Failings in the Treatment of Electronic Signatures

Gavin Jones
Masters Student, Faculty of Law, University of Hertfordshire

Abstract

The implementation of the legal recognition of electronic signatures in the UK does not distinguish between electronic signatures and 'advanced electronic signatures' as defined by the EU Directive on electronic signatures.[1] When considered against paper-based signatures, electronic signatures that do not guarantee 'data integrity'[2] fail in providing that the contract (electronic transmission) has been incorporated by signature. Further, the authentication provided by digital signatures, although ensuring data integrity and normally used as an example of 'advanced electronic signatures', cannot ensure point-in-time authentication of the signatory. They can only authenticate the signatory's electronic agent unless some form of access control known to / exhibited by only the individual 'signing'.

Article

In order to encourage electronic commerce, legislation must be both sufficiently open to encourage technological innovation and sufficiently restrictive so as to ensure participant confidence in both the business community and the public. Whilst businesses must be confident in the fact that legislation exists which protects them against fraud or allegations of impersonation, so too the public requires assurance that there is an acceptable level of consumer protection (including transaction security) comparable with other forms of commerce.

As part of this assurance EU member states are required, by Directive 1999/93/EC, to recognise "advanced electronic signatures" ensuring they:

> "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"[3]

An advanced electronic signature is defined in the EU framework for electronic signatures in such a way that includes both authentication and data integrity.[4]

For any contract to have terms and conditions incorporated by signature, data integrity must be assured. Otherwise there can be doubt over what has been signed and repudiation becomes an issue. With a paper based contract this can be achieved by both parties having signed copies of the contract. With an electronic contract this can be achieved by ensuring undisputable evidence of data integrity is included as part of the signature and ensuring that an audit of this information is stored.[5]

[1] Directive 1999/93/EC of the European Parliament of the Council on a Community framework for electronic signatures.

[2] Where data integrity is interpreted as the message received being exactly the same as the message sent and that this can be verified, not only when the transmission is received, but at a future date.

[3] Supra, n.1. Art 5(1)(a).

[4] Ibid. Art 2.

[5] Typical logging mechanisms, such as web server logs, are not normally kept for a sufficient period of time to provide an audit mechanism; hence, the web application should have its own application audit, such as an application file or table that stores the received message.

The implementation of the Directive 1999/93/EC in the UK was by The Electronic Signatures Regulations 2002.[6] As part of the explanatory notes, it was stated that the "admissibility of electronic signatures in legal proceedings" required by the Directive, were implemented by the Electronic Communications Act 2000. However, the Electronic Communications Act 2000 is too loose in its definitions.[7] Understandably, the Act does not want to restrict technological innovation, so the definition of electronic signatures is suitably unspecific.[8] However the implementation should ensure that an electronic signature exhibit analogous binding characteristics as a handwritten signature, i.e. the wording of section 7(3) should not extend beyond the definition of advanced electronic signatures to allow for authenticity and integrity to be considered separately.[9] In the paper world this is analogous to having a signature on one piece of paper and an unsigned contract on another with nothing linking the two. Additionally, section 7(3) allows for the data and the communication to be treated separately, an issue when integrity of both is vital to ensure non-repudiation of receipt.

In the absence of irregularities (e.g. fraud), a paper contract incorporated by signature has guarantied data integrity. For the law to recognise contracts incorporated by electronic signatures, it should require data integrity to be incorporated into the signature. There should also be the requirement to ensure that the contracting party is aware that they are performing an act that will result in the provision of an electronic signature incorporating contractual terms and conditions.

