Digital Certificates. PKI and other TTPs.

3.3

Universidad Carlos III de Madrid
Grupo SeTI · Dpto. Informática

Certification-service providers

Spanish Law 59/03 Art. 2.2 or Directive 1999/93/EC Art. 2.11:

"Certification-service providers"

means an entity or a legal or natural person who issues electronic certificates or provides other services related to electronic signatures.

Certification Service Providers

What Services?

- Key Certification
- **Digital time stamping**
- Key deposit
- Key directory
- etc...

Trusted third parties

Def.:

Independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers.

Digital time stamping

- Timestamp service is provided by a trusted third party known as Time Stamp Authority.
- Specify time and date → bind securely to a message
- It can be proven that a data item existed before a certain point in time.

Digital time stamping

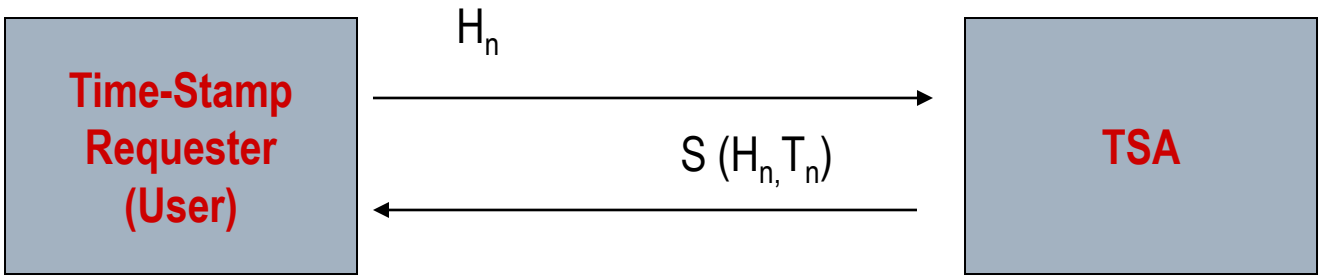
- Applications to PKI as lifetime extension of digital signature
  - Provides support for non-repudiation
  - As certificates are revoked due to their loss, or eventually expire, digital signatures cannot be allowed to suddenly become invalid
  - A Trusted Time-Stamping Service can provide a trusted time anchor
    - Certifying that a certain a document has been signed while the signatory's certificate was valid
    - Otherwise, it is easy to repudiate signatures in the future, cancelling validity of contracts etc.

Digital time stamping

- Classification of time-stamping schemes:
  - simple schemes
  - linking schemes
  - distributed schemes
  - trusted archival

