

Legal Aspects of the PenOp[®] Signature under English Law

Dr Ian Walden[★]
Bird & Bird, solicitors

Published by:

PenOp Inc.
1212 Avenue of the Americas, 18th Floor
New York, NY 10036-1602
Tel: (212) 997-8800
Fax: (212) 997-8810

PenOp Limited
Vallis House, 57 Vallis Road
Frome, Somerset BA11 3EG
Tel: +44 (1373) 452755
Fax: +44 (1373) 452744

E-mail: info@penop.com
Web: <http://www.penop.com>

This report provides a general introduction to its subject matter. It is not intended to be exhaustive, nor can it provide the detail necessary to give guidance in relation to any specific problem. Appropriate professional advice should be sought in relation to any specific circumstances.

[★] Dr Ian Walden is a consultant to City of London solicitors Bird & Bird and is a Senior Research Fellow at the Centre for Commercial Law Studies, Queen Mary & Westfield College, University of London.

© Ian Walden, January 1998. All rights reserved.

Table of Contents

Executive Summary.....	1
Introduction.....	2
Defined signatures.....	3
Non-defined signatures.....	4
PenOp's Signature Capture Service.....	7
Verification - PenOp's Signature Verification Service.....	9
Admissibility.....	11
Probative value.....	12
Concluding remarks.....	13

Executive Summary

PenOp software enables the traditional hand-written signature to be directly transposed into an electronic environment, without the need to place additional technical or legal burdens upon the signing individual.

Through the use of a stylus upon a digitising pad, the PenOp software captures an individual's signature and securely links it to a specific electronic document. This signature can be verified, where necessary, and provides strong evidence if the contents of the signed electronic document are subsequently altered.

This report examines the legal validity of the PenOp signature under English law. Such validity is examined in terms both of complying with regulatory requirements for a 'signature' and as an item of evidence in the event of a dispute. For any particular application of PenOp software, the existence of specific regulatory requirements will need to be identified and complied with. However, the report concludes that for the vast majority of transactions, a PenOp signature should be legally valid, when implemented in an appropriate manner.

A PenOp signature also contains a number of security features which, in the event of a dispute, would provide substantial forensic evidence available for analysis where the authenticity of the captured signature was challenged.

Introduction

The exponential growth of electronic commerce over recent years has seen organisations expanding the range of activities, both transactional and internal processes, which are carried out electronically. Such activities are principally based around an interchange of communications with customers, trading partners and public authorities. A significant proportion of an organisation's communications will involve the explicit acceptance of certain legal commitments and obligations, such as agreeing contractual terms or the submission of a declaration to the tax authorities. In other cases, communications may give rise to implicit responsibilities, such as the accuracy of a statement made in an email message. Traditionally, organisations have expressed their acceptance of responsibility for certain obligations through the process of 'signing' documents. In an electronic commerce environment, this process can be replicated through the use of electronic signatures.

Concerns have been expressed, however, that electronic signature systems are not fully legally valid. Electronic signatures are not seen as having comparable legal efficacy to that possessed by traditional paper-based hand-written signatures. The practical consequences of such fears may be two-fold: organisations can be wary of implementing such technology or they may maintain parallel paper systems.

The legal validity of an electronic signature can be seen as comprising two separate aspects:

- the value that an electronic signature has in terms of complying with statutory or regulatory¹ requirements, and
- the acceptability of such techniques as evidence within a court of law.

PenOp is a biometrics-based electronic signature technique which replicates the traditional hand-written signature for use in an electronic environment, with the addition of certain security features. This report examines some legal aspects of the PenOp electronic signature, particularly in terms of meeting the requirements for legal validity.

The extent to which a PenOp electronic signature may comply with regulatory requirements will be examined in Sections 2, 3 and 4. Section 5 considers the manner by which a PenOp signature can be verified. Section 6 reviews the use of technical data generated by PenOp as evidence in court.

The report examines the legal issues from an English law perspective, although many of the points raised will be similarly relevant for consideration in other jurisdictions².

¹ A requirement for a signature may be based in primary or secondary legislation, or in other procedural rules laid down by authorities exercising statutory powers. In this paper, 'regulation' shall be used as a generic term covering all such legal sources.

² see Ben Wright's "The Legality of the PenOp[®] Signature", which examines the position under US law.

