

<input type="checkbox"/> E Law	<input type="checkbox"/> Search	<input type="checkbox"/> Subscribe	<input type="checkbox"/> Issue	<input type="checkbox"/> Subject	<input type="checkbox"/> Author	<input type="checkbox"/> Title
<input type="checkbox"/> Murdoch						

E LAW | Murdoch University Electronic Journal of Law - [Copyright Policy](#)

FORMAT:

The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures

Authors: [Sharon Christensen LLB \(Hons\), LLM](#)

Gadens Professor in Property Law, Queensland University of Technology Faculty of Law

[William Duncan LLB, LLM](#)

Professor, Queensland University of Technology Faculty of Law

[Rouhshi Low](#)

Senior Research Assistant, Queensland University of Technology Faculty of Law

Subjects: [Contracts Law and Legislation](#) (Other articles)

[Electronic Commerce](#) (Other articles)

[Electronic Commerce Law and Legislation](#) (Other articles)

Issue: [Volume 10, Number 4 \(December 2003\)](#)

Category: [Refereed Articles](#)

Contents:

- [Introduction](#)
- [Paper based signatures: Requirements at Common Law](#)
 - [What constitutes a signature at law?](#)
 - [Requirements of a valid signature under the Statute of Frauds](#)
- [Validity of electronic signatures as signatures under the common law](#)
 - [How can an electronic document be signed?](#)
 - [Does an electronic signature meet the functional requirements of a hand written signature?](#)
 - [Can a digital signature meet the functional requirements of the Statute of Frauds?](#)
 - [What is a digital signature](#)
 - [Does a digital signature have characteristics common to a handwritten signature?](#)
 - [What functions can a digital signature serve?](#)
- [Comparative analysis of electronic signature frameworks and their impact on Statute of Frauds requirements](#)
 - [UNCITRAL Model Law on Electronic Signatures](#)
 - [Overview of the Model Law on Electronic Signatures](#)
 - [Meeting the functional requirements of the Statute of Frauds](#)
 - [Australia: Electronic Transactions \(Queensland\) Act 2001](#)
 - [Overview of Legislation](#)
 - [Effect of applying the Electronic Transactions Act to the Property Law Act 1974 \(Qld\)](#)
 - [Meeting the functional requirements of the Statute of Frauds](#)
 - [United States](#)
 - [Overview of legislation](#)
 - [Meeting the functional requirements of the Statute of Frauds](#)
 - [European Union](#)

- **Overview of directive**
 - **Meeting the functional requirements of the Statute of Frauds**
- **New Zealand - Electronic Transactions Act 2002**
 - **Overview of legislation**
 - **Meeting the functional requirements of the Statute of Frauds**
- **Conclusions**
- **Notes**

Introduction

1. Many countries such as the United States, the European Union, United Kingdom, New Zealand and Australia have introduced legislation to facilitate the increased usage of the Internet as a medium for contracting. The use of the internet for commercial transactions involving the sale of goods, aside from the question of security, requires only minor adjustments to the contractual law principles which apply to the transactions. In contrast, the use of the Internet for land transactions is hampered by the need to reconceptualise the accepted notions of writing and signature for use in electronic transactions. In most common law jurisdictions the Statute of Frauds imposes a requirement for land transactions to be in writing and signed by the party to be charged. This article examines the development of the legal requirements for a signature in paper based land contracts in Australia using Queensland as an exemplar for other Australian jurisdictions and considers the following issues, in particular
 - the conditions required by the Statute of Frauds for a valid signature;
 - whether an electronic signature affixed to an electronic contract can serve the same functions as a manuscript signature for the purposes of the Statute of Frauds;
 - different frameworks developed for regulating electronic signatures and the degree to which these frameworks meet the functional requirements of the Statute of Frauds.
2. The article propounds the view that current Australian legislation purporting to validate electronic transactions provides inadequate protection to parties entering electronic land transactions. The Australian legislation does not change the substantive requirements of the Statute of Frauds but purports to mandate the validity of electronic signatures provided certain criteria are met. It is suggested that the criteria, when examined in light of the reasons for signing a document in accordance with the Statute of Frauds, are insufficient to ensure an electronic signature meeting those requirements performs the same functions as a manuscript signature. The article urges the adoption of the two tiered approach in the Model Law on Electronic Signatures, Article 6 of which provides standards against which technical reliability of electronic signatures may be measured without limiting the availability of the flexible criterion embodied in Article 7 of the UNCITRAL Model Law on Electronic Commerce, which is reflected in the current legislative framework in Australia.

Paper based signatures: Requirements at Common Law

What constitutes a signature at law?

3. Very little judicial or academic comment exists to define a signature. It is suggested that this is because it is universally understood that a signature is a signatory's name written in their own hand on a piece of paper.^[1] However, in some cases courts have accepted a range of signatures including crosses, initials, printed names and rubber stamps all by analogy with a written signature.^[2] This was achieved by determining if the method had already been recognised as valid and if not, whether it was acceptable in the particular circumstances. No reasons or general principles were given, with the court in each case merely satisfying itself

that the method achieved the same purpose as a personal signature.[3]

4. Several authorities have considered the meaning of 'signed' at common law. It is clear that modern authorities are more concerned with whether the particular signature fulfils the function of a signature as intended by the legislation rather than whether the signature is in a particular form. Sir Raymond Evershed MR in *Goodman v J Eban*[4] stated that:

"It follows, then, I think, that the essential requirement of signing is the affixing, either by writing with a pen or pencil or by otherwise impressing on the document, one's name or signature so as personally to authenticate the document"

5. Romer LJ in the same case agreed stating:

The first reaction of many people, I think, would be that the impression of a name produced by a rubber stamp does not constitute a signature, and, indeed, in some sense, is the antithesis of a signature. When, however, the matter is further considered in the light of authority and also of the function which a signature is intended to perform one arrives, I think, at a different result." [5]

6. In summary, the authorities indicate a concern to ensure that the function of requiring a signature is met by whatever method is used, but to date, the ordinary meaning of signature as being a mark on a written document has prevailed in the authorities.

Requirements of a valid signature under the Statute of Frauds

7. The Statute of Frauds requires that particulars documents be signed. An examination of the cases shows that the fact an actual signature is not the result of the act of signing is not critical to the validity of the document. Even a form with a signature impressed upon it by a printing machine[6] or where the person signing places upon the document an engraved representation of that person's signature by means of a rubber stamp[7] have been held to satisfy the statutory requirement of a signature. A telex signature has also been held to be sufficient to constitute a proper signature.[8] The critical element appears to be that the signature must also contain the additional characteristic that the person making the mark approves of the contents of the document.
8. The mere existence of a person's name in a document without the characteristic of adoption of the document or approval of its contents, will not be a signature for the purposes of the Statute of Frauds because it does not effectively authenticate a document. Thus, a printed name in the body of an instrument to operate as a signature must be authenticated by the person to be charged.[9] This view appears to have been followed in Australia.[10] By this authentication, the party to be charged must expressly or impliedly indicate that he or she recognises the writing so containing his or her name or initials as being an expression of the will to contract. [11]
9. In Queensland[12] s 59 of the Property Law Act 1974 (Qld) provides for a contract or memorandum to be "signed" by the party to be charged. The Acts Interpretation Act 1954 (Qld) defines "sign" as including "the attaching of a seal and the making of a mark", but does not define signature. Under the Statute of Frauds as reflected in s 59 of the Property Law Act 1974 (Qld), a signature serves the following functions:
 - i. it identifies the signatory; and
 - ii. evidences the party's approval of the contents of the document; [13] and
 - iii. provides integrity for the contract between the parties ensuring the reliability and admissibility of the parties' agreement in a court.[14]

10. Underlying the ability of a signature to serve these functions are several important characteristics:
- i. a signature is usually affixed through a physical process by the signatory or a person authorised by the signatory;
 - ii. a signature can be affixed by mechanical means unless prohibited;
 - iii. a signature is relatively difficult to effectively forge;
 - iv. the signature becomes affixed to the document such that the signature, document and contents become one composite physical thing;
 - v. a signature is relatively difficult to remove without a trace;
 - vi. can be reproduced by a party and is relatively standard for all documents signed by the same person.^[15]
11. Given that these particular characteristics result in the fulfilment of certain functions, the challenge is whether an electronic version of a signature with similar characteristics will be able to fulfil the same functions. Before considering the application of current Australian and international legislation to the signing of a land transaction it is instructive to consider how an electronic signature would be viewed in the absence of specific legislative provisions validating its use.

