

**Open Standards Forum 2008:**

Security Challenges for the Information Society

30 September - 3 October | Ditton Manor, Near London



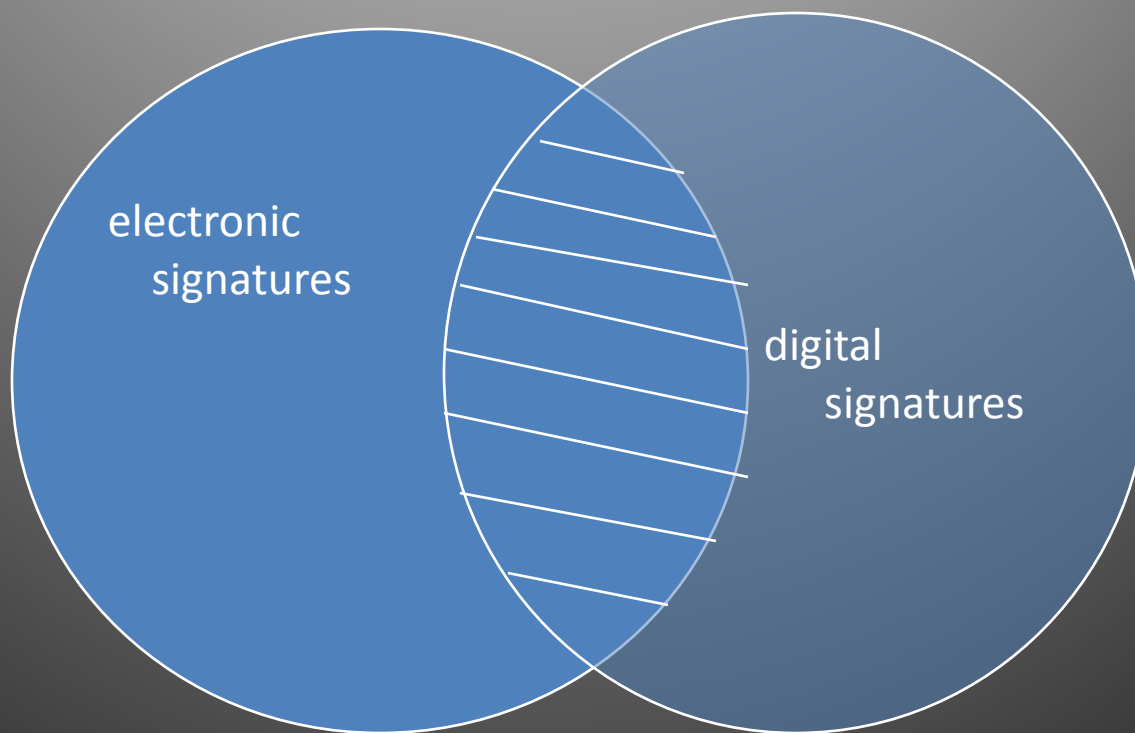
# Digital Signatures

## A Legal View

Jos Dumortier  
Professor of Law – University of Leuven/Belgium  
Attorney at Law – time.lex – Bar of Brussels

