The EU e-Signatures Directive and Authenticity

Hannelore Dekeyser
Vienna, April 5th 2006
DLM Forum
A worst case scenario

• You're being sued, and
  – Your evidence is in digital form ...
  – ... in an obsolete format ...
  – ... digitally signed ...
  – ... with outdated encryption algorithms
  – ... and the certificates have expired
A best case scenario

• You're bound to win, because
  – you have a hard copy
  – you migrated to an archival format and registered the signature's validation data
  – you have an emulator and a complete validation chain for the signature

• Sure?
Archivist's approach

• Is it an authentic record?
  – Integrity
    • essential characteristics
  – Identity
    • origin
    • context

• What's good for the archivist, is good for the judge?
Legal approach

• YES!
  – Proving matters of fact
    • e.g. security webcam
  – All records are admissible as evidence
    • Judge decides if they are convincing
    • Authenticity is a primary concern

Open evidence system
Legal approach

• NO, not always!
  – Proving transactions
    • E.g. Belgium, France, Luxembourg require an *original* signed document to prove contractual agreements(*)
    • Belgium demands preservation of invoices in *original* form

 Closed evidence system
Original signed document

- Handwritten signatures
  - The document that bears the mark placed on it by the signatories
  - \textit{photocopies, scans or microfilms}

- Electronic signatures
  - Any and all documents featuring the e-signature appended by the signatories.
  - \textit{hard copy, migrated copy?}
• generic electronic signature?
  – “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”
    • a name under an e-mail message
    • a scanned image of a handwritten signature
    • ...
  – Migrated version, emulated document
• NO! Some transactions require more...
Original signed document

• advanced electronic signature?
  – identifies the signatory uniquely, was created under his control and is linked to the data in such a manner that any subsequent change is detectable
  • digital signature technology
  – Migrated version, emulated document
Original signed document

- qualified electronic signature?
  - an advanced electronic signature + safeguards:
    - secure-signature-creation device
    - qualified certificate
    - reliable certification service provider
  - e.g. digital signature technology
  - Migrated version, emulated document
Overview

• Not original
  – hard copy
  – migrated record

=> not admissible

• Exceptions
  – strict conditions
    • sector
    • materials/methods
    • ...

• Original
  – emulated record

=> admissible

• Secondary concern:
  – Authenticity?
Transformed evidence

• eSignatures directive
  + closed evidence system/originality requirement
  = archiving problem

• Adapt legal framework
  – evaluate authenticity and integrity of records
  – evaluate preservation strategies on their merits
In cooperation with:

Interdisciplinary Center for Law & Information Technology
K.U.Leuven

http://www.law.kuleuven.ac.be/icri

http://www.ibbt.be