Validity of electronic signatures as signatures under the common law

How can an electronic document be signed?

12. There are several ways that a party to an electronic contract may attempt to sign the contract:
- Using a manuscript signature which is scanned as an image into a word processing file so that the document may be printed out for transmission by post or otherwise;
 - Typing a name at the bottom of an email or document;
 - Using a digital signature
13. All of these methods may be generically termed electronic signatures as they are methods of affixing a form of authentication to an electronic document. This should be distinguished from a "digital signature" which is a specific form of electronic signature involving encryption.

Does an electronic signature meet the functional requirements of a hand written signature?

14. Each of the methods described above will have variable success in meeting the requirements for a valid signature at law. In all cases if the law were to require a signature to take the form of a mark on a document such that it could not easily be removed or reversed, no electronic signature could satisfy the requirement. This is due to the fact an electronic document is not a physical object and any method for signing in an electronic environment will not take the form of a permanent affixation to the document. As discussed later, even a digital signature is merely an extra set of bits attached to the document or logically associated with it and as such it may be possible to remove the signature.
15. Further difficulties with some forms of electronic signatures is that while they may make a mark on the document this mark does not necessarily identify the party, indicate the party's approval or become permanently affixed to the document. These difficulties were identified by Staughton J in *Clipper Maritime Ltd v Shirlstar Container Transport Ltd (the 'Anemone')*^[16] where his Honour considered whether a telex might satisfy the requirement for writing and

signature of a guarantee for the purposes of the Statute of Frauds 1677. His Honour stated:

I reached a provisional conclusion in the course of the argument that the answerback of the sender of a telex would constitute a signature, whilst that of the receiver would not since it only authenticates the document and does not convey approval of the contents.[17]

16. While it was not necessary for his Honour to make a final decision in relation to this issue, acceptance at face value of the suggestion that an automated message could act as a signature ignores the following issues:
 1. the identification message of facsimiles and telexes only identifies the machine and not the identity of the sender;
 2. it is possible for a false identification message to be sent; and
 3. the contents of the message can be altered and replaced to be virtually untraceable.
17. In particular, using one of the first two electronic signature methods outlined above[18] will not satisfactorily evidence:
 - i. that the party placing the signature on the document was actually the person stated;
 - ii. that the person placing the signature on the document actually approves of its terms; or
 - iii. that the signature was not forged, placed on the document by another party or that the signature was not removed from one document and placed on a different document.
18. However, if emphasis is placed more on the function of a signature as developed in the authorities it may be possible to accept that an electronic document can be signed. The main functions served by a party signing a land transaction are to authenticate the document (that is to identify the party and the party's intent to enter the transaction) and to guard against a later fraudulent attribution of the transaction to a party. Of the methods described above only the final method could possibly equate functionally to a personal handwritten signature. If the courts were to view the principles developed in light of modern electronic communications and depending upon the type of technology used it may be possible to adopt the view that a digital signature authenticates the document and, therefore, will be functionally equivalent to a personal signature.
19. Therefore, while a document may be signed in a number of different forms, the Statute of Frauds would require an electronic signature to have the following key characteristics:
 - it should be capable of being affixed to the electronic document and making a mark on the document;
 - it must indicate the party's approval of the contents of the document;
 - it must be capable of identifying the party who has affixed the signature;
 - it must have the same quality of integrity as a written signature such that if the signature has been removed from the document, falsely affixed to the document, forged by another party or the contents of the document have been altered this could be easily established where the reliability of the document is called into question.

Can a digital signature meet the functional requirements of the Statute of Frauds?

What is a digital signature

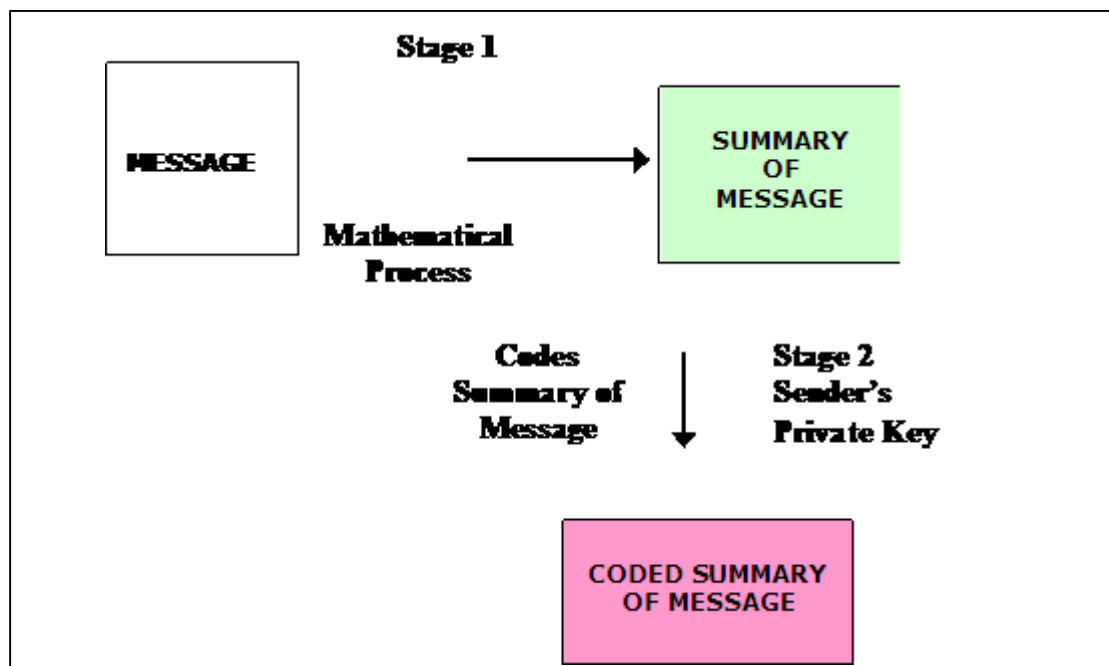
20. A digital signature using public key or dual key cryptography is operated using two keys, a

private key and a public key. The private and public keys are referred to as a public key pair. The keys will be two large prime numbers [19] mathematically related to each other but mathematically impossible to determine the private key by simply knowing the public key. The private key should be treated like a pin number and kept secret by the holder of the key.