Electronic signatures as a legal 'signature'

When considering the legal validity of an electronic signature, it is necessary to identify the governing regulatory framework applicable to the particular legal act, for which the electronic signature is being used³. A basic distinction can be made between:

- legal acts which do not require a signature formality to be complied with, and
- legal acts for which an explicit or implicit statutory or regulatory requirement for a signature is laid down.

Any organisation intending to rely on the use of electronic signatures will need to identify into which category their activities fall when implementing a system⁴.

The vast majority of commercial contracts fall into the first category, not requiring formalities. In the absence of a regulatory requirement for a signature, the courts, in the event of a dispute, would only be concerned with the absence or presence of some form of 'signature' as an item of potential evidence to be used to help prove the authenticity and validity of a particular claim. In situations where there is no regulatory requirement for a 'signature', a PenOp signature should be as legally valid as any traditional manuscript signature, with the additional support of substantial technical data for use in evidence (see further below).

Within the second category, where a 'signature' is required, a further sub-division can be made between regulations which contain an specific definition of what a 'signature' is, and those regulations which simply state a requirement for a 'signature'. In the latter category, the courts have historically exhibited a flexible approach towards interpretation, being primarily concerned to recognise the intention of the party as signatory. Where a definition is explicitly laid down, the courts will have least flexibility in interpreting whether a particular form of signature complies with the requirement.

Defined signatures

Statutes often contain definitions for terminology used within the substantive provisions. In addition, the Interpretation Act 1978 contains definitions for interpreting a broad range of commonly-used statutory terminology. The Interpretation Act states that its definitions are applicable as the legal meaning of a term unless the precise wording of a particular statute or the context indicates a contrary position. The Interpretation Act does not contain a definition for a 'signature'.

A recent survey has found that some fifteen English statutes currently contain some definition for the term 'signature' or 'signing'⁵. Fortunately, in terms of consistency, twelve of them use the same, or similar, wording:

³ For the purpose of this report, a legal act is defined as any form of communication which gives rise to the explicit acceptance of certain obligations by the signatory.

⁴ It should be noted that PenOp may also be used in contexts which do not give rise to external legal obligations, such as for employee access to computer systems.

⁵ See Reed, C., *Digital Information Law*, Centre for Commercial Law Studies, 1996.

“signature’ includes a facsimile of a signature by whatever process reproduced”⁶
The word ‘facsimile’ would seem to require an exact copy of the hand-written signature to be created. This would, therefore, seem to preclude the possibility of substituting some form of code or data item as a form of legally valid signature, such as a Personal Identification Number (PIN) or a public-key digital signature⁷. In contrast, a PenOp signature captures and can store an exact graphic image of the hand-written signature as traced on the digitising pad, and would therefore seem to fall within this statutory definition.

Whilst a requirement for a ‘signature’ may not in itself be defined, in some regulations the signature requirement is linked with another formal requirement which may either prevent or impose limitations on the way in which an electronic signature may be used. By far the most common example is where a document is required to be ‘in writing’ and ‘signed’⁸. In the absence of a specific alternative regulatory definition, the Interpretation Act 1978 states that:

“writing’ includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form”.

Current opinion holds that the phrase ‘visible form’ would seem to preclude contracts being formed in an exclusively electronic form without reduction to physical form at some point in the transaction⁹. In such situations, therefore, an organisation incorporating PenOp into an electronic commerce application may need to ensure that any legally signed documents were produced in hard copy form, including the PenOp-captured signature, at some appropriate point in the transaction process. In an environment involving individual consumers, producing such hard copy would in any case also provide the consumer with a convenient paper record.

Non-defined signatures

In English law, where there is a requirement for a signature but no formal definition is provided within the regulation, an analysis of past case law has shown a fundamental distinction being drawn by the judiciary between regulations which require a ‘personal signature’ and other signature requirements¹⁰. Where a ‘personal signature’ is required some form of the signatory’s name is usually required, including a rubber stamp with a facsimile signature¹¹ and a person’s initials¹².

⁶ eg. Building Act 1984, s.93 and Food Safety Act 1990, s.49.

⁷ For a comparison between PenOp and public-key based signature techniques, see Ben Wright’s paper, “Alternatives for Signing Electronic Documents”, available from <http://www.penop.com>.

