

# Electronic signatures and security

Stephen Mason, Barrister

# The 'hot' topic

The electronic transfer of lease information, and how much accountability lawyers **would** be prepared to take for the accuracy of an electronic 'abstract' of the paper document, as well as the **security, non-repudiation** and **authenticity** that a digital signature *brings*

# Outline

- a) a brief introduction to electronic signatures  
(electronic signatures are at least 41 years  
old this year)
- b) electronic signatures and security
- c) authentication of digital data

# Forms of electronic signature

Typing a name into an e-mail or e-document

The name in an e-mail address

Clicking the 'I accept' or 'I agree' icon

Using a personal identification number (PIN)

Using a scanned signature

Using a biometric measurement

Using a digital signature

# The practical meaning

In some jurisdictions, the format that an electronic signature takes is highly relevant

Where one party relies on an electronic signature and the other party denies using the electronic signature, the burden tends to remain (not always) as for manuscript signatures, that is:

*The party relying on the signature must prove the signature is not a forgery*

# The central problem

There is no distinction between the forms an electronic signature takes – a document is either signed or it is not signed

This means no form of electronic signature has any greater value than any other form

The problem that affects every form of electronic signature is this:

*The recipient does not know whether the signature was affixed to the e-mail or document by the person whose signature it purports to be*

# The recipient, the verifying party, the relying party

The party relying on the electronic signature has to ask themselves if they have sufficient evidence in place to rely on the signature

If a dispute occurs, consideration must be given to:

*How to prove the nexus between the application of the signature, whatever form it takes, and the person whose signature it purports to be*

The use of a digital signature does **not** prove the user caused the signature to be affixed to the e-mail or electronic document

# E-signatures and security

Two separate issues get confused:

- the signature

- the security of the document

For example:

- 'I accept' icon

- The name in an e-mail

- PIN and password

- Digital signature

It is necessary to be sure about the process of:

- managing the identity of clients

- providing proof of intent

- providing for the security of the process

# Authentication

# Further reading

## Evidential foundations:

A massive topic, see Chapter 4 of *Electronic Evidence: Disclosure, Discovery & Admissibility*, (LexisNexis Butterworths, 2007)

## Standards?

Standards can help, but see the 11 pages of standards that apply to electronic signatures in Appendix 3 of *Electronic Signatures in Law* (Tottel, 2nd edn, 2007) – which one (or 2 or 3 or more) will you follow?

# Final thoughts

Yes, getting it right is very important

Yes, there is a need to provide for a level of security that reflects the value of the transaction

Yes, digital signatures will probably help, but failing to understand their weakness within an open PKI is a serious danger

Can property be conveyed electronically? Why not?

**Thank you**

[www.stephenmason.eu](http://www.stephenmason.eu)

[www.deaeslr.org](http://www.deaeslr.org)