Signing a document

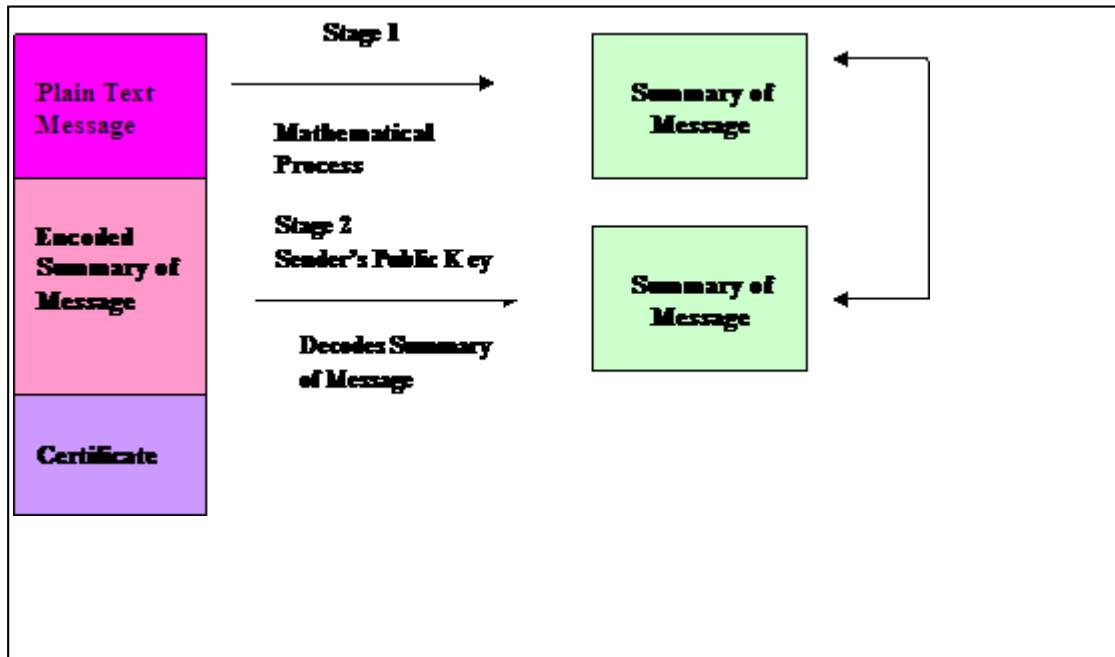
21. Firstly, a mathematical process (called a "hashing algorithm") is used to create a summary of the message. This summary will be unique to the message and it is highly improbable that two different messages will produce the same message summary. [20] This hashing mechanism is irreversible. The message will produce the same message summary every time the algorithm is used on the same text. Advantages of this process are:
 - the message summary is shorter and therefore quicker to decrypt; and
 - a small change in the text will produce a large change in the message summary.
22. Next the summary of the message is encoded with the sender's private key. The key will usually be contained on a smart card which is inserted into the sender's computer. Using the information on the card the computer performs a mathematical process which encodes the summary with the private key.

Diagram - Signing a document with a private key [21]



Decoding a document

23. The sender sends to the recipient the coded summary together with the plain text of the message and a certificate from a Certification authority which contains the sender's public key.
24. Next the recipient of the message creates a new summary of the plain text message using the same mathematical process (hashing algorithm) that was used in the first stage by the sender. Finally the recipient will use the public key of the sender to decode the coded message summary. The two summaries will be compared and if they are the same it is proved that the message was signed using the private key corresponding to the public key but this does not prove that the private key belongs to the sender. [22]

Diagram - Decoding a message with a public key [23]**Does a digital signature have characteristics common to a handwritten signature?**

25. As identified by McCullagh, Caelli and Little[24] a digital signature has certain physical characteristics:
- i. it is a series of bits that are attached to, or logically associated with another set of bits known as the digital document;
 - ii. it can easily be reproduced by the same person provided they have access to a computer, software, their private key and a digital document;
 - iii. it is easily verified by document receivers and independent third parties;
 - iv. are difficult to forge by third parties unless the forger has obtain access to the private key;
 - v. are not permanently bound to the document such that the contents of the digital document and the digital signature come one indivisible series of bits;
 - vi. involve a mathematical process;
 - vii. are exactly the same for all documents that are exactly the same when signed by the same person;
 - viii. are easy to remove without leaving a trace.
26. A digital signature will have the following characteristics in common with a handwritten signature:
- both signatures can be affixed through a mechanical means by the signatory or a person authorised by the signatory;
 - the difficulty of forging a handwritten signature and a digital signature are arguably similar, however, in the case of a digital signature stored on a smart card it could be stolen and used if the password is carelessly made available. A handwritten signature could not be copied in this way and any copy could be detected by an expert;
 - both signatures can be reproduced by a party and is relatively standard for all documents signed by the same person.
27. The characteristics of a handwritten signature that a digital signature does not possess are:

- A handwritten signature is affixed to a document using a physical process. It is arguable that this characteristic is not essential to the functions of authentication and integrity as affixation by mechanical means has been considered acceptable.
- A handwritten signature becomes affixed to the document such that the signature, document and contents become one composite physical thing. A digital signature is a series of bits that are attached to, or logically associated with another set of bits known as the digital document. In an electronic environment using current technology, a merging of the signature with the document will not occur. Whether this will prevent a digital signature from effectively authenticating a document or maintaining its integrity will depend on how easy it is to disassociate the signature from the document.
- A handwritten signature is relatively difficult to remove from the document without a trace. McCullagh, Caelli and Little[25] suggest that the technology is available for a fraudulent third party to be able to strip a digital signature from a document without a trace. Despite this flaw the authors go on to provide a variety of mechanisms that may be used to protect the digital signature or put the parties on notice that there may be a problem. This will be an important issue in a land transaction where the identity of the party is confirmed by the signature used;
- A handwritten signature will generally be a version of the signatory's name allowing for easy identification of the party. A digital signature will appear as a jumbled series of numbers somewhere on the document. This will not on its face identify the signatory but the fact the electronic document can be decoded using the public key of the signatory and the subsequent verification of the identity of the person which that particular key allows for proof of the identity of the person who signed.

28. Despite the lack of an exact correlation between the characteristics of a handwritten signature and a digital signature the writers are of the view that given the current technology it is possible for a digital signature to perform the same functions as a handwritten signature.

What functions can a digital signature serve?

29. In the writers' view a digital signature is able to achieve the requirements of the Statute of Frauds in relation to the identity of the signatory, approval of the contents of the document and maintenance of the integrity of the document in the following ways:

○ Identity

30. Using a digital signature as described above only proves that the document was signed using a particular private key, it does not identify the signer. To establish the identity of the signer it will be necessary to refer to extrinsic evidence such as a certificate provided by a Certification Authority.[26] As stated above, after signing the message, the sender sends to the recipient the coded summary together with the plain text of the message and a certificate from a Certification Authority which contains the sender's public key. This certificate, which is also digitally signed by the Certification Authority contains the following:

- the signatory's public key;
- the signatory's name and email address;
- the Certification Authority's name and email address;
- the serial number of the certificate and its validity period

31. The need for a digital certificate does not in the view of the writers detract from the ability of a digital signature to identify the party signing, but it is one of the factors which make it necessary for legislative intervention to validate the use of digital signatures.

