DIGITAL SIGNATURES AND THE ELECTRONIC TRANSFER OF LAND

by

SÉAMUS KEATING*

This article assessed the challenges posed by the use of digital signatures as part of the introduction of an electronic transfer of land ownership system. The role and function of manuscript signatures is analysed in order to explain the role that digital signatures will play in a system which allows for the electronic transfer of land ownership. The technological and legal initiatives relating to digital signatures are analysed. In particular, the development of a legal framework for digital signatures is evaluated. This article focuses on whether the form of digital signature that is provided by the Electronic Signatures Directive and the UNICTRAL Model Law on Electronic Signatures is appropriate in the context of the electronic transfer of land ownership. Electronic conveyancing will transform the current paper-based conveyancing system. Digital signatures will play a vital role in this process. The affect that the introduction of digital signatures will have on the conveyancing process has not been addressed. This research evaluates how liability for fraudulent transactions will be distributed in an electronic conveyancing process which relies on digital signatures.

KEYWORDS
Digital Signatures, Electronic Conveyancing, Electronic Signatures Directive, UNCITRAL Model Law on Electronic Signatures

1. INTRODUCTION

The process of transferring ownership of land from one person to another has evolved over several hundred years. In common law jurisdictions such

* s.keating3@nuigalway.ie

as Ireland this process, known as conveyancing is 'creaking at the seams'[1] and 'is hampered by a complex, cumbersome legislative framework and thus inherent delay'.[2] Applying electronic commerce principles to the conveyancing process has been described as obvious.[3] The focus of this article is to assess the challenges that the use of digital signatures present in the context of transferring land ownership.

2. THE FORM AND FUNCTION OF SIGNATURES

The common law and legislation relating to signatures and their use in conveyancing has evolved as innovations in technology have occurred. The universally understood concept of the signature is known as the manuscript or wet signature and usually takes the form of hand writing on a paper carrier. However, exceptions and modifications to this concept of the signature have been made by common law courts. These include crosses, initials, pseudonyms, identifying phrases, printed names and rubber stamps.

The formal requirements for the creation of a valid will are analogous to the requirement for a valid contract for the sale of land. Wills are required to be in writing, signed by the testator and attested by at least two witnesses.[4] These formalities are of relevance to our understanding of digital signatures as common law courts have focused on the intention of the testator rather than the form of signature.

In the *Estate of Cook, Deceased*[5] a will singed with the words, 'your loving mother' was regarded the held to be validly executed. Similarly in Scotland, the decision of the Outer House of the Court of Session, *Rhodes v Peterson*[6] Lord Hunter held that the words 'lots of love, mum' could be construed as a valid signature.

In *Fulton v Kee*,[7] the Court of Appeal, Civil Division of Northern Ireland dealt with a similar set of facts. The testator suffered from a medical condition which made it impossible to sign the will. The witnesses assisted the

---

1 Law Society of Ireland eConveyancing Task Force 2008 'e-Conveyancing: back to Basic Principles' <http://www.tfpb.ie/Publication%20of%20eVision.pdf> viewed 14 January 2013.

2 Ibid.

3 Law Reform Commission 2006, ''Report: eConveyancing: Modelling of the Irish Conveyancing System' LRC 79-2006, para 2.06.

4 S.78 Succession Act 1965 (Ireland)

5 [1960] 1 Weekly Law Reports 353.

6 *Rhodes v Peterson* (1972) Scots Law Times 98.

7 *Fulton v Kee* [1961] Northern Ireland Law Reports 1. See also - - 'The Execution of a Will by a Marksman', (1960-1961) 14 Northern Ireland Legal Quarterly 399.

testator by placing the pen between his figures and making the mark. Lord MacDermott found that a mark made with the necessary intent will be sufficient.[8]

These decisions indicate that in a more modern context, a person who chooses to use a more advanced form of signature such as a typed signature could validly execute a will once the required intention and physical act are present.