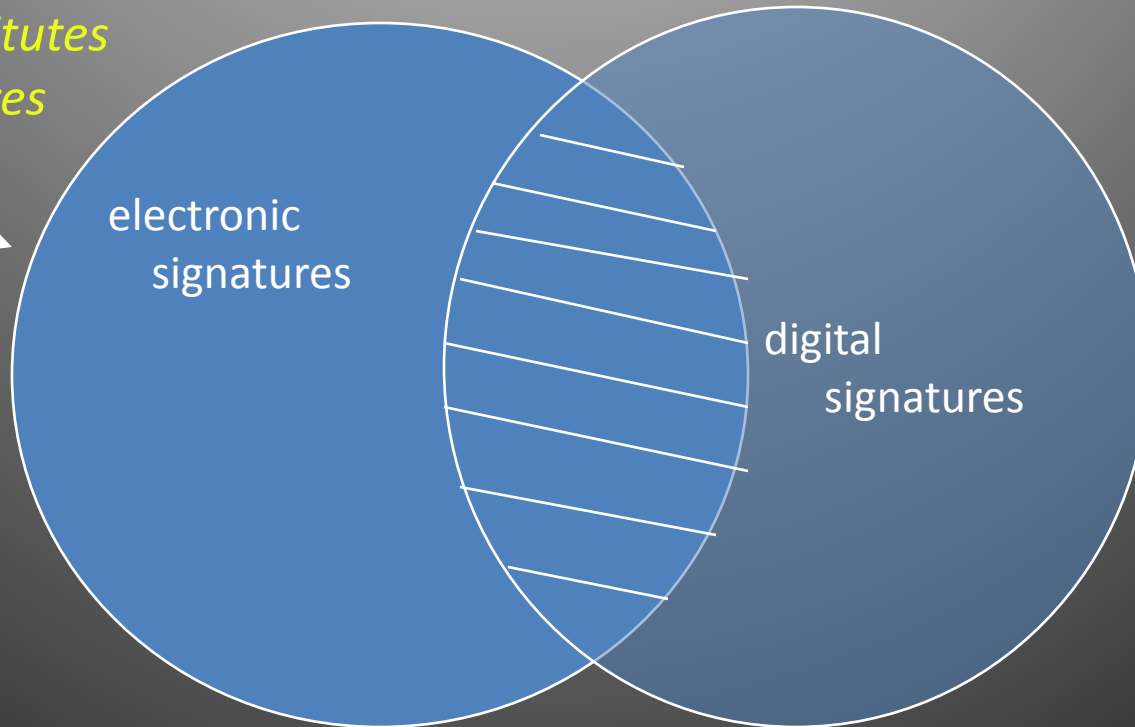


# Terminology



# Terminology

*all kinds of substitutes  
for legal signatures*



# Terminology

*all kinds of substitutes  
for legal signatures*

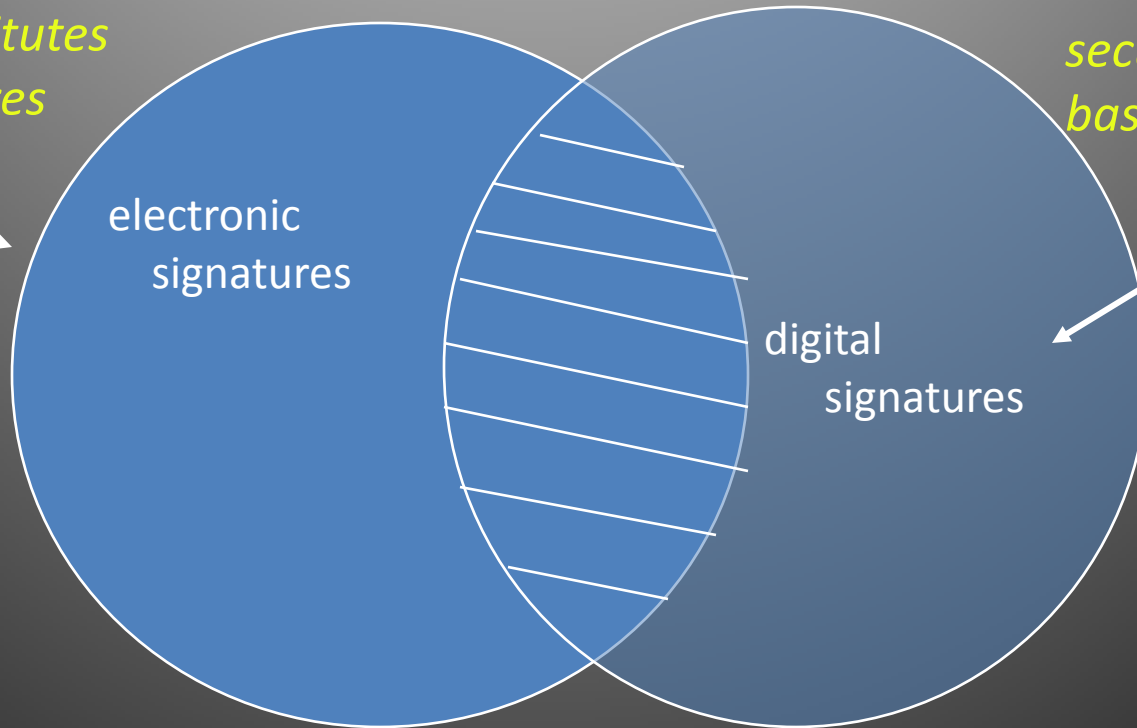


electronic  
signatures

*security technology  
based on PKI*



digital  
signatures



# Terminology

*all kinds of substitutes  
for legal signatures*



electronic  
signatures

*security technology  
based on PKI*

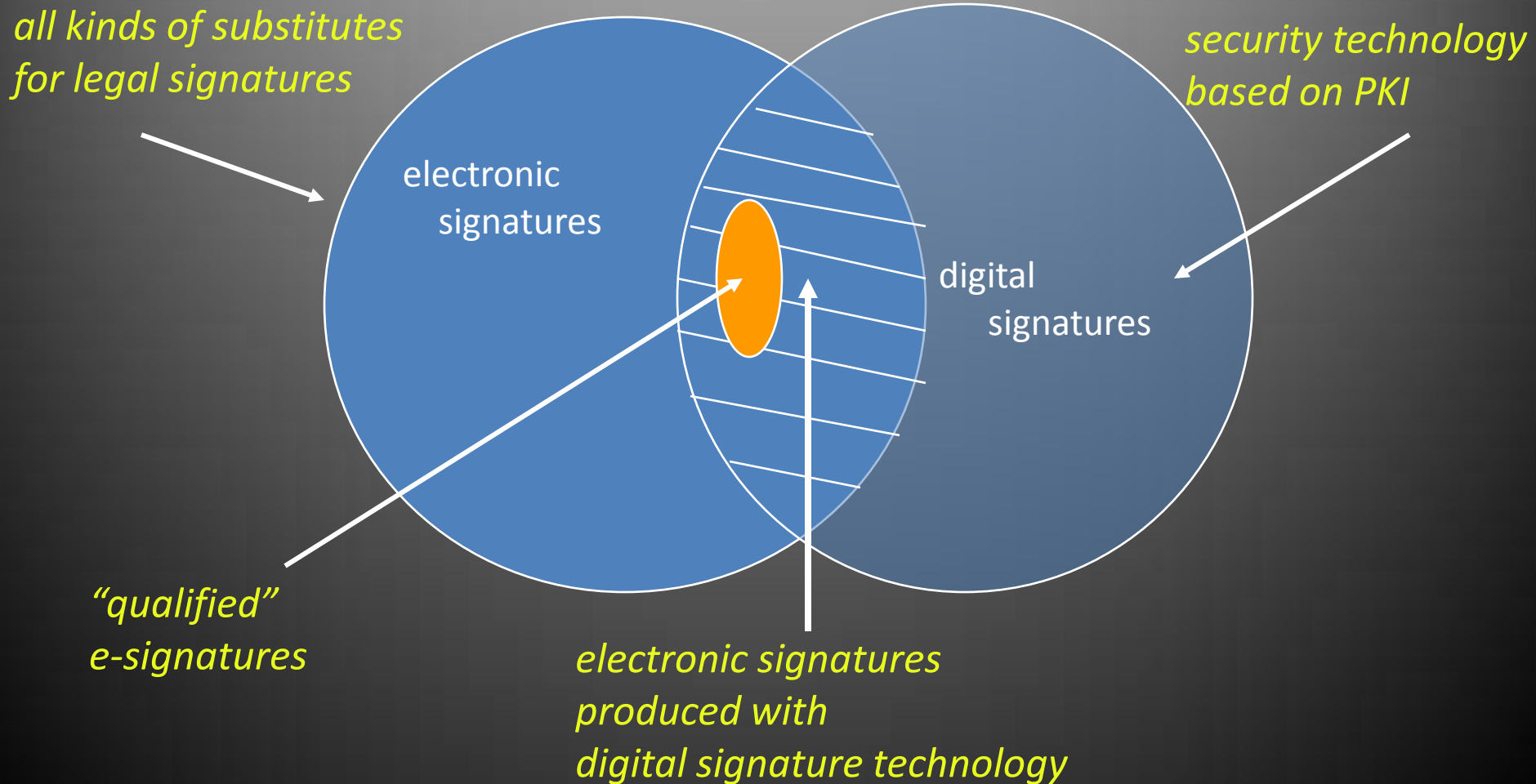


digital  
signatures

*electronic signatures  
produced with  
digital signature technology*



# Terminology



# Summary

1. Legal provisions related to digital signature technology
2. Legal provisions related to electronic signatures by means of digital signature technology
3. Legal provisions related to electronic signatures (in general)

# 1. Legal provisions on “digital signature technology”



# Digital Signature Technology

- “Making use of public key cryptography to secure the origin and the integrity of data”
- Legal provisions (typically newer ones) impose the usage of digital signature technology
- (European) example: electronic invoices
  - Electronic invoices have to be secured by means of digital signature technology
  - But it is prohibited for EU Member States to require invoices to be signed

# European VAT Directive 2006

L 347/44

EN

Official Journal of the European Union

11.12.2006

customer in cases other than those referred to in point (4) of Article 226.

## *Article 228*

Member States in whose territory goods or services are supplied may allow some of the compulsory details to be omitted from documents or messages treated as invoices pursuant to Article 219.

## *Article 229*

Member States shall not require invoices to be signed.

## *Article 230*

The amounts which appear on the invoice may be expressed in any currency provided that the amount of VAT payable is

of 19 October 1994 relating to the legal aspects of electronic data interchange <sup>(2)</sup>, if the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data.

Invoices may, however, be sent or made available by other electronic means, subject to acceptance by the Member States concerned.

2. For the purposes of point (a) of the first subparagraph of paragraph 1, Member States may also ask for the advanced electronic signature to be based on a qualified certificate and created by a secure-signature-creation device, within the meaning of points (6) and (10) of Article 2 of Directive 1999/93/EC.

2. For the purposes of point (4) of the first subparagraph of

# European VAT Directive 2006

## Article 232

Invoices issued pursuant to Section 2 may be sent on paper or, subject to acceptance by the recipient, they may be sent or made available by electronic means.

Member States may lay down specific conditions for invoices issued by electronic means in respect of goods or services supplied in their territory from a country with which no legal instrument exists relating to mutual assistance similar in scope to that provided for in Directive 76/308/EEC and Regulation (EC) No 1798/2003.