○ Approval

32. Once a digital signature is affixed approval of the contents of an electronic document should be assumed (as is the case for a handwritten signature).[27] However, there may be instances where a third party is able to affix the signature without the knowledge of the individual. An individual may keep a signature key stored on a physical token, such as a smart card, which is needed for the operation of the signature software. It may be possible for a third party, through the carelessness of the card holder (if they also have access to the password) to use the card and affix a person's signature on a document. This additional likelihood of a party's carelessness playing a part in the fraudulent use of a person's private key may persuade a court that the same assumption of approval should not be adopted for digital signatures. The court may require a party seeking to rely on the validity of the signature to adduce extrinsic evidence that the signature was applied with the signatory's authority.
33. Therefore, although a digital signature on its face is capable of proving the approval of a party to the transaction, a court may, given the untested nature of digital signature technology in a court, take a conservative view of the evidence required to prove approval of an electronic document.[28] This may necessitate the signatory where a dispute about attribution arises to provide evidence that the digital signature was not affixed with the signatory's authority or knowledge. It is the writer's view that the possibility of fraud does not detract from the functionality of a digital signature. These situations can be compared within physical media with the ability of a fraudulent individual to forge a signature or impersonate an individual. The fact that these types of fraud can be perpetrated have not historically affected the ability of handwritten signatures to perform an authenticating function.

- **Integrity**

34. The third function a digital signature is required to perform for the purposes of the Statute of Frauds is to indicate that the document has not been altered since it was signed. Within an electronic environment the question of integrity will involve two issues:
- Can a digital signature prove the integrity of the electronic document?
 - Given that a digital signature is not permanently merged with the electronic document, is it also necessary to ensure the integrity of the digital signature?
35. In relation to the first issue the integrity of the document can be determined using the one way hash function described above. The recipient decodes the coded message summary using the sender's public key. The two summaries can be compared. If the document has been changed after signing the two messages will be different and the recipient will know that the document has been altered.
36. The second issue arises because a digital signature is only associated with the document and does not become an indivisible part of the document in the same way as a handwritten signature. The signing of a document by a digital signature has been compared by McCullagh, Caelli and Little[29] to using a paper clip to affix a signature to a document. The paper clip can be removed without leaving a trace in the same manner that a digital signature can be removed from an electronic document. Despite this potentially fatal flaw, it is possible, as suggested by McCullagh, Caelli and Little[30] to ensure the integrity of the digital signature through encryption with the recipient's public key or through the use of a trusted third party who time stamps the lodgement of the message summary.

Comparative analysis of electronic signature frameworks and their impact on Statute of Frauds requirements

37. From the above discussion it can be seen that there exists some uncertainty as to whether an

electronic signature will be capable of matching the characteristics and functionality of a hand written signature. Arguably only a digital signature will be capable of fulfilling the requirements of the Statute of Frauds.

38. The following provides a comparative overview of the different approaches in defining an electronic signature and considers which approach best satisfies the functional objectives of a signature for the purposes of the Statute of Frauds. The frameworks used for this discussion are:
- UNCITRAL Model Law on Electronic Signatures. Although this is only a model framework and has no prescriptive force, it is useful for the purposes of this article to analyse its provisions as it could be adopted by Australia if found to satisfy the objectives of the Statute of Frauds, particularly so as Australia's Electronic Transactions Act is based on the UNCITRAL Model Law on Electronic Commerce and the Model Law on Electronic Signatures builds upon the signature provisions of the Model Law on Electronic Commerce.
 - The Electronic Transactions Act, Queensland. This legislation was chosen as an exemplar of the Australian framework.
 - The Uniform Electronic Transactions Act, United States. This legislation is discussed because it has a different definition of an 'electronic signature' to the Australian legislation.
 - The European Union Electronic Signatures Directive. This directive is an example of a two-tier approach which differs in terminology to the UNCITRAL Model Law.
 - Electronic Transactions Act, New Zealand. This legislation provides an example of a framework with a two tier framework for electronic signatures.

UNCITRAL Model Law on Electronic Signatures

Overview of the Model Law on Electronic Signatures

39. The UNCITRAL Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996 in furtherance of its mandate to promote the harmonization and unification of international trade law. The purpose of the UNCITRAL Model Law on Electronic Commerce is to offer national legislators a set of internationally acceptable rules that deals with the removal of statutory barriers to electronic commerce.
40. Following from the Model Law on Electronic Commerce, the Model Law on Electronic Signatures was adopted in 2001, the purpose of which is to bring additional legal certainty regarding the use of electronic signatures.^[31] The Model Law on Electronic Signatures has no prescriptive force but is intended to serve as a model law for member states in the enactment of legislation dealing with electronic signatures. Thus far, only Thailand has adopted legislation based on the Model Law.^[32]
41. The Model Law on Electronic Signatures builds upon Article 7 of the Model Law on Electronic Commerce. It establishes a presumption that, where certain criteria of technical reliability are met, electronic signatures shall be treated as equivalent to hand-written signatures. The Model Law on Electronic Signature also contains basic rules of conduct dealing with responsibilities and liabilities that might bind upon the various parties involved in the electronic signature process, such as the signatory, the relying party and trusted third parties.
42. The Model Law on Electronic Signatures follows the two tier approach to authentication. The first and broader regime is that described in article 7 of the UNCITRAL Model Law on

Electronic Commerce. Article 7 recognises any electronic signature method that is applied for the purposes of signing a data message as fulfilling the legal requirements for a handwritten signature provided that it is sufficiently reliable in the light of all the circumstances. The second and narrower regime is that created by the Model Law on Electronic Signatures. It contemplates methods of electronic signature that may be recognized by a State authority, a private accredited entity, or the parties themselves, as meeting the criteria of technical reliability set out in article 6.

43. Article 6(3) lists the criteria to be satisfied in order for an electronic signature^[33] to be considered to be reliable. These are:

44. **(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person^[34]**

Under this requirement the linkage between the data used for creation of the signature and the signatory^[35] is the essential element. Thus although the signature creation data can be shared with different users, the signature creation data must be capable of identifying one user unambiguously in the context of each electronic signature.^[36]

The term "signature creation data" is not defined in the Model Law on Electronic Signatures. According to the Guide to Enactment, the description covers those core elements which should be kept confidential in order to ensure the quality of the signature process.^[37]

45. **(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person**

Subparagraph (b) requires the signature creation data to be under the sole control of the signatory at the time when the signature creation data are used.^[38]

The Guide to Enactment provides an example of a situation where the signature creation data exists on a network and is capable of being used by a number of people. The network would presumably relate to a particular entity which would be the signatory. If the signature creation data were widely available, they should not be covered by the Model Law.

46. **(c) Any alteration to the electronic signature, made after the time of signing, is detectable**

Subparagraph (c) deals with the issues of integrity of the electronic signature. The purpose of this paragraph is to set forth the criteria to be met in order to demonstrate that a particular method of electronic signature is reliable enough to satisfy a requirement of law for a signature.

47. **(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.**

Subparagraph (d) deals with the integrity of the information being signed electronically. According to the Guide, it is intended primarily for use in those countries where existing legal rules governing the use of handwritten signatures could not accommodate a distinction between integrity of the signature and integrity of the information being signed. In subparagraph (d), the necessary linkage between the signature and the information being signed is expressed so as to avoid the implication that the electronic signature could apply only to the full contents of a data message.^[39]

Meeting the functional requirements of the Statute of Frauds

48. It is the writers' view that a signature meeting the requirements of Article 6 of the Model Law on Electronic Signatures will also satisfy the functions of a signature as required by the Statute of Frauds: such a signature will be capable of identifying the signatory,^[40] indicating the signatory's approval of the contents of the document as well as well proving the integrity of the electronic document.
49. However, one potential problem with the Model Law is that the conditions listed in article 6(3) are not the only method for establishing reliability of an electronic signature, article 6(4)(a) provides that reliability may be established in any other way.^[41] According to the Guide to Enactment, paragraph 4 is intended to "provide a legal basis for the commercial practice under which many commercial parties would regulate by contract their relationships regarding the use of electronic signatures".^[42] There is however no explanation or examples for what may consist as other ways for establishing reliability.