⁸ eg. Marine Insurance Act 1906, s.22.

⁹ eg. The Society for Computers and Law, Report of the Legislative Working Party “Digital Information and Requirements of Form”, May 1997.

¹⁰ Reed at 233. See also *Firstpost Homes Ltd. v. Johnson and other* (1995), The Times, 14.08.1995 for an examination of the signature requirement under the Law of Property (Miscellaneous Provisions) Act 1989.

¹¹ *Goodman v J.Eban* [1954] 1 All ER 763, [1954] 1 QB 550.

In the most recent case examining 'personal signatures', *Re a debtor*¹³, the court held that a faxed copy of a signed proxy form satisfied the 'signed' requirement under the Insolvency Rules 1986. The judge went on to consider whether a document signed by the signatory, using a signature "which has been scanned into the computer and is stored in electronic form", and only reduced to hard copy form by the recipient, would be valid. He held that such a document would be validly 'signed'.

It would therefore seem that, as with statutory definitions of 'signature', under certain UK regulations a distinction may potentially be drawn between the validity of electronic signatures systems which generate *copies* of a hand-written signature and signature mechanisms which create compilations of data to act as *equivalents* to the hand-written signature. A similar position has been echoed within other regulatory environments: eg.

- European Union regulations implementing the Single Administrative Document (SAD) include provisions allowing 'competent authorities', such as Customs & Excise:

"to replace the hand-written signature with another method of identification...which has the same legal consequences as a hand-written signature."¹⁴

Such alternative mechanisms are only permissible, however, where they met any 'technical-administrative conditions' laid down by the authority.

- In the US, the Federal Drug Administration's Final Rule on Electronic Signatures lays down a distinction between electronic signatures and hand-written signatures, with additional procedures being required where electronic signatures are used. Section 11.3(b)(7) states:

"Hand-written signature means the scripted name or legal mark of an individual hand-written by that individual.... *The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark*"¹⁵ (emphasis added)

In such environments, an appropriately implemented PenOp system would seem to clearly fall within the notion of a 'hand-written' signature and should not need to comply with the additional conditions.

¹² English legislation also uses the term 'under the hand of' to denote an act of signing, eg. Law of Property Act 1925, section 136: "Any absolute assignment by writing under the hand of the assignor...".

¹³ (*No. 2021 of 1995*) [1996] 2 All ER 345.

¹⁴ Commission Regulation n°2453/92/EC of 31 July 1992 implementing Council Regulation 717/91/EEC concerning the single administrative document, O.J. L249, 28/08/92, art. 18.

¹⁵ Federal Register, Rules and Regulations, March 20, 1997 (Volume 62, Number 54), pp. 13429-13466. PenOp have produced a White Paper examining the applicability of the FDA Final Rule to PenOp signatures: see <http://www.penop.com>.

It is clear from an examination of statutory usage and case law relating to the legal nature of a 'signature' that the fundamental object of a signature is to indicate that the signatory *assents* to the content of the document. As stated in *Re a debtor*:

“to indicate, but not necessarily prove, that the document had been considered personally by the creditor and is approved of by him.”¹⁶

Directly arising from such assent, a signature will also *identify* the signatory¹⁷ and provide authentication as to the *integrity* of the document.

One traditional element of an indication of assent, reiterated through judicial opinion, has been the requirement for a signature to 'mark'¹⁸ the document or be 'affixed'¹⁹ to it. This need to establish such a link in terms of legal validity has an obvious evidential purpose.

In a digital environment, it is highly debatable whether an electronic signature can be said to strictly 'mark' a digital document in any physical sense, although affixing may be seen to occur in certain situations²⁰. However, it would also seem reasonable to suggest that where a unique and secure logical relationship between an electronic signature and the document to which it applies can be proven, this should address judicial concerns and allow concepts of 'marking' and 'affixing' to be broadly interpreted to encompass such electronic signature techniques.

The manner in which the PenOp electronic signature achieves the features of assent, identity and document integrity is examined in the following sections.

¹⁶ Proof of *actual* intention would be an evidential issue for resolution at trial.

¹⁷ The signatory may be acting as agent on behalf of his principal (eg. an employee signing on behalf of his employing organisation).

