QED

PERSPECTIVES ON E-SIGNATURES

Stephen Mason, Barrister

Alan Liddle, DCS Consulting

Outline

Reasons for using signatures

Technical requirements

Forms of e-signature

Signature components

The practical issue

Technical challenges

Issues for the relying party

How courts assess the evidence

Providing the evidence

Some reasons for using a signature

Primary purpose

evidence that the signatory approves and adopts the contents of the document – often referred to as content commitment

content of the document shall be binding

Secondary purpose

authenticate the identity of the person

content of the document has not been altered subsequently to the affixing of the signature

Record keeping purpose

[For a complete list, see Stephen Mason, *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), chapter 1]

Technical requirements

There are no technical requirements in their own right

Where and how the technology can help

- The signatory probably signed – *protected private keys*
- The signatory knew what they are signing – SCA & *WYSIWYS*
- The signatory was who they seem/purport to be – *authentication*
- Content of what was signed is not changed – *integrity via crypto*
- The signature is of use to the relying party
  - It is easy to understand – *presentation and assertions*
  - It has all that is needed to make use of the signed item – *formats*
  - It is robust enough to support the burden of proof required of it – *AdES?*

Forms of electronic signature

Typing a name into an e-mail or electronic document

> Interest in property; loan; employment; contract; assignment of guarantee; insurance policy; public administration; judiciary; statute of frauds; wills

Clicking the ‘I accept’ or ‘I agree’ icon

Name in an e-mail address

Using a scanned signature

Using a personal identification number (PIN)