Australia: Electronic Transactions (Queensland) Act 2001

Overview of Legislation

50. The Electronic Transactions (Queensland) Act 2001 (Qld) is part of the national framework of electronic transactions legislation. Each of the States in Australia has passed an electronic transactions Act with provisions similar to the Electronic Transactions Act 1999 (Cth). The Commonwealth Electronic Transactions Act is based on the UNCITRAL Model Law on Electronic Commerce.
51. Section 14 of the Electronic Transactions (Queensland) Act 2001 (Qld) purports to deem the requirement under a State law for a signature to be met by an electronic signature which meets certain criteria. There are two broad requirements for an application of s 14:
52. **1. The signature of a person must be required by a "State law"**

Section 14 will apply where a State law, in this case s 59 of the Property Law Act 1974 (Qld), "requires" a signature. The primary question to be asked is whether s 59 of the Property Law Act 1974 (Qld) requires a contract or memorandum to be signed.^[43] Section 59 simply provides that a contract will not be enforceable unless it is in writing and signed by the party to be charged, but it does not actually "require" that the contract be in writing or signed.^[44] To overcome this problem the word "require" under s 14 of the Electronic Transactions Act would need to be broadly interpreted to include not only a positive obligation but also a where failure to comply will result in an invalid transaction. It is suggestion that it is possible to take a wide view of requirement as being either a command or the provision of negative consequences if the document is not signed.^[45]

53. **2. The signature method used must meet the following criteria:**

54. *(a) the method used identifies the person and indicates the person's approval of information;*

The explanatory memorandum to the Queensland Electronic Transactions Act does not explain what is required by this condition. Guidance can be obtained from the explanatory memorandum to the Electronic Transactions Act 1999 (Cth) which^[46] provides that this condition merely requires that the signature method used must allow a person to indicate his/her approval of the information contained in the communication.^[47] This can then be used to establish that person's intention to apply his/her signature to the information contained in the electronic communication. In establishing the person's identity the signature method need not necessarily be a unique identifier, but it must identify that person sufficiently for the purposes of that communication.

55. *(b) the method used is as reliable and appropriate for the purpose for which the information is communicated;*

According to the Explanatory Memorandum to the Commonwealth Electronic Transactions Act, the reliability and appropriateness of the signature method is to be determined having regard to all the relevant circumstances at the time the signature method was used to sign the electronic communication. This requirement is intended to ensure that a signature method that was appropriate at the time it was used is not later rendered invalid.^[48]

With regard to this condition, the purpose of the Property Law Act 1974 (Qld) in requiring a signature and the functions that the signature serves will be relevant to any consideration of reliability and appropriateness. A crucial factor will be the ability of the signature method to authenticate the document and maintain the integrity of the document for later reference. As discussed, this can be achieved where a digital or biometric signature is used.

56. *(c) the person to whom the signature is required to be given consents to the requirement being met by using the method*

Section 59 merely requires the signature of the party to be charged to appear on the document, there is no requirement for the signature to be given to a particular person. The party to be charged may ultimately be either of the parties to the transaction. It is therefore suggested that both parties will need to consent to the method being used. The type of consent that will be acceptable under this section may be narrower than s 11 as the person needs to consent to "the method". For proper consent to be given the person will need to know what method is being used. Accordingly, consent may occur expressly or due to a previous course of dealing.

Effect of applying the Electronic Transactions Act to the Property Law Act 1974 (Qld)

57. If the above conditions are satisfied, s 14 then provides that the requirement for a signature will be "taken to have been met for an electronic communication". This deeming provision will not however, prevent the signature from being challenged as a forgery in the same way as a manuscript signature. The only effect is that the signature cannot be challenged merely because it is in electronic form. It must still meet the functional requirements identity, approval and integrity as reflected in s 59 of the Property Law Act 1974 (Qld).

Meeting the functional requirements of the Statute of Frauds

58. As indicated above, one of the primary objects of s 59 (and other Statute of Frauds equivalents) is to prevent fraudulent practices. Thus one problem with s 14 is that it only requires the method used to indicate the person's approval of the information communicated. It does not require that the integrity of the information be protected.^[49] One issue for a party agreeing to use an electronic signature method is whether the method is sufficiently reliable in the circumstances. This could be an area in which the court and the parties disagree with dire consequences for the validity of the agreement.
59. Secondly, s 14 does not expressly require that the signature method must be contained in the electronic communication itself. The Commonwealth Explanatory Memorandum does however provide that the signature method used must be linked with the communication in some way in order to indicate the person's approval of the contents of the communication.^[50] There is however no explanation as to what is required for the signature to be linked with the communication.
60. Thirdly, there is no specific condition requiring that the signature method be able to detect any subsequent alterations to the document since it was signed. This can be contrasted with the

European Union Directive on Electronic Signatures and the UNCITRAL Model Law on Electronic Signatures discussed below which specifically requires that any subsequent change of the data should be detectable.

61. Finally the current definition in s 14 does not distinguish between signatures placed on the document by the signatory or those placed by a third person.
62. These problems highlight one of the difficulties in using a generic definition of a signature in a transaction where the signature traditionally was required to serve particular functions which can only be achieved by detailing a higher level of requirement. In the writers' view the uncertainties created by this general approach need to be addressed through providing more specific criteria for the type of signature which will be effective.[\[51\]](#)

United States

Overview of legislation

63. The National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Electronic Transactions Act in July 1999 for adoption by the states. The Uniform Electronic Transactions Act was drafted to conform with the UNCITRAL Model Law on Electronic Commerce. The purpose of the Uniform Electronic Transactions Act is to promote greater uniformity between the various state enacted regulations on electronic signatures. Prior to the Uniform Electronic Transactions Act, the majority of states began enacting electronic signature legislation on their own, thus creating a patchwork of various electronic signature regimes throughout the United States. Later in 2000, the United States Congress enacted the Electronic Signatures in Global and National Commerce Act 2000 (E-Sign Act) as an interim measure to ensure that each state will recognize the validity of electronic signatures until such time as all states have adopted the Uniform Electronic Transactions Act.[\[52\]](#) Both E-Sign and Uniform Electronic Transactions Act contain provisions specifying that electronic contracts and electronic signatures shall not be denied legal effect or enforceability because they are electronic. The two pieces of legislation overlap significantly but they are not identical. For the purposes of this discussion, the definitions of what is an "electronic signature" in both the E-Sign Act and the Uniform Electronic Transactions Act are similar.
64. Under the Uniform Electronic Transactions Act, an electronic signature is defined broadly in terms of adopting a symbol with the intent to sign the record.[\[53\]](#) Similar to the Electronic Transactions (Queensland) Act, the Uniform Electronic Transactions Act follows the principle of technology neutrality - no specific technology is required to be used in order to create a valid electronic signature. The critical element in the Uniform Electronic Transactions Act is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record. Thus, any form of electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record, will constitute an electronic signature under the Uniform Electronic Transactions Act so long as:
 - some affirmative step is taken by the signer, done with intent to sign the record;[\[54\]](#) and
 - the electronic signature is linked or logically associated with a record.[\[55\]](#)
65. Assuming that the requisite intent and association with the record, the following would qualify as an electronic signature:
 - A manual signature transmitted by facsimile;
 - Typed name;
 - Digitised picture or image of a manual signature;

