sequence>
    <xsd:element name="OtherValue" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

Valors de revocació d'atributs

```
<xsd:element name="AttributeRevocationValues"
  type="RevocationValuesType"/>
```

Segell de data i hora d'arxiu

```
<xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>
```



Agència Catalana
de Certificació

Guia de sintaxi i formats de signatura electrònica - Part 2: Signatura XML
