

## ELECTRONIC SIGNATURE

### I. Presentation.

### II. Regulatory Framework.

### III. Issues.

### IV. Conclusion.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

1

## ELECTRONIC SIGNATURE

### I. Presentation

1) The need to clarify the use of electronic signature (hereinafter « e-sign ») :

- E-sign: it means data in electronic form (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 of signing the record and which serve as a method of authentication ;
- E- commerce (BtoB, BtoC, BtoA, PtoP) ;
- Certification authorities.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

2

## ELECTRONIC SIGNATURE

### I. Presentation

2) Implementation Status :

- North America;
- Asia – Pacific Ocean;
- South America;
- Africa and Middle-East; and
- Europe.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

3

## ELECTRONIC SIGNATURE

### I. Presentation

3) The Purpose of establishing a national regulatory scheme in each country around the world for the e-sign is to facilitate the use of e-signs and to contribute to their multilateral legal recognition between countries. The establishment of a relatively uniform regulatory environment for e-signs and certain certification-service-providers is necessary to ensure the proper functioning of the international e-commerce market.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

4

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

Comparison of E.U. and U.S. legislation (E.U. : Directive 1999/93/EU and U.S. : (i) the Electronic Signatures in Global and National Commerce Act (hereinafter the « E-sign Act ») and (ii) the Uniform Electronic Transactions Act (hereinafter the « UETA »)).

- a) Points of Convergence between E.U. and U.S. Legislation.
- b) Key Difference between E.U. and U.S. Legislation.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

5

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

a) Points of Convergence between E.U. and U.S. legislation :

(i) Legal recognition of the e-sign;

The Section 101 (a) of the E-sign Act and the article 5 § 2 of the Directive 1999/93/EC provide that a signature, contract, or other record relating to a transaction pertaining to interstate or foreign commerce may not be denied legal effect, validity or enforceability solely because it is in electronic form.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

6

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

- a) Points of Convergence between E.U. and U.S. legislation (continued);
- (ii) Recognition of the legal validity of an electronically signed contract;
  - (iii) Transnational Interoperability and Recognition of e-sign products and services (certification, archiving, storing of electronic records, trust services, etc.);
  - (iv) The e-sign is considered the legal equivalent of a hand-written signature only if the requirements for hand-written signatures are fulfilled;

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

7

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

- a) Points of Convergence between E.U. and U.S. legislation (continued) :
- (v) Notarization and acknowledgment of the e-sign by a qualified third party (attorney, notary, public official or other): the performance of such authentication may be conducted electronically and without the presence of the qualified third party and such authentication can be executed and stored in accordance with the conditions to be developed by future implementation legislation;

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

8

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

- a) Points of Convergence between E.U. and U.S. legislation (continued) :
- (vi) Consumer Protection:  
European law and the E-sign Act provide different ways of protecting the consumer:
    - information to be disclosed in writing to the consumer, whether in electronic or other forms;
    - consent of consumer is required to contract electronically with the e-sign;
    - the consumer, prior to consenting, is provided with a clear and conspicuous statements and information.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

9

## ELECTRONIC SIGNATURE

### II. Regulatory Framework

- b) Key Difference between E.U. and U.S. Legislation :
- (i) **E.U.** : Under the Directive 1999/93/EC, « advanced e-signs » can be established through:
    - the use of qualified certificates and certification-service-providers; and
    - the satisfaction of the requirements for secure signature-creating devices defined in the Directive 1999/93/EC.
  - (ii) **U.S.**: the tendency of using « advanced e-signs », although more secure, is not contemplated in the E-sign Act or UETA. Market self-regulation is the driving force in the U.S.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

10

## ELECTRONIC SIGNATURE

### III. Issues

a) Identification Issue :

Only use of technology can establish electronic authentication. Identify means prove a person's identity.

To identify a person, we can use three authentication technologies.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

11

## ELECTRONIC SIGNATURE

### III. Issues

a) Identification Issue (continued),

(1) **Three authentication technologies** :

- (i) the first type is based on a physical support that we possess, a microchip or any other similar object;
- (ii) the second type is based on the acknowledgment of certain information, a PIN code or other;
- (iii) the third type is based on biometric technologies, which identify the unique physical traits of each person (finger prints, voice, etc.).

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

12

**ELECTRONIC SIGNATURE**  
**III. Issues**

a) Identification Issue (continued).

(2) **Risks of Using Biometric Technology :**

- (i) Biometric solutions are based on statistical analysis and are, thus, not 100% reliable;
- (ii) Biometric, human information is translated into binary form and this information is recorded on a tangible medium or stored in electronic or other form, which is retrievable in readable form.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

13

**ELECTRONIC SIGNATURE**  
**III. Issues**

b) The Issue of the Recognition of E-sign and Certificate for Foreign Commerce.