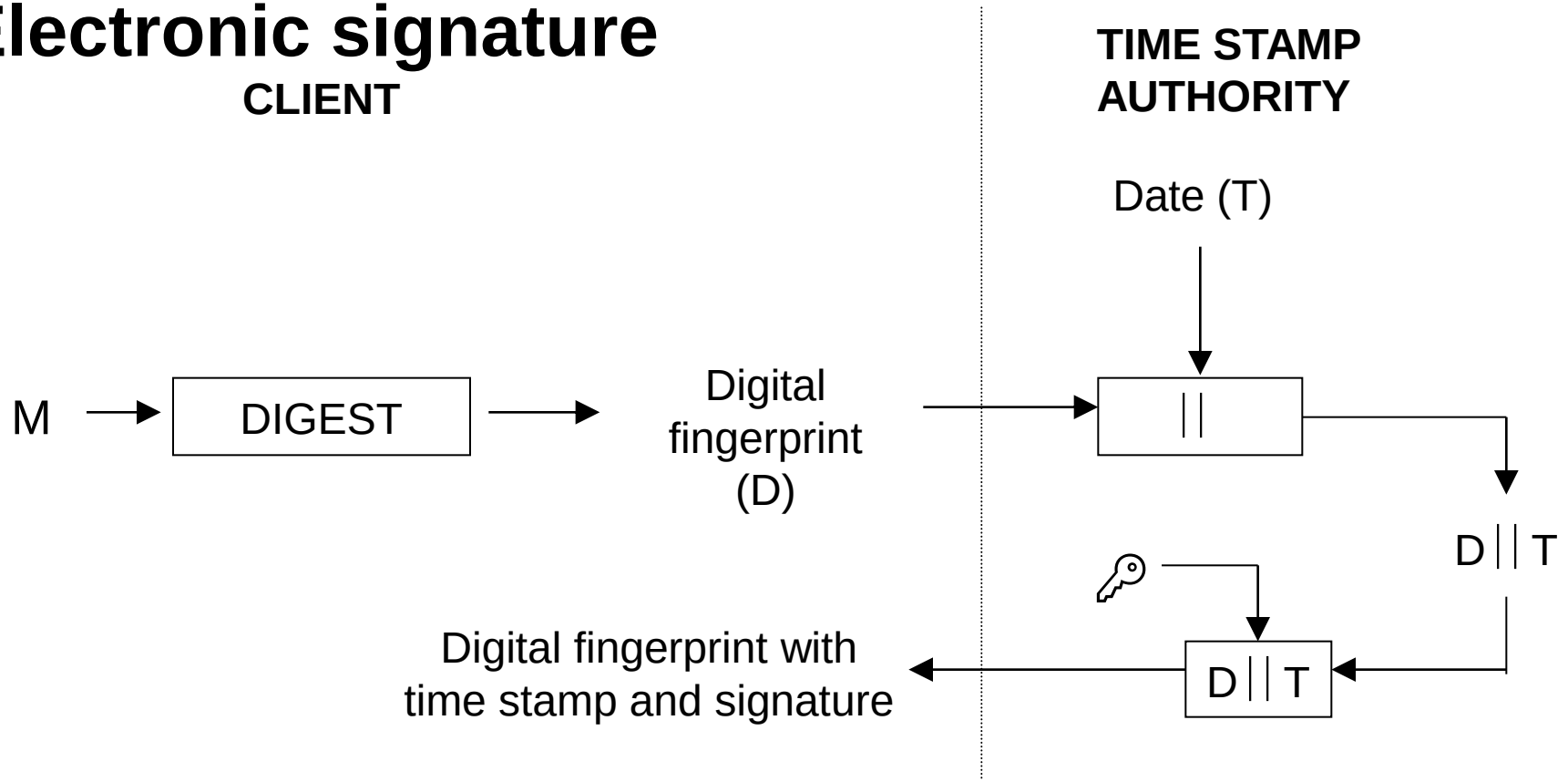
Digital time stamping

- Simple:
  - Independent time-stamps (TS)
  - Example: digital signature on pair (time, document)