The creation of a valid contract for land is subject to special rules. S.2 Statute of Frauds (Ireland) 1695 required the contract to be evidenced in writing.[9] The formalities imposed on those obtaining an interest in land can be justified on a number of grounds; the protection of vulnerable parties, the prevention of fraud and perjury and promoting certainty. The purpose of this statute was the '*prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury and subornation of perjury*'.[10]

The modern judicial approach is to recognise the function of a signature over the form. Professor Reed has written 'a signature will be valid, irrespective of the form it takes, if it performs the functions which the law requires of a signature'.[11] A constant theme in the evolution of signatures has been the need to ensure that the identity and intention of executor is evidenced.

3. DIGITAL SIGNATURES – LEGISLATIVE BACKGROUND

While digital signatures have emerged relatively recently, the concept of digital signatures has existed in law since the 1990s. The UNCITRAL Model Law on Electronic Commerce (MLEC) and Model Law on Electronic Signatures (MLES) were enacted to provide guidance to national states when drafting legislation to provide for electronic commerce. The MLEC introduced the concept of functional equivalence and provides that a document in paper form and a document in digital form would be given the same recognition.[12] Providing that a document can be read by all can remain un-

---

8 *Baker v Dening* (1838) 8 Adolphus and Ellis Reports 94.

9 See Land and Conveyancing Law Reform Act 2009, S.51.

10 Ibid, preamble.

11 Chris Reed, 'What is a Signature?' (2000) 3 The Journal of Information, Law and Technology. <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/> viewed 28 July 2012.

12 UNCITRAL Model Law on Electronic Commerce, Part I, Chapter 2Article 5

altered over time and can allow for authentication by signature and can be reproduced over time it will be the equivalent of a paper document.[13]

Article 7 provides that where legislation requires the signature of a person, this requirement will be met where a method is used to identity the signatory and to indicate their approval of the contents of the electronic document.[14] The Model Law on Electronic Signatures (MLES) expands on the principles contained in Article 7 of the MLEC and focuses on two functions of a signature; identifying the signatory to a document and confirming that the signatory approved of the contents.

Article 2(a) MLES requires that the signatory be identifiable through the electronic signature. The connection between the signatory and the signature is maintained by a certificate. Article 2(b) defines a certificate as a 'data message of other record confirming the link between a signatory and signature creation data'.[15] In practice this link would be created when the signatory applies for a certificate from a certification provider. Such a certificate could take the form of a cryptographic verification key. The certification provider is defined in Article 2(e) as a person who issues certificate relating to electronic signatures.

Article 6 of the MLES contains the core principles of the model law and develops the principles set out in Article 7 of the MLEC. An electronic signature is considered reliable where the signature creation data and the signatory are uniquely linked;[16] where the signatory and the electronic signature are uniquely linked at the time of execution[17] and when any alteration post execution is detectable.[18] The purpose of this article is to ensure that any 'legal consequence would have flowed from the use of a handwritten signature; the same consequence should flow from the use of a reliable electronic signature'.[19] The MLES sets a high standard, particularly in Article 6 where not only should the electronic signature and the signatory be linked, but the electronic signature must be under the control of the signatory at the time of execution and no one else. However, while this is a high standard it is also warranted as in order to provide for functional equivalence, the tool

[13] UNCITRAL Model Law on Electronic Commerce, Part B, para 16
[14] UNCITRAL Model Law on Electronic Commerce, Part I, Chapter 2, Article 7.
[15] Ibid, Article 2(d).
[16] UNCITRAL Model Law on Electronic Signatures, Part II, Article 6(a).
[17] UNCITRAL Model Law on Electronic Signatures, Part II, Article 6(b).
[18] UNCITRAL Model Law on Electronic Signatures, Part II, Article 6(c).
[19] UNCITRAL Model Law on Electronic Signatures – Guide to Enactment, para 115.

used for signing, whether it is a fountain pen or a cryptographic digital signature must under the exclusive control of the signatory at the time of execution.

The increase in internet usage and electronic commerce from the 1990s prompted the European Union to prepare a European framework for digital signatures and encryption. In 1996 the European parliament passed a resolution requesting the Commission to prepare measures to ensure the integrity and authenticity of electronically transmitted documents.[20] The Electronic Signatures Directive[21] was the result of this process. The Electronic Signatures Directive (ESD) reflects the principles set out in the MLEC and the MLES.