The legal and technical interoperability for the use of e-signs will be a problem because countries regulate this matter differently.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

14

**ELECTRONIC SIGNATURE**  
**III. Issues**

b) The Issue of the Recognition of E-sign and Certificate for Foreign Commerce (continued).

Three possible solutions concerning this issue:

- (i) The Minimalist Approach : Liberty to contract and interoperability of all the e-signs and certificates between different countries in international commerce. It can function in B to B and in B to C exchanges;
- (ii) The Approach of Mutual Recognition: The use of certification-service-providers and their e-signs and certificates in one country would have the same legal force in another country.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

15

**ELECTRONIC SIGNATURE**  
**III. Issues**

b) The Issue of the Recognition of E-sign and Certificate for Foreign Commerce (continued).

- (iii) The Multilateral Approach: To provide an enforceable legal warranty and interoperability, in respect to e-signs and certificates, between several countries, through international arrangements.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

16

**ELECTRONIC SIGNATURE**  
**III. Issues**

c) The Issue of Liability :

Three persons are, at least, involved in an electronic transaction :

- (i) The certification-service-provider;
- (ii) The signatory; and
- (iii) The person who receives the electronically signed document.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

17

**ELECTRONIC SIGNATURE**  
**III. Issues**

c) The Issue of Liability (continued) :

In respect to the certification-service-providers, there are three different aspects to an electronic transaction :

- (i) the certification;
- (ii) the registration and time-stamping; and
- (iii) the production of certificates.

The liability of each actor in the provision of certification services is different and has to be defined by each country.

18/10/01

By: Randy M. Yaloz (Andonis Vafeas) Euro Legal Counsel Group

18

## ELECTRONIC SIGNATURE

### III. Issues

#### c) The Issue of Liability (continued) :

The signatory and the person who receives the electronically signed document have to take certain precautions with the data in their possession:

- The signatory must keep his/her PIN code secret, not disclose it to other persons and notify the loss or theft thereof to the appropriate authorities;
- The person who receives the electronically signed document, must verify certain elements such as the date, the identity of a signatory, volume of the transaction and the validity period of certificate.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

19

## ELECTRONIC SIGNATURE

### III. Issues

#### d) Issue of Integrity:

The success of the e-sign not only relies on the creation of systems for the e-sign and certification, but also secure computer systems. To create a secure e-sign, we need the following:

- (i) the algorithms;
- (ii) the Secure Key for a Symmetrical Encryption System such as D.E.S. and the Private and Public Key for an Asymmetrical Encryption System; and
- (iii) the electronically signed document.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

20

## ELECTRONIC SIGNATURE

### III. Issues

#### e) Issue of Data Storage :

- (i) One of the approved standards in electronic archiving is the French norm NF Z43-09 adopted by the AFNOR (French Association of Standards) ;
- (ii) To obtain the performance required for the archiving of electronic data, we need third parties to guarantee the integrity and accessibility of today's electronically signed documents over time;

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

21

## ELECTRONIC SIGNATURE

### IV. Conclusion

- (a) Use of « Advanced e-signs » :
  - Higher level of security (E.U. initiative);
  - and
  - Promising alternative for agreements of considerable importance and value.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

22

## ELECTRONIC SIGNATURE

### IV. Conclusion

- (b) Use of Accredited Certification-Service-Providers:
  - Greater assurances of security;
  - Necessity to respect strict norms set and overseen by the State; and
  - More protective for purposes of proof in cases of liability.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

23

## ELECTRONIC SIGNATURE

### IV. Conclusion

- (c) Possible Interim Solution for Worldwide Recognition of E-sign and Certificates (« Piggyback » solution):
  - Parties in different countries can agree, irrespective of the contract's governing law, to subject only the e-sign and certification to the legal standards set in an E.U. Member State through the use of a Member State's certification-service-provider.

18/10/01

By: Randy M. Yaloz (Andonis  
Vafecas) Euro Legal Counsel Group

24

## **ELECTRONIC SIGNATURE**

### **IV. Conclusion**

(d) Accreditation of Qualifications of Certification-Service-Providers by the State versus Market Recognition of Qualifications:

- In France, there exists a « Comité Directeur de la Certification » (Steer Committee for Certification) established and controlled by the Office of the Prime Minister. It will supervise the evaluation and accreditation of the certification-service-providers.
- In the U.S., certification authorities are likely to be private companies such as Digital Signature Trust or Verisign.