- Alphanumeric string or asterisk;
 - Biometrics;
 - Digital signatures;
 - Clicking through a series of screens to affirm intention to make an Internet purchase; [56]
 - Clicking on a button labelled "I agree" or "purchase now"; [57]
 - Voice on an answering machine;
 - Including your name as part of an electronic mail communication or including the firm name on a facsimile.
66. The Uniform Electronic Transactions Act definition also requires that the electronic signature be linked or logically associated with the record. According to the prefatory notes and comments, in the paper world it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated. However since these tangible manifestations do not exist in the electronic environment, the electronic signature definition in the Uniform Electronic Transactions Act expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. [58]

Meeting the functional requirements of the Statute of Frauds

67. Although the drafting style and framework of the Uniform Electronic Transactions Act is more compatible with the terminology used by the Property Law Act 1974 (Qld) in respect of a land contract, it is the writers' view that the signature provisions under the Uniform Electronic Transactions Act are inadequate to ensure that the electronic signature used serves the same function as a manuscript signature as required under the Statute of Frauds for the following reasons. First, the Statute of Frauds requires that if the signature has been removed from the document, falsely affixed to the document, or forged by another party or the contents of the document have been altered, that this fraud must be capable of being easily established. The Uniform Electronic Transactions Act does not seem to require this in s 2(8).
68. Secondly, the Statute of Frauds also requires the signature to be capable of identifying the person who has affixed the signature, but the Uniform Electronic Transactions Act does not expressly provide for this, unless the phrase "executed or adopted by a person" can be read to mean that the signature must also be capable of identifying the person who has affixed it.
69. The third potential problem with this definition is that there is no explanation as to what is required for the electronic signature to be regarded as linked or logically associated with the record. For the purposes of the Statute of Frauds, it is obviously desirable that any changes in the signature be detectable. The wide meaning of "logically associated" means that a mechanism for detecting alteration will not necessarily be a feature of a signature meeting the requirements of the section.

European Union

Overview of directive

70. On 13 December 1999, the European Parliament and Council adopted the Directive of the European Parliament and of the Council on a Community Framework for Electronic Signatures. [59] Similar to the UNCITRAL Model Law on Electronic Signature, the Electronic Signatures Directive follows a two-tiered approach by "setting requirements for e-authentication methods with a certain minimum legal power ... and by attributing greater legal effect to certain widely used techniques." [60] The first tier of the Electronic Signatures Directive prohibits discrimination between handwritten and electronic signatures. Article 5 requires member States to ensure that an electronic signature [61] is not denied legal

effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.[62]

71. Consequently, the first level of the Electronic Signatures Directive accepts most electronic signatures on a technologically neutral basis, similar to the UNCITRAL Model Law on Electronic Commerce. The second tier of the Electronic Signatures Directive accords an "advanced" electronic signature with the same legal effect as a manuscript signature on a paper document. An advanced electronic signature must satisfy the following requirements:

1. it is uniquely linked to the signatory;
2. it is capable of identifying the signatory;
3. it is created using means that the signatory can maintain under his sole control; and
4. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable[63]

72. An advanced electronic signature based on a "qualified certificate",[64] produces a rebuttable presumption that it "(a) [satisfies] 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; and (b) [is] admissible as evidence in legal proceedings".[65]

Meeting the functional requirements of the Statute of Frauds

73. It is the writers' view that a signature that meets the above requirements for an advanced electronic signature will also satisfy the functions of a signature as required by the Statute of Frauds. An advanced electronic signature will be required to be capable of identifying the signatory, indicating the signatory's approval of the contents of the document as well proving the integrity of the electronic document in the sense that a signature satisfying the requirements of an advanced electronic signature should be capable of detecting any subsequent alterations to the document since it was signed.

New Zealand - Electronic Transactions Act 2002

Overview of legislation

74. Similar to the Electronic Transactions (Queensland) Act 2001 (Qld), s 22 of the Electronic Transactions Act 2002 (NZ) makes provision for an electronic signature to fulfil a legal requirement for a signature.[66] Section 22 is consistent with s 14 of the Electronic Transactions (Queensland) Act 2001 (Qld) and sets out the same criteria of identity, approval, reliability appropriate to the circumstances and consent. However, the legislation goes one step further than the Queensland Act by including in s 24 a presumption for when the signature is as reliable as appropriate for the circumstances.[67]

75. These provisions mirror Article 6(3) of the UNCITRAL Model Law on Electronic Signatures, discussed above. The same issues discussed in that context apply to the New Zealand Act. The criteria listed for the creation of the presumption are consistent with the type of functionality expected for a signature under the Statute of Frauds, however a party is able to prove the reliability of the signature in other ways.[68] One disadvantage to this approach is that a signature which does not fulfil the criteria will not be presumed to be equivalent to a

manuscript signature unless proved otherwise. This may place undue requirements on parties wishing to enter transactions or provide information where the type of formality required for a land transaction is not necessary.

Meeting the functional requirements of the Statute of Frauds

76. In the writers' view the New Zealand framework is compatible with the Statute of Frauds and provides for an electronic signature that would fulfil the functions of a manuscript signature under that legislation.

Conclusions

77. This article refers to a number of model laws, directives and legislation which purport to implement legal frameworks which validate the use of electronic media and signatures for commercial transactions, including land transactions. In the introduction to this article, we propounded the view that current Australian legislation purporting to validate electronic transactions provides inadequate protection to parties entering electronic land transactions. The approach in the Australian legislation, is to mandate the validity of electronic signatures provided certain criteria are met. These criteria provide a minimum standard to which an electronic signature must adhere to be valid. However, when viewed in light of the reasons for requiring a signature on a land transaction under the Statute of Frauds these criteria are clearly inadequate to ensure a party to such a transaction is protected from fraud to the same extent as under a paper based transaction. It is submitted that the integrity of electronic land transactions can be improved by the introduction of a two tier concept as used in the Electronic Signatures Directive or the UNCITRAL Model Law on Electronic Signatures.
78. This view is also generally held amongst commentators in the United States. Generic first tier legislation does not address the issue of authenticity which would be required to satisfy the writing requirement of the Statute of Frauds and which requires more than the mere act of signing a document. Authentication goes directly to the integrity of the contents of the document which in a paper based medium is accomplished by each party having a counterpart of the document signed by the other party. This would not occur where a document remained electronic and was stored in a static format.^[69] Despite majority support for a two tier approach there is disagreement amongst American commentators. Some consider that electronic transaction legislation, whilst not mandating the use of electronic signatures, otherwise satisfies traditional contract law writing requirements including those under the Statute of Frauds as long as certain conditions are met under that statute.^[70] Other commentators, however, are far less sanguine about the application of this legislation and consider that something more is necessary before the mere existence of an electronic signature regardless of how it is generated that is whether it is a true digital signature created through public key infrastructure or merely a typed name in an email, will satisfy requirements of writing where these requirements are mandated by Statute of Frauds requirements.^[71]
79. While the writers' advocate this approach as the next step in Australia it is recognised that there are some difficulties which may impact on the integrity of electronic signatures under such a regime. Only certain types of electronic signatures namely digital signatures using PKI or biometric technology will satisfy the definition. A major criticism argued by some commentators,^[72] and endorsed by the writers, is the need for Public Key Infrastructure to be more fully developed including the certification processes. Government has shown a desire to remain outside of this process leaving commercial enterprises to take up the challenge. For this to occur on a large scale the operation of this infrastructure must be viewed as a viable business model before there would be investment in it. It is clear that in other countries such as Germany or Austria which have national electronic signature statutes, only a small number of private corporations operate Public Key Infrastructure which is required if second tier

regulation is to occur.^[73]