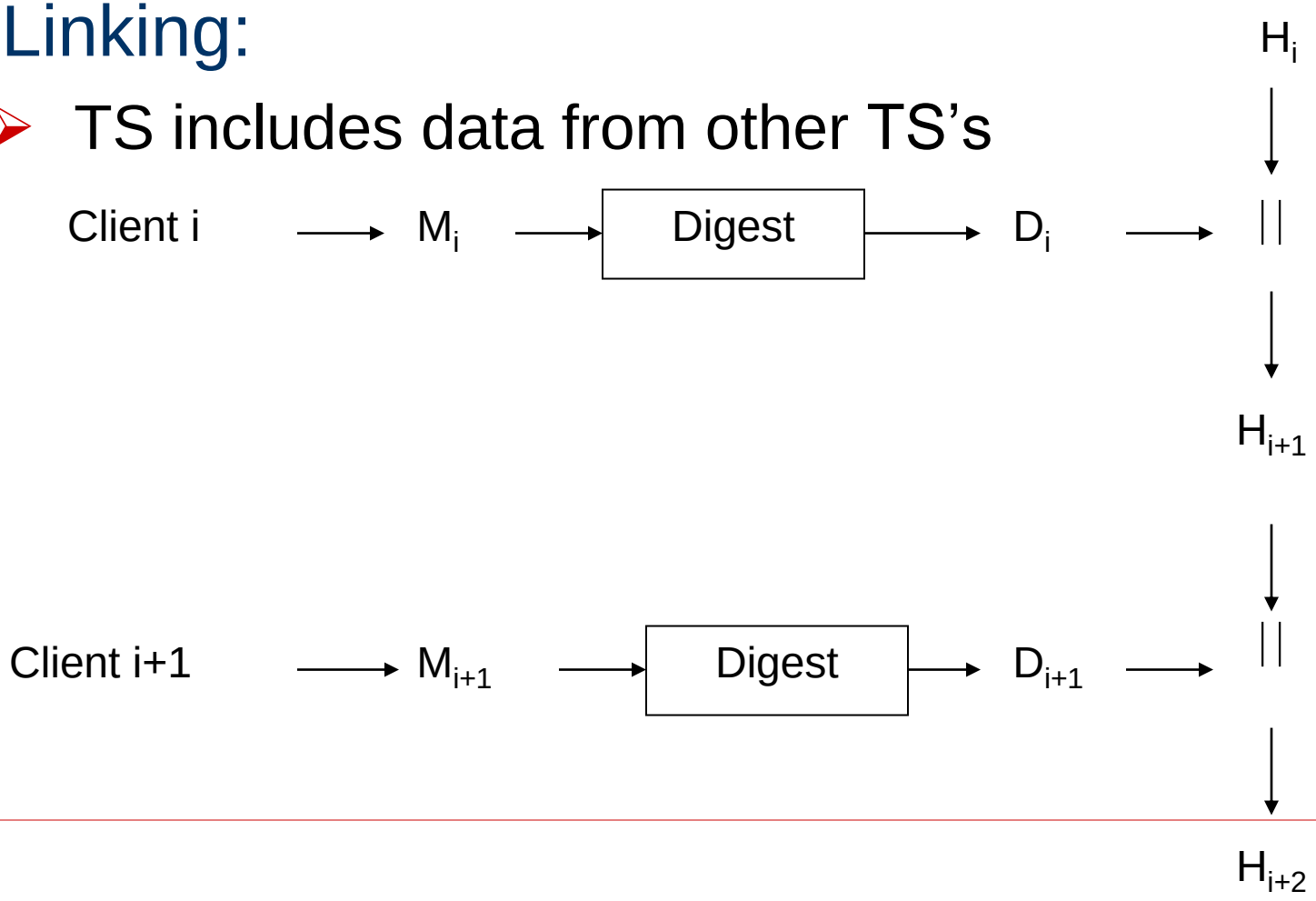
Digital time stamping

Electronic signature



Digital time stamping

- Linking:
  - TS includes data from other TS's



Digital time stamping

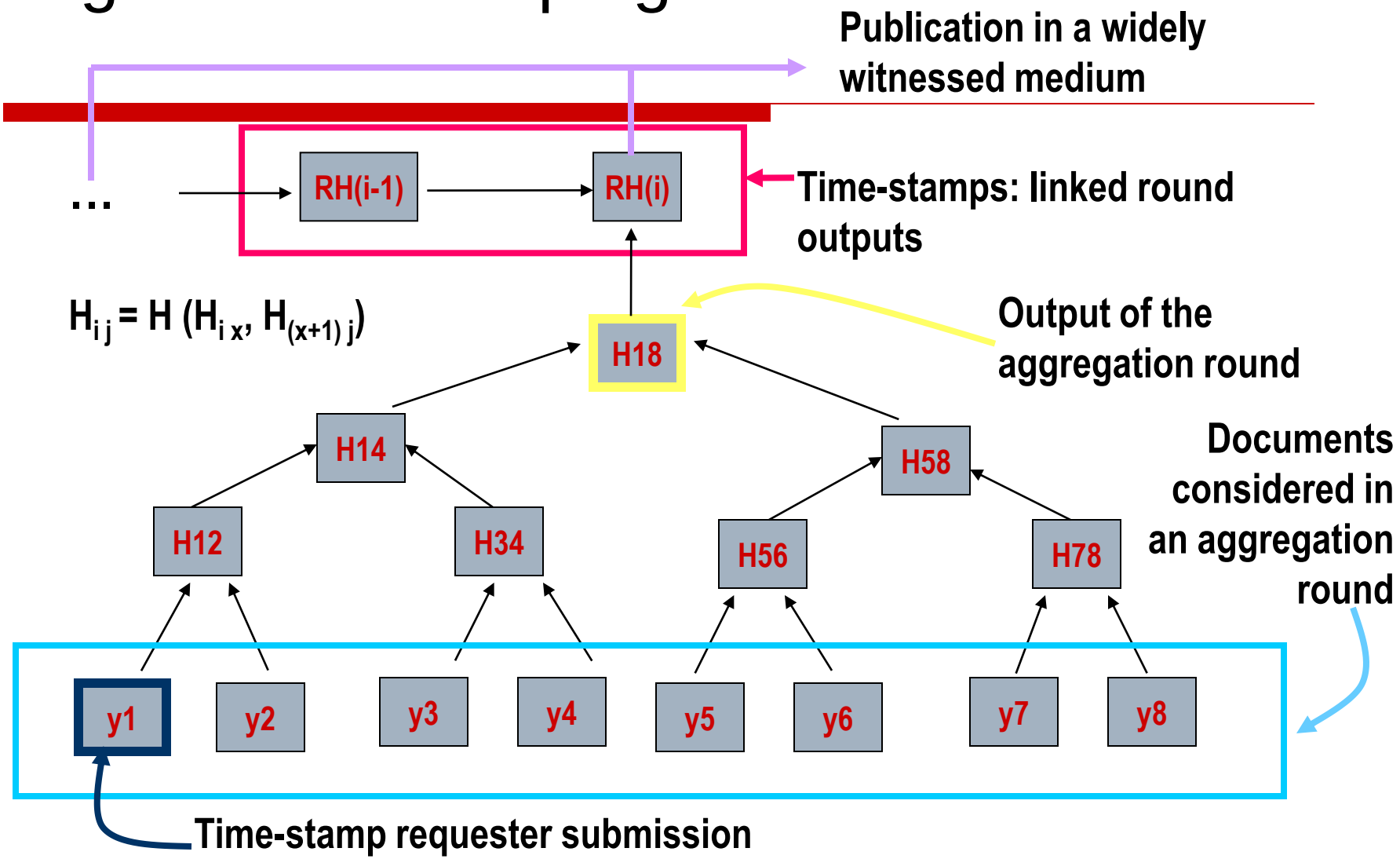
- Linking (general scheme):
  - **Aggregation**:

    all documents received in a small time interval –the aggregation round - are considered simultaneously and the output depends on all them
  - **Linking**:

    output of the aggregation round is taken and linked to previous aggregation round values
  - **Publication:**

    TSA publishes periodically the most recent TS in a widely-witnessed medium, committing itself to all the previous issued ones

Digital time stamping



Digital time stamping

- Distributed:
  - Multiple users/TSAs cooperate to generate a TS, possibly using a secure distribution of secret data
- Other:
  - Not all the timestamping schemes can be classified into these three sections

Digital time stamping

- IETF
  - **PKIX-TSP** (RFC 3161) PKIX Time-Stamp Protocol

    Describes a format of a request sent to a TSA and the returned response. Also it establishes several security relevant requirements to TSA operation.

Digital time stamping

- ETSI
  - **ETSI TS 102 023**: Policy requirements for time-stamping authorities
  - **ETSI TS 101 861**: Time stamping profile

Digital time stamping

- ISO
  - **ISO/IEC 18014-1**: Time-stamping services framework
  - **ISO/IEC 18014-2:** Mechanisms producing independent tokens
  - **ISO/IEC 18014-3:** Mechanisms producing linked tokens

Digital time stamping

- Synchronization with trusted time servers
  - Network time protocol (NTP)
    - UDP Protocol
    - Port 123

Digital time stamping

Processes

- Time stamp
- Verification
- **Renewal**

Electronic signature

'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

Qualified electronic signatures

Qualified electronic signatures:

Requirements of electronic signatures to have the same legal effects as the hand-written signature (and so, to be admissible as evidence in legal proceedings):

- Be an advanced signature
- Be based upon a qualified certificate
- Have been generated by a secure signature creation device

Advanced electronic signature

- ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
  - (a) it is uniquely linked to the signatory;
  - (b) it is capable of identifying the signatory;
  - (c) it is created using means that the signatory can maintain under his sole control; and
  - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

Qualified certificates

Law 59/03 Art. 11.1:

The electronic certificates which are issued by a certification-service provider are qualified certificates, when the provider fulfils the requisites established in this law as regards verification of identity and other circumstances of the applicants and the reliability and guarantees of provided certification services.