With respect to handwritten signatures, Scrutton LJ, in L'Estrange v F. Graucob Ltd [1934], concluded:

> "…When a document containing contractual terms is signed, then, in the absence of fraud, or, I will add, misrepresentation, the party signing is bound…"[10]

For technology to achieve the same level of certainty as a handwritten signature, then focus should be on the potential security risks that technology introduces. In a software developer article, IBM identify four security risks as requiring addressing in assuring the safety of e-Commerce transactions and associated data. These are:

- Privacy
- Authentication
- Integrity
- Non-repudiation.[11]

This can be extended to include Authorisation and Audit.[12] For a full legal recognition of the contract / transaction and the signature incorporating it, end-to-end non-repudiation should be addressed. This non-repudiation should cover origin (to include submission) and receipt.

Technically, to ensure non-repudiation at origin, the contracting party will need communicate the data in such a way that the integrity of the data is preserved and can be verified as such on receipt. Included with the data needs to be evidence that can uniquely authenticate the originating contracting party.

[6] The Electronic Signatures Regulations 2002 SI 2002/318.

[7] Electronic Communications Act 2000 s. 7.

[8] Ibid s.7(2).

[9] This may be to satisfy Article 5(2) of the Directive that requires that electronic signatures are not denied legal effectiveness and admissibility as evidence.

[10] L'Estrange v F. Graucob Ltd [1934] 2 KB 394 (Divisional Court)

[11] See: http://www-106.ibm.com/developerworks/library/s-pain.html

[12] See: http://www.rsasecurity.com/solutions/vpn/framework.html

Technically, for non-repudiation of receipt, the recipient contracting party must be uniquely identifiable (authenticated) against the communication, and the communication, including the originator, the content and the date and time of receipt logged (audited) as such. Further, the data integrity must be confirmed.

One form of advanced electronic signature that is commonly used is a digital signature. A digital signature is:

> "a data item which accompanies or is logically associated with a digitally encoded message and which can be used to ascertain both the originator of the message and that the message has not been modified since it left the originator."[13]

An example of how a digital signature works is shown in *figure 1*. The key point to note is that the signature contains a digest of the message[14] encrypted with the originator's private key. The signature is decrypted by the recipient and compared against a digest of the message created by recipient. If the decrypted signature and the digest are equivalent, then the message is authenticated (by virtue of the fact that the public key decrypts the signature) and message integrity is verified.