80. Despite the infancy of Public Key Infrastructure in Australia, it is suggested that the two tier concept as used in the Electronic Signatures Directive or the UNCITRAL Model Law on Electronic Signatures is preferable to the current definition used in the Electronic Transactions legislation in each State of Australia because it allows for flexibility- the first tier can apply to any type of electronic signatures. The second tier requires more stringent conditions to be fulfilled and those conditions satisfy the functionalities required of a signature under the Statute of Frauds. Since the electronic signature provisions in both the Commonwealth and State Electronic Transactions Acts are based on article 7 of the UNCITRAL Model Law on Electronic Commerce, one option for Australia would be to adopt the Model Law on Electronic Signatures. The Model Law on Electronic Signatures through article 6 provides standards against which the technical reliability of electronic signatures may be measured without limiting the availability of the flexible criterion embodied in article 7 of the Model Law on Electronic Commerce. However, until Public Key Infrastructure is developed in Australia, so that issues of authentication and security in signature requirements are addressed, the various iterations of the electronic transactions legislation in Australia, exemplified by the Queensland Electronic Transactions (Qld) Act 2001, provide little assistance in assuring the integrity of electronic land transactions.

<input type="checkbox"/> E Law	<input type="checkbox"/> Search	<input type="checkbox"/> Subscribe	<input type="checkbox"/> Issue	<input type="checkbox"/> Subject	<input type="checkbox"/> Author	<input type="checkbox"/> Title
<input type="checkbox"/> Murdoch						

Document author: Sharon Christensen, William Duncan and Rouhshi Low
Document creation: December 2003
HTML last modified: December 2003
Authorised by: [Archie Zariski](#), Managing Editor, E Law
[Disclaimer & Copyright Notice](#) © 2003 [Murdoch University](#)
URL: http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104_text.html

Notes

[1] Refer to Reed C "What is a Signature?" 2000 (3) Journal of Information, Law and Technology located at <http://elj.warwick.ac.uk/jilt/00-3/reed.html> See also the words of Denning LJ in Goodman v Eban [1954] QBD 550 at 56 "In modern English usage when a document is required to be "signed by" someone that means that he must write his name with his own hand upon it."

[2] Refer to R v Moore Ex Parte Myers (1884) 10 VLR 322.

[3] In re Clarke 27 LJPM&A 18 (illiterate testator made his mark on will but wrong name written against the mark - extrinsic evidence admitted to show true identity of maker of mark); in re Field Curt 752; Baker v. Denning 8 A&E 94 (signature valid even though signatory could write his name), In re Doe d. Phillips v. Evans 2 LJ Ex 19 (signature by seal valid for purposes of Insolvency Act); In Re Byrd Curt 117 (signature by seal invalid for purposes of Wills Act); Schneider v. Norris 2 M&S 286.

[4] [1954] 1 QBD 550 at 557. This case involved a solicitor's bill which had been signed with a facsimile of the firm's name imposed by a rubber stamp.

[5] [1954] 1 QBD 550 at 563.

[6] Re a debtor (No 2021 of 1995) [1996] 2 All ER 345 at 349 per Laddie J.

[7] Goodman v J Eban Ltd [1954] 1 QB 550 at 55 per Lord Evershed MR.

[8] Standard Bank London LTD v The Bank of Tokyo [1995] 2 Lloyd's Report 169.

[9] Cohen v Roche [1927] 1 KB 16 at 176 per McCardie J.

[10] Farrelly v Hircock (No 1) [1971] QdR 341 at 356 per Wanstall J (as he then was).

[11] Williams J, The Statute of Frauds, Section 4 - In the Light of Its Judicial Interpretation, supra at 87-88.

[12] Similar provisions exist in other States of Australia: [insert comparative provisions]

[13] Tiverton Estates Ltd v Wearwell Ltd [1975] 1 Ch 146.

[14] Leeman v Stocks [1951] 1 Ch 941 at 947-948.

[15] For further discussion of the characteristics of a signature refer to McCullagh A, Caelli W, Little P, "Signature Stripping: A Digital Dilemma" 2001 (1) Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html>

[16] [1987] 1 Lloyd's Rep 546.

[17] Ibid at 554.

[18] That is placing a scanned signature or typing a name on a document.

[19] There are several different technologies used to create digital signatures. See A McCullagh, "Legal Aspects of Electronic Contracts and Digital Signatures" in Going Digital 2000: legal issues for e-commerce, software and the internet, Fitzgerald A, Fitzgerald B, Cifuentes C, Cook P (ed), St.

Leonards, NSW, Prospect Media, 2000 at 195.

[20] The message summary may be referred to by a variety of names including "hash value", "message digest", "cryptographic check" or even a "seal".

[21] See Faber D, Digital Signature Guidelines, Judicial Studies Board, July 2000.

[22] This issue is discussed below.

[23] Ibid.

[24] McCullagh A, Caelli W, Little P, "Signature Stripping: A Digital Dilemma" 2001 (1) Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html>

[25] McCullagh A, Caelli W, Little P, "Signature Stripping: A Digital Dilemma" 2001 (1) Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html>

[26] The Certification Authority will need to be a trusted third party that has established appropriate security procedures for the identification of parties applying for keys, maintaining the currency of the certificates given and maintaining security in the creation of private and public keys. In Australia, the government has rejected the establishment of government regulated Certification Authorities. The government has proposed the establishment of the National Electronic Authentication Council (NEAC) to develop appropriate policies that the certification industry in Australia will be required to meet.

[27] See *L'Estrange v Graucob* [1934] 2 KB 394, *Saunders v Anglia Building Society* [1971] AC 1004.

[28] This view is consistent with the Electronic Transactions legislation, which provides for an electronic communication sent by a party to be attributed to that party only if it was sent with that party's authority. Refer to s 26 Electronic Transactions (Queensland) Act 2001 (Qld).

[29] McCullagh A, Caelli W, Little P, "Signature Stripping: A Digital Dilemma" 2001 (1) Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html>

[30] McCullagh A, Caelli W, Little P, "Signature Stripping: A Digital Dilemma" 2001 (1) Journal of Information, Law and Technology <http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html>

[31] The text of the Model Law on Electronic Signatures can be found on the UNCITRAL website at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf>

[32] Information on the status of texts can be found on the UNCITRAL website <http://www.uncitral.org/en-index.htm>

[33] The term "electronic signature" is defined in Article 2 as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".

[34] The Electronic Signatures Directive, discussed below, has a similar requirement, the difference being that the UNCITRAL Model Law on Electronic Signatures requires the signature creation data to be linked to the signatory, whereas the Directive requires the electronic signature to be linked to the signatory.

[35] The term signatory is defined as a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents: Article 2(d) Model Law on Electronic Signatures.

[36] An example of such a situation would be where several employees share the use of a corporate signature creation data. In such a situation, the signature creation data must be capable of identifying one user unambiguously in the context of each electronic signature.

[37] In the context of electronic signatures which are not digital signatures, the term "signature creation data" is intended to designate those secret keys, codes or other elements which, in the process of creating an electronic signature, are used to provide a secure link between the resulting electronic signature and the person of the signatory. An example is provided: in the context of electronic signatures based on biometric devices, the essential element would be the biometric indicator, such as a fingerprint or retina-scan data. In the context of digital signatures relying on asymmetric cryptography, the core operative element that could be described as "linked to the signatory" is the cryptographic key pair (the private and public keys). However, only the private key is covered by this description of "signature creation data". The text being electronically signed is also not covered by this description: UNCITRAL Guide to Enactment to the Model Law on Electronic Signatures 2001, para. 97.