However, the ESD differs from the MLEC and the MLES as it provides for three forms of electronic signature; the basic electronic signature, an advanced Electronic Signature (AES) and an AES with a qualified certificate which is described as a qualified electronic signature (QES). While the ESD is technologically neutral, the EU Commission has recognised that in practice the definitions provided are based on Public Key Infrastructure (PKI).[22]

Article 2(1) of the ESD defines an electronic signature as being 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'. Article 2(2) provides for an AES. The definition of an AES is similar to the electronic signature set out in the MLES. The ESD provides that an AES must meet the following requirements; be uniquely linked with the signatory;[23] be capable of identifying the signatory;[24] be controlled exclusively by the signatory[25] and linked to the electronic document in such a way that any alteration post execution is detectable.[26]

The AES does not explicitly require that the signatory acknowledge the contents of the electronic document although as Article 2(1) provides that the signature is either attached to or embedded in the electronic document this would be implied.

---

[20] European Parliament Resolution A4-244-96 of 10.09.96

[21] Council Directive (EC) 99/93 on a Community framework for electronic signatures [1999] OJ L013/12 (Electronic Signatures Directive).

[22] Commission, 'Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures' COM (2006) 120 final, 4.

[23] Ibid, Article 2(2) (a).

[24] Ibid, Article 2(2) (b).

[25] Ibid, Article 2(2) (c).

[26] Ibid, Article 2(2) (d).

Arguably the standard required by the AES is overly elaborate for many consumer contracts. The AES does comply with the concept of functional equivalence as the AES must be uniquely linked to the signatory and be controlled exclusively by the signatory. Mason has commented that this requirement displays a bias towards cryptographic tokens such as smart ID cards.[27] He has argued that it is unlikely for an individual to remember a private key as it is too complex and tokens containing the private key would be required. A token may take the form of a diskette, smart card or an encrypted memory stick. It is clear that as such token can be removed from or lost by the signatory and cannot be uniquely linked to the signatory. It is likely that a private key which is created using biometric data would be the only form of private key that could be uniquely linked to the signatory.

The AES also requires a link to the electronic document which would allow for the detection of any alterations. This would suggest the use of PKI which could lock a document, preventing further amendments.

The intention was that an AES would, when coupled with a qualified certificate from a certificate provider, offer the highest level of security. An AES based on a qualified certificate was described in the ESD as a QES.[28] The qualified certificate which is the main difference between a QES and an AES would be issued by a certification service provider (CSP). The CSP would certify the authenticity of the signatory's public key, which would verify the identity of the holder of the AES applied to the electronic document.[29]

The QES is intended to offer full functional equivalence to a manuscript signature. In 2008 the Commission restated the principle that a QES benefits from a presumption of functional equivalence to a manuscript signature under the ESD.[30] However, it is important to note the intention of the ESD in respect of the QES. The Commission was aware of the trend in Europe to develop electronic identity cards (EID) and it is arguable that the QES reflects a view that EID would play a significant role '*as an identification docu-*

[27] Mason, S, 2012, Electronic Signatures in Law, 3rd edition, Cambridge University Press, para 4.3 and 4.7.

[28] Commission, 'Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market', COM (2008) 798 final, 6.

[29] The certificate may take many technical forms and contain information on the expiry date of the electronic signature. In practice recipient's computer application will verify the authenticity of the signature used.

[30] Ibid, 7.

ment and to provide on-line access to public services for the citizens. In most cases these ID cards will contain the three functionalities: identification, authentication and signing'.[31]

The ESD unlike the MLES does not impose obligations on a party relying on a certificate to ensure that it is valid and to verify that the identity of the subscribers is one and the same as the person possessing the certificate. Instead the ESD sets out a list of recommendations for security verification.[32]

The UNCITRAL model laws and the ESD provide for digital signatures. Given the formalities which are required by current conveyancing procedures, it is likely that only the QES is appropriate in an electronic conveyancing system. Such digital signatures will rely on PKI technology. The ESD allows Member States to decide on the level of electronic signature that is suitable for different types of contracts. However, the QES as understood by the Commission suggests that EID cards are required to give full effect to the intention of the ESD. Certainly, transactions involving land require a signature that is entirely the functional equivalent of a manuscript signature and it is logical an EID card would play an integral role in such a system. In addition, the standards for the QES in respect of the degree of control and the unique link that the signature is to have with the person to whom it is vested are quite high. This standard is necessary if the QES is to be truly the functional equivalent of a manuscript signature.