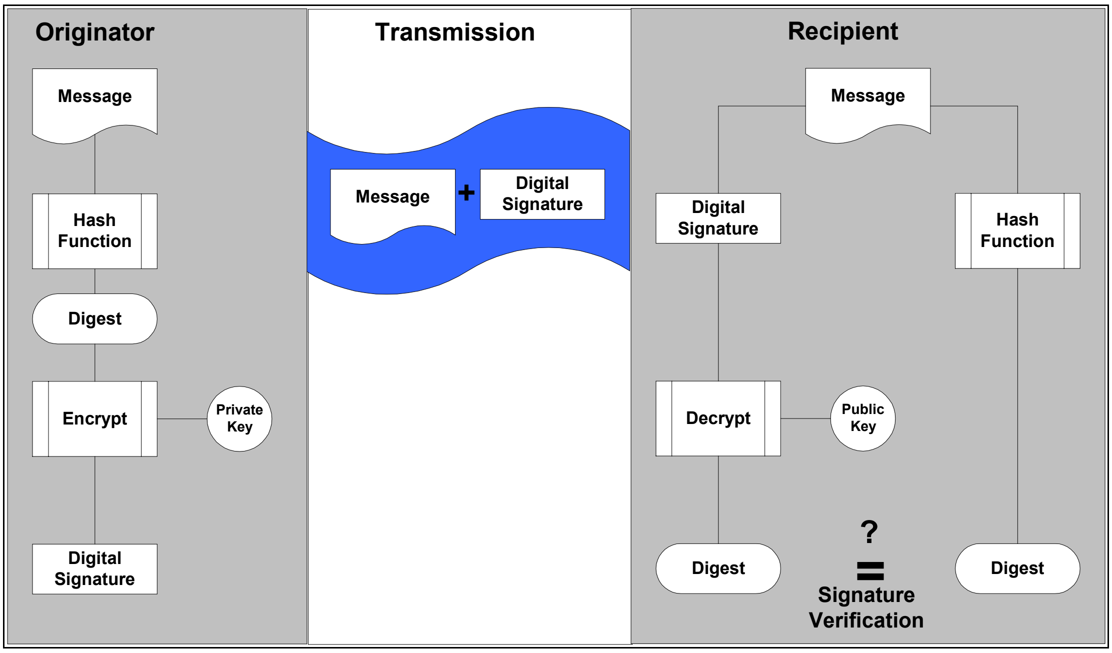

Figure 1 Digital Signature Creation and Validation

A digital certificate can be used in creating the digital signature. For security architectures that require authentication, this certificate is normally provided either by the contracting party or by a trusted third party (TTP).[15] The TTP will authenticate the participant and then issue a unique certificate valid for a given time period. The participant can then use this certificate to prove their authenticity to any other party that "trusts" the TTP until the expiry of the certificate.[16]

[13] M. S. Baum and W. Ford, *Secure Electronic Commerce*, 2nd ed, (Prentice Hall PTR, New Jersey, 2001), p109.

[14] Note, it may simply contain the message encrypted with the originator's private key; however, a digest created using a hash function is more normal as it saves substantially on the data size of the signature.

[15] See supra, n.6. Sch. 2 for the requirements for issuing "qualified" certificates.

[16] For a discussion on the involvement of TTPs in secure e-Commerce and the functions they perform, including:

1. Public-key certification
2. Identity Confirmation
3. Time Stamping

The participant needs to store the certificate and the associated private key securely. This normally results in the certificate being associated with a specific hardware device (e.g. PC) rather than the individual.[17] Unless the hardware device is mobile, then the certificate is not portable and if the individual has a number of hardware devices, they may require a certificate on each device to perform the same activity. Further, as multiple users may use the hardware device, the certificate (and therefore the digital signature generated using it) cannot guarantee authenticity of the individual, unless access control is used in addition.[18] I.e. authenticity can only be associated with the contracting agent (hardware device),[19] not with the individual unless further security measures are in place.[20]

It could be argued that it is the participant's responsibility to ensure the security of the certificate on their local machine; however, the Directive has not taken a position on the liability for loss associated with certificate misuse, except for issues associated with the security and issuance of certificates by the Certification Service Provider. This may be argued as a failing in the Directive and applied regulation, as there is an emphasis on the authentication using electronic signatures and lacking recognition that this authentication may be compromised. This has been recognised in the UNCITRAL Model Law suggesting responsibility on the signatory / certificate holder in the event that they do not exercise reasonable care.[21]

Further, digital signatures have limitations, as, unlike handwritten signatures, digital signatures are not a point-in-time authentication event. Additionally, software, private keys and certificates are all updated / recreated regularly making it difficult to ensure that a transaction signed today will still be able to be authenticated in the future.[22] Electronic signatures that will provide point-in-time authentication need to be based on unique individual characteristics that require some form of real time scan, such as an iris or a fingerprint scan. The technology associated with these 'biometric electronic signatures'[23] is still in its infancy, although the legislation has been worded flexibly enough to allow for legal recognition of these signatures.[24] However, the end result may still not resolve the authentication issues entirely, as the electronic code generated from the scan will need to be verified against some authenticating database and any security breach of such a store will undermine the validity of such authentication.[25]

In order to provide an environment for electronic commerce where an electronic signature has the same power to incorporate as a handwritten signature in the paper world, the law needs to either tightly define an electronic signature, or the attributes that electronic signatures must

4. Records Retention
5. Delivery Intermediation
6. Dispute Resolution

See: Baum, supra, n.13. p353 – 361.

[17] Although certificates can be issued such that they (and their private keys) are exportable. A certificate can be exported from an Internet Explorer browser by selecting Tools > Options and then going to the 'Content' tab and selecting 'Certificates', highlighting a certificate and using the 'Export' wizard.

[18] Such as username/password or PIN access to the machine.

