

European Digital Signatures Legislation

Dr Ian Walden

Centre for Commercial Law Studies, QMW, University of London
Consultant, Bird & Bird

Introductory remarks

- √ Issues of security & trust
 - » security services: authentication, non-repudiation, integrity, confidentiality, availability & accountability
- √ Legal validity
 - » form requirements
 - » evidence
- √ Certification services
 - » notarisational

Signatures

- √ Legal definitions
 - » copies & equivalents
 - “signature’ includes a facsimile of a signature by whatever process reproduced”
 - » personal signatures, eg. *In Re a debtor* [1996] 2 All ER 345
- √ Signature functions
 - » identity, eg. *Goodman v J.Eban Ltd* [1954] 1 All ER 763
 - » intention to be bound
 - » validate integrity of document
- √ Verification

Legislative initiatives

- √ United States
 - » Utah Digital Signature Act 1995
 - » Electronic Signatures in Global and National Commerce Act 2000
- √ UNCITRAL Model law (1996)
 - » Article 7(1)(b) “that method is as reliable as was appropriate for the purposes for which the data message was generated...”
 - » eg. Bermuda, Australia, Singapore, Japan
- √ European Union directive
 - » German Digital Signature Law 1997 (revised Sept. 2000)
 - Telecommunications & Post (Root CA)

EU Directive 99/93/EC

- √ Definitions (art. 2)
 - » 'advanced electronic signature'
 - "it is uniquely linked to the signatory;
 - it is capable of identifying the signatory;
 - it is created using means that the signatory can maintain under his sole control; and
 - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"
- √ Legal effects (art. 5)
 - » 'satisfy' and 'admissible'
 - advanced electronic signature; with qualified certificate and created by a secure-signature-creation-device
 - » 'not denied legal effectiveness'

'Qualified Certificates'

- √ Formatted in accordance with Annex I
- √ Issued by a certification service provider (Annex II)
- √ Requirements for secure electronic signature creation devices (Annex III)
- √ Recommendations for secure signature verification (Annex IV)
- √ European Electronic Signature Standardisation Initiative
 - » Policy Requirements for Certification Service Providers Issuing Qualified Certificates ETSI STF 155 T1 (15th July 2000)

'Qualified Certificates'

- √ Identification information
 - » CSP and State of establishment
 - » signatory or pseudonym
 - 'specific attribute'
- √ Corresponding signature-verification data
- √ Period of validity
- √ The advanced electronic signature of the issuing CSP
- √ Usage limitations
- √ Transaction value limitations

'Certification Service Provider'

- √ Annex II requirements:
 - » demonstrate the reliability necessary for providing certification services;
 - » ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
 - » ensure that the date and time when a certificate is issued or revoked can be determined precisely;
 - » verify the identity and any specific attributes of the person to which a qualified certificate is issued;
 - » employ personnel who possess the necessary expert knowledge, experience, and qualifications;
 - » they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
 - » use trustworthy systems and products which are protected against modification

- √ take measures against forgery of certificates and guarantee confidentiality when generating 'signature-creation data';
- √ maintain sufficient financial resources to operate in conformity with the requirements, eg. obtaining appropriate insurance;
- √ record all relevant information concerning a qualified certificate for an appropriate period of time, eg. legal proceedings;
- √ not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- √ customer transparency regarding terms and conditions regarding the use of the certificate, existence of an accreditation scheme and procedures for complaints and dispute settlement. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
- √ use trustworthy systems to store certificates in a verifiable form

Legal framework for CAs

- √ **Statutory framework**
 - » market access (art. 3)
- √ **EU Directive, Art. 6: liability for 'qualified certificates'**
 - » for accuracy of information, creation & verification data, revocation register
 - » limitations on use & value
- √ **Contractual documentation**
 - » Certificate policy
 - » Certification practice statement
 - » Service level agreement

Electronic Communications Act 2000

- √ Part I Regulation of 'cryptography support services'
 - » s.15 'sunset clause'
- √ Part II Facilitation of electronic commerce, data storage, etc.
 - » admissible in evidence (s.7)
 - » certification
 - » section 8 orders “..for the purpose of authorising or facilitating..”
 - “the doing of anything which under any such provisions is required to be or may be authorised by a person’s signature or seal”
 - conditions and requirements (s.8(4))

tScheme

- √ Alliance for Electronic Business
- √ Approvals process
 - » publication of 'Profile Criteria'
 - » Trust service provider
 - independent assessors
 - submit evidence of compliance
 - » assessed and approved
 - contractual Scheme conditions
- √ Governmental recognition

Related Regulatory Framework

- √ Data protection
 - » eg. 'appropriate technical and organisational measures'
 - 'state-of-the-art'
- √ Access to keys
 - » ie. Regulation of Investigatory Powers Act 2000
 - exemption for keys "used for the purpose only of generating electronic signatures" (s. 49(9))
- √ Export control
 - » ie. Council Regulation (22 June 2000)
 - exemption for 'authentication and digital signature functions'

Concluding remarks

- √ relative security & trust
 - » payment (eg. credit cards)
- √ differential security & validity
 - » legal certainty
 - » licensing schemes
- √ regulating technology / methodologies
 - » the principle of neutrality
- √ legal risk management