4. DIGITAL SIGNATURES – TECHNOLOGICAL BACKGROUND

A digital signature is data affixed to or a cryptographic transformation of a data unit which allows the recipient to prove the source and integrity of the data unit.[33] The Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) project defines a digital signature as being '*a digitised analogy of a written signature, produced by a cryptographic procedure acting (commonly) on a digest of the message to be signed*'.[34]

---

[31] Commission, 'Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures' COM (2006) 120 final, 6.

[32] Ibid, Annex IV.

[33] Mason, S, 2012, Electronic Signatures in Law, 3rd edition, Cambridge University Press, para 10.4.

[34] Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC), 'Glossary - Digital Signatures' <http://ec.europa.eu/idabc/en/document/652/5892.html> viewed 14 January 2013.

While an electronic signature can take many forms, such as the typed name at the end of an email, a digital signature is the product of a mathematical equation known as an algorithm. An algorithm applies cryptography to conceal data disguising the plaintext message so that the message has no ordinary meaning. In practice the plaintext message is converted into an unintelligible alphanumeric text.

Cryptography can perform a number of roles that are relevant in an electronic conveyancing context. It can ensure the authenticity of the message, the integrity of the message, the confidentiality of the message and can prevent alterations to the message. In order to understand how a document can be signed electronically, it is necessary to understand how cryptography works.

There are two types of encryption; asymmetric and symmetric cryptographic systems. Symmetric cryptographic systems are conventional in that the data is encrypted using one encryption key and decrypted using the same key. Both the sender and recipient must agree on the key which is to be used to encrypt. This system is limited to use by trusted groups of users such as the government and the military. In such groups the key must be publically available to all. As such, the key cannot be distributed over an unsecure network if the authenticity and integrity of the message is to be retained.

Asymmetric cryptographic systems address the disadvantages with symmetric cryptographic systems. There are two keys in an asymmetric system; the public key and private key and the system is known as Public Key Infrastructure (PKI). The public key is used to encrypt the data and is available to the world at large while the private key is controlled by the parties. The private key algorithm is applied to the plaintext. This private key algorithm is also known as a hash function.[35] The private key algorithm is applied to the document to be signed and secondly it is applied to the signature of the individual or entity signing the document.[36] Once the plaintext is encrypted a computer application will derive an alphanumeric number from the encrypted data. This is known as the 'hash result' and once it is attached to the original message it becomes the digital signature.[37]

---

[35] Tupper, S, 2000 'From Seal to Cyber-Notary Uncertainty in Electronic Commerce and the Case for a Digital Signature Law in Michigan' 45 Wayne Law Rev. 237 (1999-2000), 256.

[36] Mason, S & Bohm, N, 2003, 'The signature in electronic conveyancing: an unresolved issue?' (2003) Conveyancer and Property Lawyer 460.

The recipient of a message encrypted using asymmetric encryption can verify that that the message did come from the sender and that it has not been altered since being sent by the use of a public key. The public key is obtained from a certification provider. The recipient's computer, using the public key checks the hash result against the digital signature on the sender's message. If the hash result matches the digital signature, the recipient can accept *prime facie* that the message is authentic, was not altered since being sent and was signed by the party who clams to have signed it. If the recipient is required to sign the document also, which is the case with some deeds involving land where both parties are prejudiced in some manner; the recipient repeats the above process using their private key.

Parties may create their own public and private keys. However, no matter how secure these keys are, a third party will insist on independent verification of the authenticity and integrity of the message. Therefore, an independent certification authority is required. The certification authority will issue the public key which would enable either party wish to verify the transaction.