[19] With networking, such as the Internet, this device and the associated storage device that contains the certificate is open to attack and replication.

[20] Thus violating the definition of an 'advanced electronic signature' in supra, n.1. Art. 2(2)(c).

[21] UNCITRAL Model Law on Electronic Signatures (2001) Art 8(2).

[22] For security reasons, certificates are issued with expiry periods, normally one year or less.

[23] Signatures based on the interpretation of physiological characteristics such as fingerprint recognition, voice recognition, handwriting recognition, face recognition, hand geometry recognition or retinal scans.

[24] Although Baum, supra, n.13. (p129) dismisses biometrics as "too limited", using biometrics as part of an authorisation (access control) process prior to being able to provide an authenticating digital signature and then encoding this with the digital signature to create an electronic signature has to have superior authentication and non-repudiation characteristics.

[25] For a discussion on a proposed biometric signature recognition project for the Nationwide, see: http://www.albassera.com/aweb_home_pld.php?pgid=./library/apd4020007.html&pgct=1

exhibit. Given the shortcomings of present technologies, especially in the domain of authentication, any definition of electronic signature that restricts future innovation is not beneficial. Therefore, attention should be directed at defining the attributes of signatures to ensure non-repudiation. These means ensuring that both authenticity and integrity of both the communication and the data are required before an electronic signature can be legally recognised in the way that a handwritten signature is. The EU Directive appears to have recognised this by providing a two-flavour definition of electronic signatures, the more secure of which, is determined to be equivalent of a handwritten signature.

BIBLIOGRAPHY

Books

M. S. Baum and W. Ford, *Secure Electronic Commerce*, 2nd ed, (Prentice Hall PTR, New Jersey, 2001).

Articles

C. Spyrelli, 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication', Journal of Law Information and Technology (2002 Issue 2).

Cases

L'Estrange v F. Graucob Ltd [1934] 2 KB 394 (Divisional Court).

Legislation

Directive 1999/93/EC of the European Parliament of the Council of 13 December 1999 on a Community framework for electronic signatures [2000] OJ L13.

Electronic Communications Act 2000 s. 7.

The Electronic Signatures Regulations 2002, SI 2002/318.

Other Written Sources

UNCITRAL Model Law on Electronic Signatures (2001) Art 8(2).

Other Sources

The Albassera Project, *In Profile – Biometrics in the retail banking sector,* http://www.albassera.com/aweb_home_pld.php?pgid=./library/apd4020007.html&pgct=1 [Accessed on 11th April 2003]

W. Caelli and A. McCullagh, *Non-Repudiation in the Digital Environment,* http://www.firstmonday.dk/issues/issue5_8/mccullagh/#note4 [Accessed on 30th March 2003]

S. Cannady and T. H. Stockton (IBM), *Easing the Pain*, http://www-106.ibm.com/developerworks/library/s-pain.html [Accessed on 29th March 2003]

The Electronic Signatures Regulations 2002, SI 2002/318, http://www.hmso.gov.uk/si/si2002/20020318.htm [Accessed on 29th March 2003]

A Gutzman, *Legalizing Ink: The New Electronic Signature Law,* http://ecommerce.internet.com/news/insights/ectech/article/0,,9561_413551,00.html [Accessed on 30th March 2003]

RSA Security, *RSA VPN Security Portfolio,* http://www.rsasecurity.com/solutions/vpn/framework.html [Accessed on 29th March 2003]

C. Spyrelli, *Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication,* Journal of Law Information and Technology (2002 Issue 2), http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html [Accessed on 30th March 2003]

Western Australia e-Commerce Centre, *Authentication, Integrity and Non-Repudiation,* http://www.ecommercecentre.online.wa.gov.au/matrix/sec-auth.htm [Accessed on 30th March 2003]

Working Group "Biometrics and Electronic Signatures", *website,* http://www.biosig.org/english/biosig-e.html [Accessed on 11th April 2003]