## Article 233

1. Invoices sent or made available by electronic means shall be accepted by Member States provided that the authenticity of the origin and the integrity of their content are guaranteed by one of the following methods:

(a) by means of an advanced electronic signature within the meaning of point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures <sup>(1)</sup>;

(b) by means of electronic data interchange (EDI), as defined in Article 2 of Commission Recommendation 1994/820/EC

<sup>(1)</sup> OJ L 13, 19.1.2000, p. 12.

<sup>(2)</sup> OJ L 338, 28.12.1994, p. 98.

## Article 236

Where batches containing several invoices are sent or made available to the same recipient by electronic means, the details common to the individual invoices may be mentioned only once if, for each invoice, all the information is accessible.

## Article 237

The Commission shall present, at the latest on 31 December 2008, a report and, if appropriate, a proposal amending the conditions applicable to electronic invoicing in order to take account of future technological developments in that field.

# European VAT Directive 2006

Conclusion: Electronic invoices

- should not be signed
- but should be secured by means  
of digital signature technology

# Confusion

- Legal provisions often use the term “electronic signature” when referring to “digital signature technology”
- Europe: “advanced electronic signature”

# “Advanced Electronic Signature”

- 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;*
- d) *it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable”.*

## Other example: European Directive on Vehicle Registration Certificates

“Write access is permitted only after an asymmetric authentication with session key exchange for protecting the session between the vehicle registration card and a security module (e.g. a security module card) of the national competent authorities (or their authorised agencies). Thereby card verifiable certificates according to ISO/IEC 7816-8 are exchanged before the authentication process. The card verifiable certificates contain the corresponding public keys to be retrieved and to be used in the following authentication process. These certificates are signed by the national competent authorities and contain an authorisation object (certificate holder authorisation) according to ISO/IEC 7816-9 in order to encode role specific authorisation to the card. (...)”

The security assurance has to be approved by common criteria evaluation according to EAL4+. The augmentations are as follows: 1. AVA\_MSU.3 Analysis and testing for insecure states; 2. AVA\_VLA.4 Highly resistant (...)”

# Terminology

*all kinds of substitutes  
for legal signatures*



electronic  
signatures

*security technology  
based on PKI*



digital  
signatures

*electronic signatures  
produced with  
digital signature technology*





# Conclusion: Legal provisions ...

- (typically newer ones) may prescribe the use of digital signature technology for:
  - data authentication (example: e-invoices)
  - entity authentication (example: vehicle registration certificates)

# Industry guidelines, etc.

Example: SAFE-BioPharma Association

# SAFE-BioPharma Association™

## Signatures and Authentication for Everyone



## Welcome

**The mission of SAFE-BioPharma Association is to be the digital identity and signature standard for the global biopharmaceutical and healthcare communities.**

SAFE-BioPharma™ Association is the non-profit association that created and manages the SAFE-BioPharma™ digital identity and signature standard for the pharmaceutical and healthcare industries.

The SAFE-BioPharma™ standard...

- mitigates legal, regulatory and other business risk associated with electronic transactions.
- facilitates interoperability between disparate information systems.
- provides a secure, enforceable, and regulatory-compliant way to verify identities and apply digital signatures in electronic transactions.
- helps **green** the pharmaceutical and healthcare industries by dispensing with paper originals and other cumbersome forms of back up.

### Recent Announcements

- ♦ **SAFE-Biopharma Association and CDISC Join Forces to Advance Healthcare Information System Interoperability**
- ♦ **Register for 4th Annual Integrating Electronic Health Records and eClinical Technologies Conference Sept. 15-16, Baltimore**

### SAFE-BioPharma Media



- [Click for "The SAFE-BioPharma Standard"](#)
- [Click for the "SAFE-BioPharma Credentialing Demo"](#)

## 2. Legal provisions on electronic signatures by means of “digital signature technology”

# Terminology

*all kinds of substitutes  
for legal signatures*



electronic  
signatures

*security technology  
based on PKI*



digital  
signatures

*electronic signatures  
produced with  
digital signature technology*





## LAWS OF MALAYSIA

ACT 562

### DIGITAL SIGNATURE ACT 1997 [REPRINT 2002]

*Incorporating latest amendment - A1121/2001*

Date of Royal Assent :

Date of publication in the Gazette :

Date of coming into operation:

18th June 1997

30th June 1997

1st October 1998 [P.U.(B) 397/98]

---

#### ARRANGEMENT OF SECTIONS

---

[Long Title & Preamble](#)

#### PART I - PRELIMINARY

[Section 1. Short title and commencement.](#)

[Section 2. Interpretation.](#)

#### PART II - THE COMMISSION AND THE LICENSING OF CERTIFICATION AUTHORITIES

[Section 3. Appointment of Commission.](#)

[Section 4. Certification authorities to be licensed.](#)

[Section 5. Qualifications of certification authorities.](#)

[Section 6. Functions of licensed certification authorities.](#)

[Section 7. Application for licence.](#)

[Section 8. Grant or refusal of licence.](#)

[Section 9. Revocation of licence.](#)

[Section 10. Appeal.](#)

[Section 11. Surrender of licence.](#)

[Section 12. Effect of revocation, surrender or expiry of licence.](#)