The certificate is proof of the public key being associated with the sender and when taken in conjunction with the digital signature and hash function, it would be sufficient proof of intention to satisfy conveyancing law requirements.[38]

The complexity of the encryption algorithms are such that an individual would not be able to commit them to memory. As a result a private key would need to take the form of a token. However, control of the private key is an issue. Mason has noted that '*the greater the security of the mechanism does not, in fact, offer the subscribing party any protection against attacks, such as the theft of a key of the corruption of a terminal*'.[39]

In addition,[40] if the private key is not uniquely linked with the signatory as it may be removed from or lost by the subscribers with relative ease. A smart card with the private key in an embedded chip could, if combined with additional security features, provide a higher level of authentication. Such a system could involve the holder of a smart card containing the

---

[37] Tupper, S, 2000 'From Seal to Cyber-Notary Uncertainty in Electronic Commerce and the Case for a Digital Signature Law in Michigan' 45 Wayne Law Rev. 237 (1999-2000), 256.

[38] Ibid, 258.

[39] Mason, S, 2012, Electronic Signatures in Law, 3rd edition, Cambridge University Press, para 15.10.

[40] See para 4.28 supra.

private key validating the private key using a card reader which would be connected through the internet to the certification provider. The holder of the smart card would be required to enter a personal identification number to enable the card. Alternatively the private key could be contained on a USB memory stick.

The future of digital signatures lies with digital identity cards containing biometric data and PKI. Research conducted on behalf of the digital identity card industry predicts that the number of electronic identity cards will exceed traditional identity cards by 2015.[41] Sweden recently began to introduce digital identity cards that will contain the holder's photograph, fingerprints and electronic signature. This data will be gathered by a private company through enrollment kiosks which will enable instant capture.[42]

Emerging economies have embraced digital identity cards which incorporate biometric data. The Indian government launched the unique identity scheme (UID) in 2010.[43] The UID will involve the gathering of biometric data from 1.2 billion citizens and is the largest biometric identity scheme in the world. Each digital identity card will include the personal and demographic details of the resident and will be associated with their iris and fingerprint biometric information. Biometric identifiers are used to generate a unique identifier number (UIN). When citizens need to authenticate their identity, they must provide their UIN and biometric data, which is verified using data held.[44] Biometrics offers the advantage of a strong link to the signatory and can authenticate an individual in the physical domain.[45]

The Estonian government has championed sustainable development through technology. Digital identity cards, which are not obligatory, contain a digital signature. In addition, each holder of a digital identity card receives an official e-mail address which is intended for use official correspondence with government authorities and is recognized as the citizen's of-

---

[41] Acuity Market Intelligence, The Global National eID Industry Report' (2010) <http://www.acuity-mi.com/GNeID_Report.php> viewed 14 January 2013.

[42] Gemalto, 'Sweden Renews Multi-Year Contract on ePassports and eID Cards with AB Svenska Pass, a Gemalto Company' <http://www.gemalto.com/php/pr_view.php?id=973> viewed 14 January 2013.

[43] The Economist, 'Reform by numbers' (London, 14 January 2012) <http://www.economist.com/node/21542814> viewed 29 July 2012. See also The Economist, 'India's identity scheme: The magic number' (London, 14 January 2012) <http://www.economist.com/node/21542763> viewed 14 January 2013.

[44] Gemalto 'eID in India' <http://www.gemalto.com/digital_identity/india.html> viewed 14 January 2013.

[45] Pope, N, 2005 'Practical considerations in securing electronic signatures' Digital Evidence and Electronic Signature Law Review, vol. 2, p. 67.

ficial electronic residence.[46] In Lithuania an electronic conveyancing system is being developed where biometric information will be integrated with a digital signature to identify notaries.[47] These initiatives are seen as being in line with a broader European trend, which aims to integrate eGoverment services and identity cards.[48]

Technology has provided viable alternatives to the manuscript signature. Jurisprudence has focused on the function of the signature: to show intention and authenticate identity. This standard can only be fully met though the use of tokens such as smart cards which contain the required private keys and which are uniquely linked to and are under the sole control of the signatory. The use of biometric data to link the signatory and the smart card would satisfy the legislative requirements.

5. CONCLUSIONS

The jurisprudence relating to signatures illustrates that the role of a signature in evidencing intention and identity are key functions. Therefore, the form of the signature is irrelevant so long as the signature can be used to show the intention and identity of the signatory.