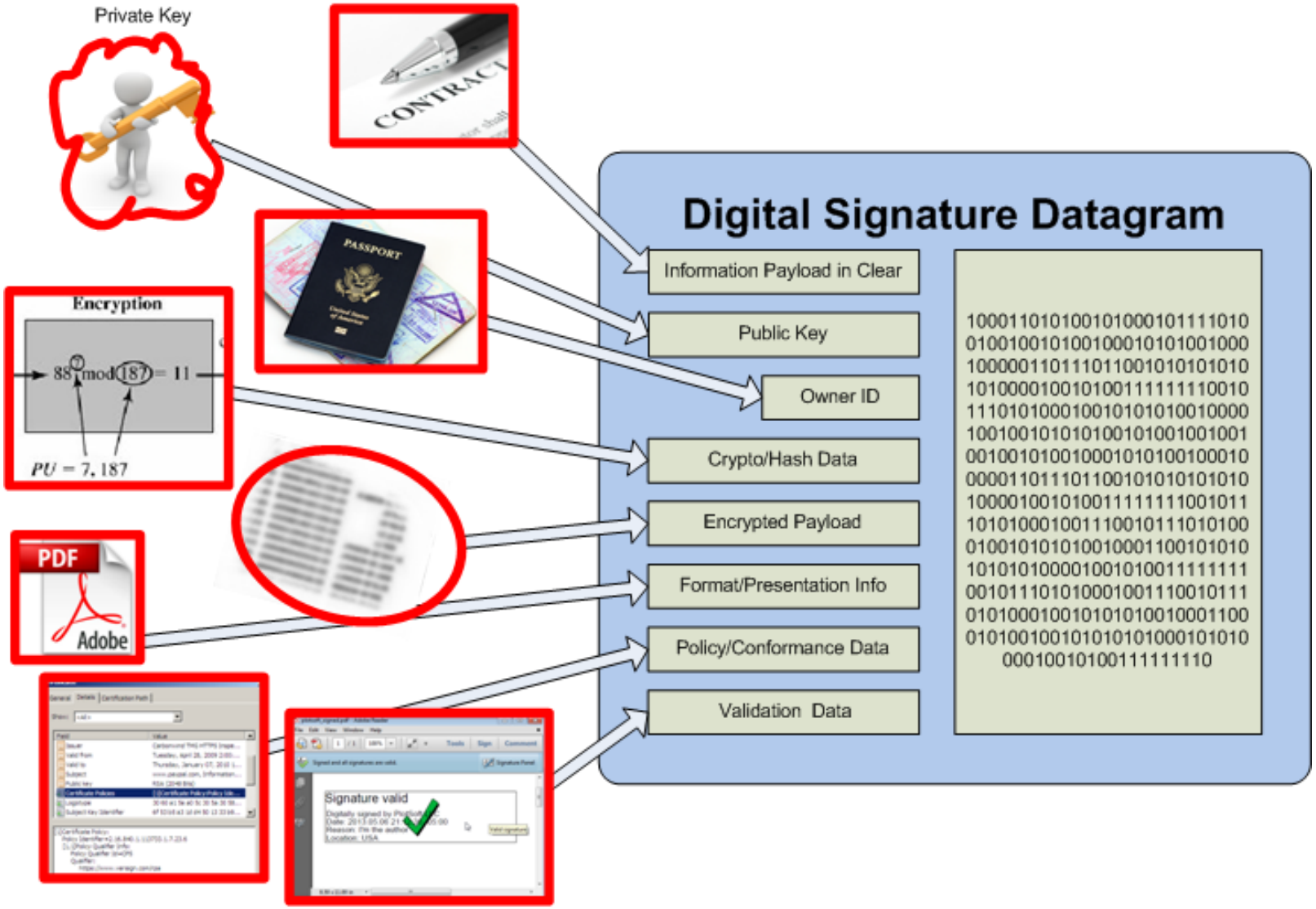
Using a digital signature

Using a biometric measurement

Electronic sound

Name in an e-mail address

QED - Easy to say but how can we do it?



The practical issue

In some jurisdictions, the format that an electronic signature takes is not relevant

Where one party relies on an electronic signature and the other party denies using the electronic signature, the burden remains as for manuscript signatures, that is:

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

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*

Technical challenges

- How robust is robust is robust?
  - Non digital signatures
  - Digital signatures
  - Qualified QAdES/AdES
  - Lightweight certificates
  - Natural persons and organisations
- Formatting and presentation
  - What the signatory sees
    - The signature creation application
    - Longevity – the Hash
- What the relying party sees… but what do they need?

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*

No form of electronic or digital signature proves the user caused the signature to be affixed to the e-mail or electronic document

This gives rise to the technology and information assurance challenges so that the relying party has substantial proof

How courts assess the evidence

But where is the evidence?

To be of value to the relying party there must be some robustness and evidence for the burden of proof

Assurance and compliance

- Compliance regimes – demonstrable?
- Audit regimes – classic evidence
- Interoperability – knowing what the “trust” is

What is important?

In conclusion

The method of signature you use depends on the business and legal context

Work out the problem before you try to solve it

Assurance and evidence are both important and difficult

QAdES sets a high standard but is difficult, expensive and complex - be sure you need this universal solution

Just solve your problem – don’t be a purist – this saves money and effort

Questions

Alan Liddle

DCS@deeps.co.uk

Stephen Mason

stephenmason@stephenmason.co.uk

Some useful references

EU Standards

- Regulation (EU) No 910/2014 on Electronic Signatures
- ETSI EN 319 411-1 Gen Reqs. for Cert Providers
- ETSI EN 319 411-2 Reqs. for Qualified Cert Providers
- ETSI EN 319 412-2 Certs for Natural Persons
- ETSI EN 319 412-5 Qualified Certificate Statements
- ETSI TR 119 100 Guidance on Standards - Creation &Validation
- ETSI TR 119 101 Reqs. on Standards - Creation &Validation

RFC 3126 CMS Advanced Electronic Signatures (CAdES)

RFC 3275 XML-Signature Syntax and Processing

http://stephenmason.co.uk
http://ials.sas.ac.uk/about/about-us/people/stephen-mason

Free journal

Digital Evidence and Electronic Signature Law Review

http://journals.sas.ac.uk/deeslr

Draft Convention on Electronic Evidence

http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Free books

Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence

Stephen Mason, *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016)

http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

International Electronic Evidence (British Institute of International and Comparative Law, 2008)

https://www.biicl.org/international-electronic-evidence