[Section 13. Effect of lack of licence.](#)

[Section 14. Return of licence.](#)

# Example: 21 CFR Part 11 (USA)



U.S. Food and Drug Administration



Department of  
Health and  
Human Services

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

[FDA Home Page](#) | [CDRH Home Page](#) | [Search](#) | [A-Z Index](#)

[Questions?](#)



[510\(k\)](#) | [Registration & Listing](#) | [Adverse Events](#) | [PMA](#) | [Classification](#) | [CLIA](#)  
[CFR Title 21](#) | [Advisory Committees](#) | [Assembler](#) | [Recalls](#) | [Guidance](#) | [Standards](#)

## [New Search](#)

[Help](#) | [More About 21CFR](#)

[Code of Federal Regulations]  
[Title 21, Volume 1]  
[Revised as of April 1, 2008]  
[CITE: 21CFR11.1]

TITLE 21--FOOD AND DRUGS  
CHAPTER I--FOOD AND DRUG ADMINISTRATION  
DEPARTMENT OF HEALTH AND HUMAN SERVICES  
SUBCHAPTER A--GENERAL

### [PART 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES](#)

#### Subpart A--General Provisions

##### Sec. 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

CHAPTER I--FOOD AND DRUG ADMINISTRATION  
DEPARTMENT OF HEALTH AND HUMAN SERVICES  
SUBCHAPTER A--GENERAL

PART 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A--General Provisions

Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.



CHAPTER I--FOOD AND DRUG ADMINISTRATION  
DEPARTMENT OF HEALTH AND HUMAN SERVICES  
SUBCHAPTER A--GENERAL

PART 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A--General Provisions

Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

**(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.**

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.



Français	Contact us	Help	Search	Canada Site
Home	About us	History	FAQ	Site Map



## Canada Gazette

Welcome to the official newspaper of the Government of Canada published since 1841



[Notice](#)

News and announcements

Mandate

Consultation

Recent *Canada Gazette* publications

Part I:  
Notices and proposed regulations

Part II:  
Official regulations

Part III:  
Acts of Parliament

Learn more about the *Canada Gazette*

Publishing information

Publishing requirements

Deadline schedule

Insertion rates

Request for insertion forms

Subscription information

Useful links

Vol. 139, No. 4 — February 23, 2005

Registration  
SOR/2005-30 February 1, 2005

PERSONAL INFORMATION PROTECTION AND ELECTRONIC  
DOCUMENTS ACT CANADA EVIDENCE ACT

### Secure Electronic Signature Regulations

P.C. 2005-57 February 1, 2005

Whereas the Governor in Council is satisfied that the technology or process prescribed in the annexed *Secure Electronic Signature Regulations* can be proved to meet the requirements set out in paragraphs 48(2)(a) to (d) of the *Personal Information Protection and Electronic Documents Act* ([see footnote a](#));

Therefore, Her Excellency the Governor General in Council, on the recommendation of the Treasury Board, pursuant to subsection 48(1) of the *Personal Information Protection and Electronic Documents Act* ([see footnote b](#)) and paragraph 31.4(a) ([see footnote c](#)) of the *Canada Evidence Act*, hereby makes the annexed *Secure Electronic Signature Regulations*.

that

(a) is used in asymmetric cryptography to decrypt data contained in an electronic document that was encrypted through the application of the private key in the key pair; and

(b) corresponds only to the private key in the key pair. (*clé publique*)

## TECHNOLOGY OR PROCESS

2. For the purposes of the definition "secure electronic signature" in subsection 31(1) of the Act, a secure electronic signature in respect of data contained in an electronic document is a digital signature that results from completion of the following consecutive operations:

(a) application of the hash function to the data to generate a message digest;

(b) application of a private key to encrypt the message digest;

(c) incorporation in, attachment to, or association with the electronic document of the encrypted message digest;

(d) transmission of the electronic document and encrypted message digest together with either

(i) a digital signature certificate, or

(ii) a means of access to a digital signature certificate; and

(e) after receipt of the electronic document, the encrypted message digest and the digital signature certificate or the means of access to the digital signature certificate,

(i) application of the public key contained in the digital signature certificate to decrypt the encrypted message digest and produce the message digest referred to in paragraph (a),

(ii) application of the hash function to the data contained in the electronic document to generate a new message digest,

(iii) verification that, on comparison, the message digests referred to in paragraph (a) and subparagraph (ii) are identical, and

that

(a) is used in asymmetric cryptography to decrypt data contained in an electronic document that was encrypted through the application of the private key in the key pair; and

(b) corresponds only to the private key in the key pair. (*clé publique*)

**2.** For the purposes of the definition "secure electronic signature" in subsection 31(1) of the Act, a secure electronic signature in respect of data contained in an electronic document is a digital signature that results from completion of the following consecutive operations:

(a) application of the hash function to the data to generate a message digest;

(b) application of a private key to encrypt the message digest;

(c) incorporation in, attachment to, or association with the electronic document of the encrypted message digest;