[38] This is similar to the Electronic Signatures Directive. However, the UNCITRAL Model Law on Electronic Signatures requires the signature creation data to be under the signatory's sole control, whereas the Electronic Signatures Directive refers to the method used to create the electronic signature to which the signatory must maintain under his or her sole control.

[39] UNCITRAL Guide to Enactment on the Model Law on Electronic Signatures 2001, para. 126.

[40] The Electronic Signatures Directive requires that the electronic signature (to qualify as an advanced electronic signature) be capable of identifying the signatory. This requirement is not set out in the UNCITRAL Model Law on Electronic Signatures but is contained within the Model Law's definition of an electronic signature.

[41] Article 6(4): "Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature"

[42] UNCITRAL Guide to Enactment on the Model Law on Electronic Signatures 2001, para. 128.

[43] Similar provisions apply in other Australian jurisdictions: Imperial Acts (Substituted Provisions) Act 1986 (ACT), Sch 2 Pt 11 cl 4; Conveyancing Act 1919 (NSW), s 54A; Law of Property Act 2000 (NT), s 62; Law of Property Act 1936 (SA), s 26(1); Conveyancing Law of Property Act 1884 (Tas), s 9; Instruments Act 1958 (Vic), s 136; Statute of Frauds 1677 (Imp) (WA), s 4.

[44] Note that the signature provision of the UNCITRAL Model Law on Electronic Commerce (Article 7) specifically provides that its signature provision applies whether the requirement (where the law requires the signature of a person) is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

[45] See Sneddon M, "Legislation to facilitate electronic signatures and records: Exceptions, standards and the impact of the Statute Book" (1998) University of New South Wales Law Journal 334, 360.

[46] See section 10(1)(a) Electronic Transactions Act 1999 (Cth)

[47] Explanatory memorandum to the Commonwealth Electronic Transactions Act at p.31, it also recognises that some signature technologies such as digital signatures will also verify the integrity of the electronic communication, simply by the nature of the way they operate.

[48] Explanatory memorandum to the Commonwealth Electronic Transactions Act at p.32.

[49] See Explanatory Memorandum to the Commonwealth Electronic Transactions Act at p.31.

[50] See Explanatory Memorandum to the Commonwealth Electronic Transactions Act at p.31. An example is provided: a signature method may be applied to a communication but then transmitted as a packet of information separate to the communication. If the signature can be shown to indicate the person's approval of the information contained in the communication then the signature will satisfy the requirements in paragraph (a).

[51] A good example would be the UNCITRAL Model Law on Electronic Signatures or the Electronic Signatures Directive, both in this article.

[52] See <http://www.bmck.com/uetacomp.htm> for a list of states which have enacted the Uniform Electronic Transactions Act.

[53] Uniform Electronic Transactions Act 1999 (US) section 2(8): "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

[54] The Uniform Electronic Transactions Act does not say how this intention can be shown. The commentary to the Uniform Electronic Transactions Act simply states that the critical element is the intent to sign: "One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record": Uniform Electronic Transactions Act 1999 (US) comments to section 2, comment 7. The Uniform Electronic Transactions Act does describe attribution procedures which are used to verify that an electronic signature, message, or record is that of the person purporting to provide it: see s 9(a) of the Uniform Electronic Transactions Act.

[55] Manual signatures appear on the writing itself so are associated with the writing.

[56] See Uniform Electronic Transactions Act 1999 (US) comments to section 2, comment 7: "This definition includes as an electronic signature the standard webpage click through process. For example, when a person orders goods or services through a vendor's website, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks "I agree," the person has adopted the process and has done so with the intent to associate the person with the record of that process".

[57] Fry P, "Introduction to the Uniform Electronic Transactions Act: Principles, Policies and Provisions" (2001) 37 Idaho Law Review 237, 257; also see commentary: for example, when a person orders goods or services through a vendor's website, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks "I agree," the person has adopted the process and has done so with the intent to associate the person with the record of that process: Uniform Electronic Transactions Act 1999 (US) comments to section 2, comment 7.

[58] Uniform Electronic Transactions Act 1999 (US) comments to section 2, comment 7.

[59] Directive of the European Parliament and of the Council on a Community Framework for Electronic Signatures, European Parliament Document (1999/93/EC) (1999), OJ 2000 L13/12, [hereinafter Electronic Signatures Directive]. Date for compliance: 19 July 2001. In the United Kingdom, the Electronic Signatures Directive has been implemented by the Electronic Signatures Regulations 2002 and section 7 of the Electronic Communications Act 2000. The provisions of the Directive which are implemented by the Electronic Signatures Regulations relate to the supervision of certification-service-providers, their liability in certain circumstances and data protection requirements concerning them. Provisions in the Directive relating to the admissibility of electronic signatures as evidence in legal proceedings were implemented by section 7 of the Electronic Communications Act 2000.

[60] Spyrelli, C, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication" Journal of Information, Law and Technology 2002(2) <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html> .

[61] Electronic signature is defined in Article 2 as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".

[62] Electronic Signatures Directive, article 5.

[63] Electronic Signatures Directive, article 2(2).

[64] A qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II: see Article 2(10). A "certificate" is an "electronic attestation which links signature-verification data to a person and confirms the identity of that person": see Article 2(9).

[65] Electronic Signatures Directive, article 5(1).

[66] S 22 provides: (1) Subject to subsection (2), a legal requirement for a signature other than a witness' signature is met by means of an electronic signature if the electronic signature a. adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and b. is as reliable as is appropriate given the purpose for which, and the circumstance in which, the signature is required. (2) A legal requirement for a signature that relates to information legally requirement to be given to a person is met by means of an electronic signature only if that person consents to receiving the electronic signature.

[67] Section 24 provides: (1) For the purposes of sections 22 and 23, it is presumed that an electronic signature is as reliable as is appropriate if---

(a) the means of creating the electronic signature is linked to the signatory and to no other person; and (b) the means of creating the electronic signature was under the control of the signatory and of no other person; and (c) any alteration to the electronic signature made after the time of signing is detectable; and (d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(2) Subsection (1) does not prevent any person from proving on other grounds or by other means that an electronic signature--- (a) is as reliable as is appropriate; or (b) is not as reliable as is appropriate

[68] See s 24(2).

[69] Hartley J, "Electronic Signature and Electronic Records in Cyber-Contracting" (2003) 49 The Practical Lawyer 1 at 5.

[70] For example, Berenstein G and Campbell C, "Electronic Contracting: The Current State of the Law and Best Practices" (2002) 14 Intellectual Property & Technology Law Journal 1 at 4.

[71] Huey N, "E-mail and Iowa's Statute of Frauds: Do E-sign and UETA Really Matter? (2003) 88 Iowa Law Review 681 at 690; Broderick M, Gibson V and Tarasevich P, "Electronic Signatures: There Legal Now What?" (2001) 11 Internet Research: Electronic Networking Applications and Policy 423 - 434.

[72] Bell J, Gomez R, Hodge P and Mayer-Schonberger V, "Electronic Signature Regulation - An Early Score Card - Comparing Electronic Signatures Legislation in the US and the European Union" (2001) 17 Computer Law & Security Report 399.

[73] Ibid at 402.