Qualified certificates

Law 59/03 Art. 11.2 or Directive 1999/93/EC Annex I:

Qualified certificates must contain:

1. an indication that the certificate is issued as a qualified certificate;
2. a unique identity code of the certificate;
3. the identification of the CSP (cert. service provider) and State in which it is established;
4. the advanced electronic signature of the CSP issuing it;
5. The name of the signatory or a pseudonym, which should be identified as such;

Qualified certificates

6. signature verification data which correspond to signature creation under the control of the signatory;
7. an indication of the beginning and end of the period of validity of the certificate;
8. limitations on the scope of use of the certificate, if applicable; and
9. limits on the value of transactions for which the certificate can be used, if applicable.

XML Digital Signature (XMLDSig)

- Authentication, data integrity, non-repudiation
- Joint W3C/IETF effort
  - XML syntax for representing signature of web resources and portions thereof
  - Procedures for computing and verifying such signatures
  - Canonicalization of XML data
  - Trust in key is out-of-scope
- W3C Recommendation + IETF RFC 3075
- JSR-105: XML Digital Signature APIs

XML Digital Signature (XMLDSig)

- Signature of digital content is a two-stage process
  - First, the digital content is digested and the resulting value is placed in an XML element
  - Second, the digested value is picked and signed
- After the XML (or some part thereof) is digitally signed, the resulting XML signature is represented as an XML element that is identified as <Signature>

XML Digital Signature (XMLDSig)

- The original content is related to the digital signature based on these XML signature type definitions:
  - **Enveloping signature**: The <Signature> element includes the element that is digitally signed. The digitally signed element becomes the child of the <Signature> element
  - **Enveloped signature**: The <Signature> element becomes a child element of the data being signed. The <Signature> element refers to the signed element by using information in its <Reference> element
  - **Detached signature**: The <Signature> element and the signed element are kept separate

XML Digital Signature (XMLDSig)

- In addition to a reference to the digital content being signed, the <Signature> element includes information about the following:
  - The method used to canonicalize the digital content
  - The algorithm used to generate the signature for the canonicalized element to be signed
  - Additional information that specifies how to process the element to be signed before it is digested

XML Digital Signature (XMLDSig)

- Signature
  - SignedInfo
    - CanonicalizationMethod
    - SignatureMethod
    - Reference
      - Transforms
      - DigestMethod
      - DigestValue
  - SignatureValue
  - KeyInfo

XML Digital Signature (XMLDSig)

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2000/..." />
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="#PurchaseOrder">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>qZk+nkcGcWq6piVxeFdcbJzQ2JO=</DigestValue>
    </Reference>
  </SignedInfo>

  <SignatureValue>
   IWijxQjUrcXBYc0ei4QxjWo9Kg8Dep9tlWoT4SdeRT87GH03dgh
  </SignatureValue>

  <KeyInfo>
     <X509Data>
       <X509SubjectName>CN=Alice Smith, STREET=742 Park Avenue,
        L=New York, ST=NY, C=US</X509SubjectName>
     </X509Data>
  </KeyInfo>