(d) transmission of the electronic document and encrypted message digest together with either

and the digital signature certificate or the means of access to the digital signature certificate,

(i) application of the public key contained in the digital signature certificate to decrypt the encrypted message digest and produce the message digest referred to in paragraph (a),

(ii) application of the hash function to the data contained in the electronic document to generate a new message digest,

(iii) verification that, on comparison, the message digests referred to in paragraph (a) and subparagraph (ii) are identical, and

# Terminology

*all kinds of substitutes  
for legal signatures*

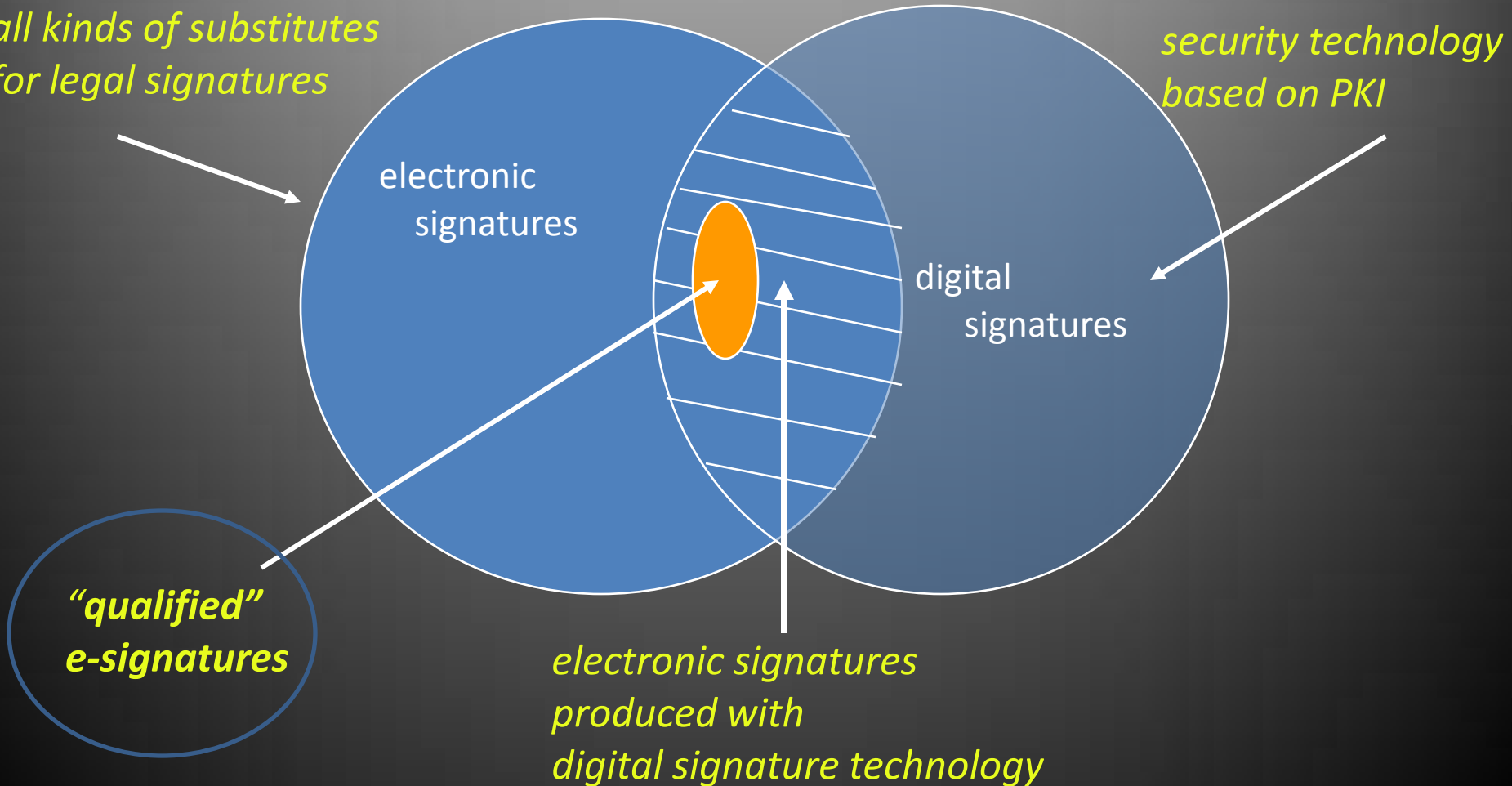
*security technology  
based on PKI*

electronic  
signatures

digital  
signatures

*“qualified”  
e-signatures*

*electronic signatures  
produced with  
digital signature technology*



# “Qualified Electronic Signatures”

- European concept: advanced signature
  - based on “qualified” certificate (issued by “qualified” CA)
  - created using a “secure signature creation device”
- Objective: (automatic) equivalent of the handwritten signature
  - (= current rules referring to “signing” automatically apply)

# “Qualified Electronic Signatures”

- European concept: advanced signature
  - based on “qualified” certificate (issued by “qualified” CA)
  - created using a “secure signature creation device”
- Objective: (automatic) equivalent of the handwritten signature
  - (= current rules referring to “signing” automatically apply)

Automatic ??