Conveyancing must be distinguished from common consumer contracts such as purchasing an airline ticket online. For most of society the purchase of a house is the most expensive transaction that they ever enter into. The formalities relating to the execution of deeds of transfer or conveyances or mortgages are justified on consumer protection grounds and the '*prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury and subornation of perjury*'.[49]

Therefore, the introduction of electronic conveyancing offers the prospect of making the conveyancing process much more efficient by transforming it into a paperless system.

The definition of the Qualified Electronic Signature (QES) provided in the ESD was apparently technologically neutral, but in practice favors PKI technology contained on tokens such as smart cards. As previously noted,

---

[46] AS Sertifitseerimiskeskushttp (Estonian State Certification Centre), 'The Estonian ID Card and Digital Signature Concept: Principles and Solutions', p 7. <www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf> viewed 14 January 2013.

[47] Stitlis, D Petrauskas, R & Rotomskis, I, 2006 'Implementation of Public E-Services for Immovable Property Contracts in Lithuania' Digital Evidence and Electronic Signature Law Review , vol 3, p 82.

[48] Ibid.

[49] Statute of Frauds (Ireland) 1695, preamble.

the ESD requires that the QES be uniquely linked with the signatory;[50] be capable of identifying the signatory[51] and can be controlled exclusively by the signatory.[52] It appears that not only does the ESD suggest the use of PKI smart cards, but that the smart cards were to take the form of an Electronic Identity Card (EID).

This understanding of the QES has been accepted in some European countries.[53] However, there is a lack of case law on the ESD which addresses this issue.[54] In addition there is 'currently no natural market demand for Qualified Certificates and related services'.[55] Examples of PKI systems that meet the high standards required in an electronic conveyancing context have not been introduced. As a result, the form that a digital signature should take in an electronic conveyancing system is far from clear.

It is important to note that the ESD merely obliges Member States to ensure that a QES is given the same legal status as a handwritten signature. The ESD does not regulate the legal use and consequences of a handwritten signature itself, and not the legal consequences of the QES.[56] As such, policy makers will need to consider whether a digital signature contained on a smart card will meet the requirements for a QES.

If policy makers introduce an electronic conveyancing system which relies on a form of QES that is not uniquely linked to and under the sole control of the holder, it is possible that the use of such a digital signature could be challenged on the basis that the form of digital signature used did not meet the standards required by the ESD.

These standards; the requirement for a signatory to be uniquely linked to the smart card and for that card to be under the signatory's sole control can in practice only be satisfied by an EID or another form of smart card that offers a quick and effective means of linking the holder and the card. Member states have a wide discretion in respect of the method used to link the signatory and the smart card. However, as can be seen, the trend in some EU states such as Sweden, Estonia and Holland is to include within EID a digit-

---

50 Electronic Signatures Directive Article 2(2) (a).

51 Ibid, Article 2(2) (b).

52 Ibid, Article 2(2) (c).

53 Pope, N, 2005 'Practical considerations in securing electronic signatures' Digital Evidence and Electronic Signature Law Review , vol. 2, p67.

54 Kelm, S, 2005 'On the implementation of the 1999 European Directive on electronic signatures' Digital Evidence and Electronic Signature Law Review , vol. 2 p. 9.

55 Ibid, p.10.

56 Ibid, p. 9.

al signature and biometric identifiers that would enable the person presented with such a card to verify that the holder of the card is one and the same as the person who is entitled to use the digital signature contained on it.

The conveyancing process requires a form of digital signature which is both legally and technically the equivalent of a manuscript signature. The definitions and principles provided in the ESD foresee a form of digital signature uniquely linked to and under the sole control of the signatory. While there is an understanding of digital signatures in a legal and technical context, the practical implementation of these requirements has not been addressed. Therefore, legislators will need to ensure that the digital signature model introduced is one that can conclusively link the signatory with the digital signature contained on a smart card or token. This requirement could be met by the introduction of a smart card which provides a means of conclusively verifying that the person presenting the card is entitled to use the digital signature contained in the card. While this may be seen as impractical due to cost implications and other factors, it is necessary that the form of digital signature to be used in the electronic conveyancing process remains faithful to the function of the manuscript signature.