</Signature>
```

A certificate can be included with public key
<X509Certificate>MIID5jCCA0+gA...lVN</X509Certificate>

Enhanced electronic signatures

Classes of signature:	**General electronic signature** as required in 5.2	**Qualified electronic signature -** as specified in 5.1 (Annex I, II, III)	**Enhanced electronic signature** (applicable to both general and qualified electronic signatures)
Level of legal certainty:	Can not be denied legal effect (art 5.2)	Same legal effect as hand-written signature (art 5.1)	Enhancement of technical evidence
Explanation:	Any electronic signature that is not a qualified electronic signature.	Minimum technical level required for the signer so that his electronic signature can be considered as legally equivalent with a hand-written signature.	Additional technical requirements for a verifier, such as time-stamping, but also for the signer, to enhance technical security and obtain protection against certain threats.

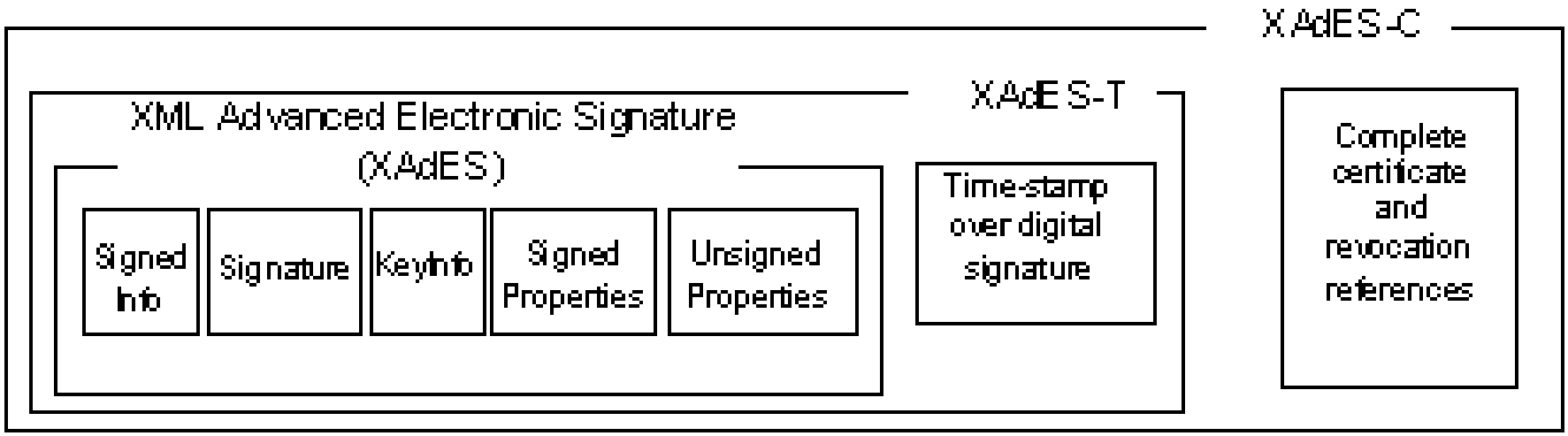
XML Advanced Electronic Signatures (XAdES)

- **ETSI TS 101 903** + W3C Specification (http://www.w3.org/TR/XAdES/)
- Defines XML formats for advanced electronic signatures that remain valid over long periods
  - compliant with the European Directive 1999/93/EC
  - incorporate additional useful information in common uses cases (includes evidence as to its validity even if the signer or verifying party later attempts to deny the validity of the signature)
- Provides for really usable signatures