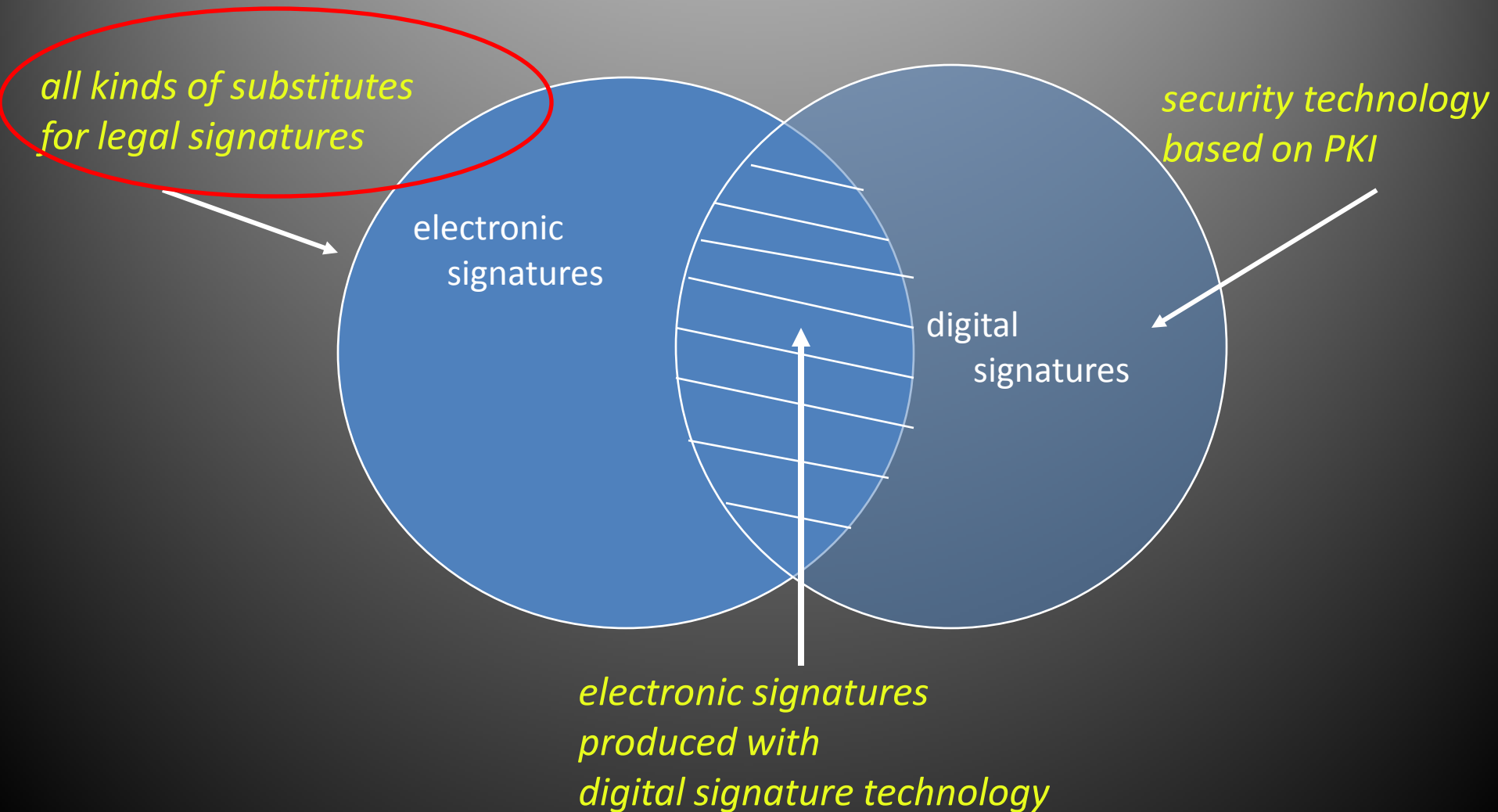


# Results of European approach

- Each of the 28 Member States has its own legal framework for “qualified” signatures
- Major issue today: interoperability
  - Common profile for qualified certificates
  - “Trusted” list of “qualified” CSPs (95 in 23 MS)
  - European validation platform?
  - ...

