Cross Border recognition of authentication methods/electronic signatures

Robert Boekhorst, Madrid, 15 December 2005

Introduction

Cross border recognition of authentication methods/electronic signatures:

- What is “cross border recognition”; Why is it relevant?
- Which international laws are there in relation to electronic signatures?
- How did the EU address cross border recognition in the Electronic Signatures Directive (Directive 1999/93/EC (“the Electronic Signatures Directives, ESD”)?
- Standardization: Do we need it, what can be said about the level of standardization?
- In view of the answers to the above questions, are there practical solutions?

Cross border recognition, why is it relevant?

Cross border recognition has the following aspects:

- A technical one: interoperability
- Several legal ones: Will an electronic signature product of a supplier of country A be recognised under the national laws of country B?
- What are the legal effects of use of an electronic signature in a cross border transaction?

International Legislation

- Initiatives from the UN, and the ICC and OECD
- However, non of these initiatives provide for binding international laws
- Important initiative: The UNCITRAL Model law on electronic commerce and the Model law on Electronic Signatures (MES)
- With respect to cross border recognition Article 12 MES is key. Principle: “non discrimination on the grounds of location”
- Since the mid nineties: many national laws throughout the world have been adopted throughout the world
- European Signatures Directive is currently only binding international law. Obviously, this directive only binds Member States

Cross Border Recognition EU

In the EU the ESD has created a legal framework aimed at facilitating use of the electronic signature and their legal recognition

The following articles are relevant for cross border recognition:

- Market access (Article 3 ESD)
- Home state control, free circulation of electronic signature products in the internal market (Article 4 ESD)

- Legal effects of electronic signatures (Article 5)
- International recognition of third countries (Article 7)

Legal effects in EU

Article 5 ESD

- What has been harmonised?
- What not?

Article 5 Legal effects of electronic signatures (1)

1. *Member States* shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
   a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
   b) are admissible as evidence in legal proceedings.

Meaning that the following criteria must have been complied with:

.....

Article 2 ESD

2. '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;

Annex I

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

Annex II

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

— only authorised persons can make entries and changes,

— information can be checked for authenticity,

— certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and

— any technical changes compromising these security requirements are apparent to the operator.

Annex III

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

   (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

   (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

   (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

Article 5 Legal effects of electronic signatures (2)

2. *Member States* shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
   - in electronic form, or
   - not based upon a qualified certificate, or
   - not based upon a qualified certificate issued by an accredited certification-service-provider, or
   - not created by a secure signature-creation device.

Cross Border Recognition of non Member States

Article 7 contains three alternatives for recognition of *qualified certificates issued by a certification service* provider established in a third country:

- The certification service provider must comply with directive requirements *and* must have been accredited
- An EU certification service provider guarantees the certificate
- Recognition by bi- or multilateral agreements

Note: There is no obligation as to the electronic signature product as such, nor an ordinary certificate. Here each individual national law of the EU Member will provide the answer

These kind of additional requirements appear often in electronic signature legislation around the world

Standards

There have been international initiatives on standardization initiated by for example:

- ITU (x.509)
- American Bar Association
- Asian Pacific Economic Cooperation (Apec)
- The Internet Engineering Task Force
- The W3C
- OASIS Digital Signature Services

- European Commission: the European Electronic Signature Standardisation Initiative (EESSI). Result: CEN Workshops Agreements, (such as CWA 14167 and CWA 14167) (article 3 subparagraph 5 ESD)

- ETSI produced numerous technical specifications, for instance: Electronic Signatures Formats TS 101 733, Qualified Certificate Profile, TS 101 862 and Policy Requirements for Certification Authorities Issuing Qualified Certificates, TS 101 456 (see: www.ict.etsi.org)

However, no global standard exists currently

Practical solutions for B2B transactions

- Make a choice of law and forum
- Insert a Signature Policy in the electronic agreement
- Explore the possibilities to insert evidentiary clauses

Conclusions

In the EU context the validity of electronic signatures created by the ESD is a bare minimum:

- The number of requirements for functional equivalence (Article 5) that have to be satisfied are (too?) substantial
- All other kinds of electronic signatures are uncertain as to the legal effect or admissibility, this again depends on national laws and interpretation by national courts
- Recognition of EU originating electronic signatures in third countries is diverse and requires prior assessment of the applicable laws of such country
- Recognition in the EU of electronic signatures originating from non EU countries, depends on national laws in the EU: As regards the ESD, only qualified certificates are recognised when the Article 7 conditions are complied with
- Yet, electronic signatures are here to stay and many of the existing uncertainties can be overcome in a practical way