XML Advanced Electronic Signatures (XAdES)

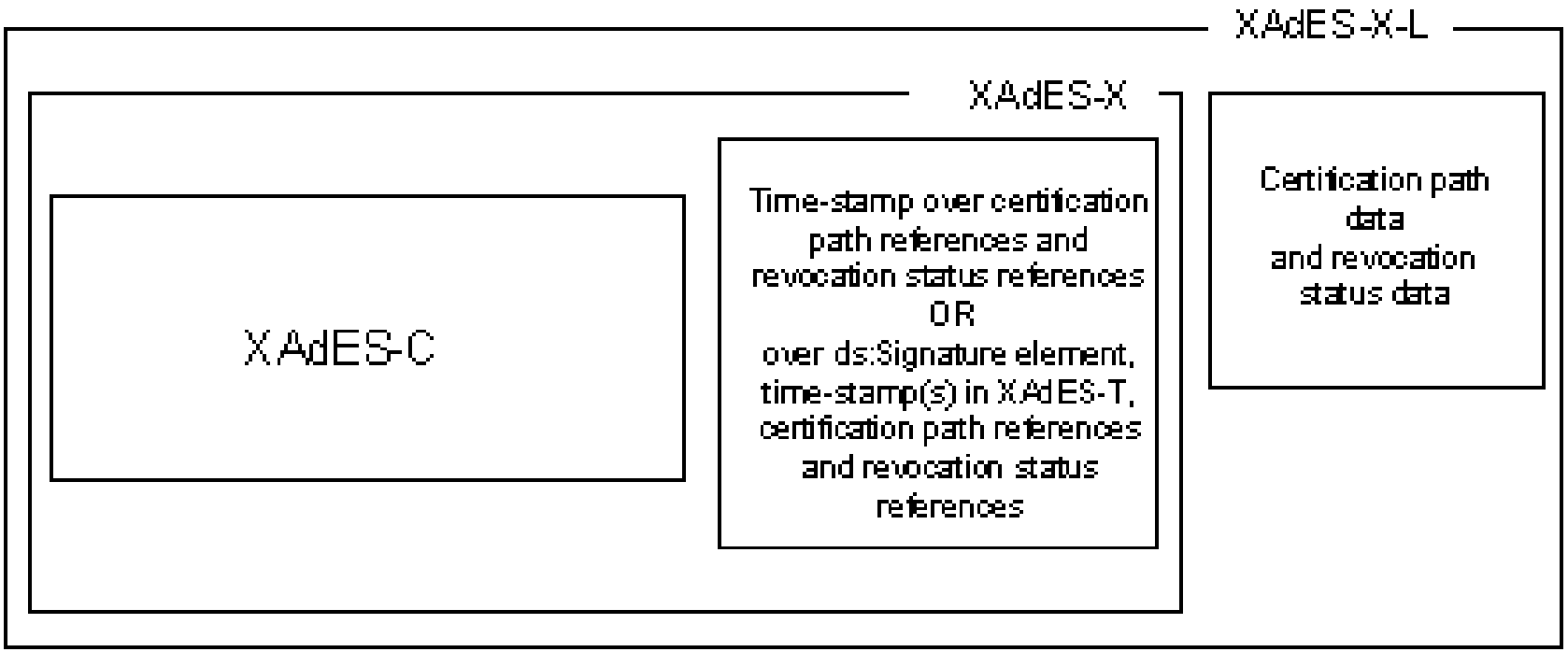
- XAdES formalises 6 types of signatures and specifies roles and their responsibilities
- It builds on XMLDSIG in following ways:
  - XAdES-BES (Basic Electronic Signature)
  - XAdES-EPES (Explicit Policy Electronic Signature)
  - XAdES-T (with Time Stamp)
  - XAdES-C (Complete Validation Data)
  - XAdES-X (Extended Validation Data)
  - XAdES-XL (Extended Long Validation Data)
  - XAdES-A (Archival)

XML Advanced Electronic Signatures (XAdES)



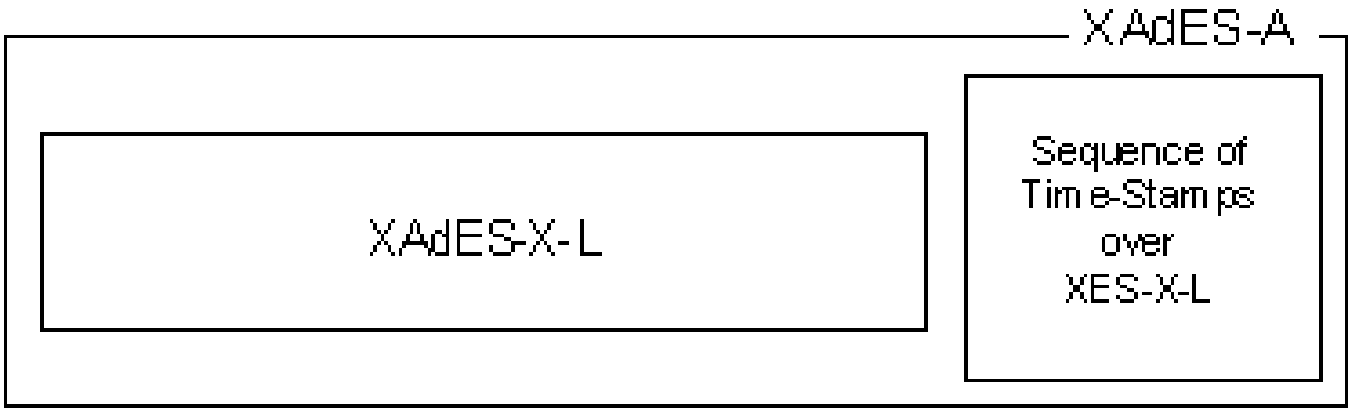
Source: W3C XAdES 2003

XML Advanced Electronic Signatures (XAdES)



Source: W3C XAdES 2003

XML Advanced Electronic Signatures (XAdES)



Source: W3C XAdES 2003

Electronic invoices

Def.:

e-Invoice is an electronic harmonized trade document, or instruction, that details the goods sent / services delivered or goods received / services obtained with a statement of the due and payable amount together with a statement of any Value Added Taxes applicable. It is transmitted through electronic means from the seller to the buyer. Its **authenticity and integrity** are preserved.

Electronic invoices

- A relatively complex format is needed (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg or txt)
  - Facturae format (www.facturae.es)
- It must guarantee the e-invoice's integrity and authenticity
  - **Qualified electronic signatures** fulfill this requirement
- It must reflect the consent of both parties (issuer and receiver)