### 3. Legal provisions on electronic signatures

# Terminology



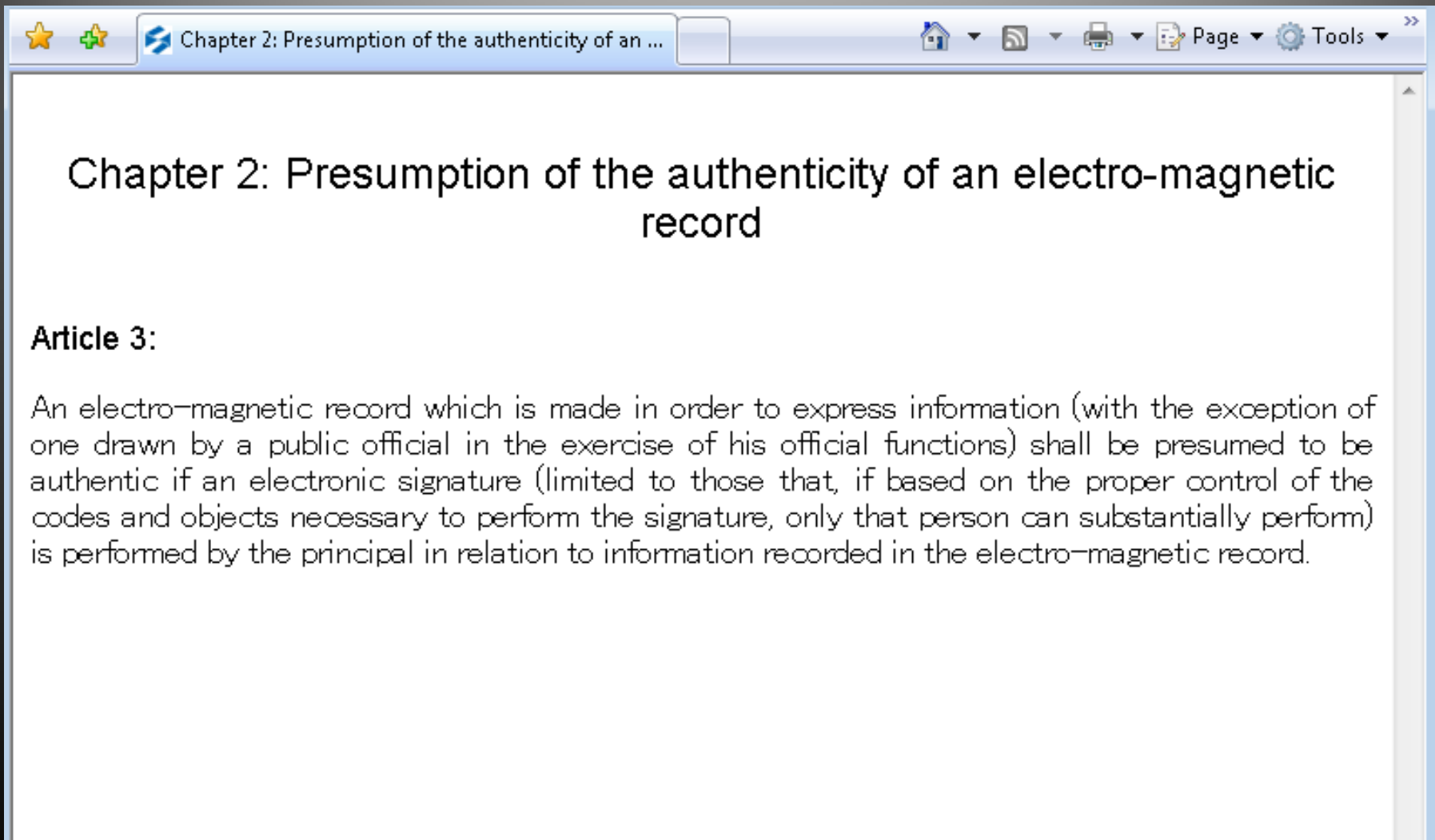
# USA : ESIGN & UETA

“electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

a “record” is defined under ESIGN and UETA as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”

Compare EU Definition: *“any data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”.*

# Japan: Law on electronic signatures and certification services (2000)



The image is a screenshot of a PDF viewer window. The title bar at the top shows a star icon, a green plus icon, and the text "Chapter 2: Presumption of the authenticity of an ...". To the right of the title bar are icons for home, RSS, print, and a "Page" dropdown menu, followed by a "Tools" dropdown menu. The main content area of the window displays the following text:

## Chapter 2: Presumption of the authenticity of an electro-magnetic record

**Article 3:**

An electro-magnetic record which is made in order to express information (with the exception of one drawn by a public official in the exercise of his official functions) shall be presumed to be authentic if an electronic signature (limited to those that, if based on the proper control of the codes and objects necessary to perform the signature, only that person can substantially perform) is performed by the principal in relation to information recorded in the electro-magnetic record.

# Argentine: law of 2001

## FIRMA DIGITAL

### Ley 25.506

**Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias.**

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

## LEY DE FIRMA DIGITAL

### CAPITULO I

#### Consideraciones generales

**ARTICULO 1º** — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

**ARTICULO 2º** — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

# Conclusions

- Legislation has preceded generally accepted best practices
- Consequence: diversity, complexity, confusion
- Current approach: sector-based, case-by-case



Jos Dumortier  
K.U.Leuven – ICRI / time.lex

<http://www.icri.be> – <http://www.timelex.eu>

jos.dumortier@timelex.eu