¹⁸ In *Re a debtor*, Laddie stated: ‘..a proxy form is signed...if it bears upon it some distinctive or personal marking which has been placed there by, or with the authority of, the creditor.’

¹⁹ In *Goodman v J.Eban*, Evershed MR stated: ‘..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.’

²⁰ Where a PenOp signature is embedded within a document: eg. the PenOp[®] Microsoft Word[™] Component.

PenOp's Signature Capture Service

The PenOp Signature Capture Service records the signature traced by the signatory using a stylus upon a digitising pad. Signature capture is initiated within a particular application, such as Adobe Acrobat[™] or Netscape Navigator[™]²¹. Upon completion, the signatory has the opportunity view the image and to either approve the signature, retry or abort the process.

This act of signing is the point at which the signatory indicates his acceptance or approval of the contents of the document. PenOp directly translates the hand-written signature into an electronic environment. The traditional manner in which a signatory's assent is given is therefore retained. The captured signature may be embedded within the document itself, such as a word-processing file, or it may be stored separately in a database²².

The indication of assent by the signatory to the document is also supported by PenOp's Gravity Prompt[®] feature. It appears at the moment a person is asked to sign a document, through presentation of the PenOp Signature Capture Window. It provides an opportunity to present certain information to the person, such as a reminder that an expression of intent is being shown by the signatory through completion of the signature process.

The word content of the 'Gravity Prompt' is to be determined by the application developer. Documents giving rise to specific legal commitments (eg. a deed) may require a particular form of words in order to comply with regulatory requirements. Since the PenOp signature is intended to constitute a legal commitment by the signatory, the information conveyed in the 'Gravity Prompt' also has legal significance. An application developer will therefore need to seek appropriate legal advice when utilising this feature.

²¹ See further the case studies described in Annex 2 below.

²² eg. the PenOp[®] Documentum[®] Plug-in.

Integrity - PenOp's Biometric TokenTM

As a security mechanism, the PenOp electronic signature is designed to create a strong evidential link between:

- a person and his signature, and
- the signature and the signed document.

Establishing the link between the person and his signature is an evidential issue, based both on the forensic characteristics generated by the PenOp system itself (see Section 6 below) and other external circumstantial evidence relating to the act of signing (eg. location of the claimed signatory at the relevant time).

The manner in which PenOp establishes a secure link between the signature and the signed document is based on the generation of a unique biometric token. The nature of PenOp's Biometric Token both uniquely links the signature to the signed document and indicates whether the contents of the document have subsequently been altered. It is this latter feature which most closely relates to the integrity feature of a legally valid signature.

The Biometric Token is generated within the PenOp system at the moment the signature has been captured. It is a data item consisting of a number of discrete elements or data fields and representing the act of signing:

- the claimed identity of the signatory (eg. name or ID number)
- date and time stamp data
- identity of the hardware on which the signature was recorded
- measurement statistics relating to the captured signature
- the wording displayed by the Gravity Prompt (see Section 3 above)
- the image of the signature²³
- a document and an integrity checksum

The document checksum is a string of data calculated from the data comprising the document. PenOp uses the MD5 digest algorithm developed by RSA Data Security Inc.. The integrity checksum is the last component of the signature capture operation. The other fields of the Biometric Token are encrypted temporarily and a one-way hash of this data is calculated, again using the MD5 digest algorithm. This figure constitutes the integrity checksum which is then incorporated into the Biometric Token and the whole token is encrypted and stored.

The document checksum is a mathematically unique representation of the document, therefore any change in the document subsequent to the time of signature would sever the mathematical relationship. As such it provides an extremely secure link between the signature and the document.

²³ This feature is optional. However, where the PenOp signature is designed to comply with a regulatory requirement for a 'signature', consideration should be given to its retention.

Verification - PenOp's Signature Verification Service

Verification of a signature, confirming that the person signing the document is who they say they are, is not generally considered to be a requirement with respect to the legal validity of a signature under English law. Verification is a data security feature providing the recipient with relative assurance and proof that the document has not been fraudulently signed.

As verification is not a requirement for legal validity, an organisation making use of an electronic signature system, such as PenOp, will need to decide whether such a feature should be implemented.

If the objective is to replicate, as far as possible, paper-based processes in an electronic environment, then verification may not be considered necessary. For example, paper-based tax returns are signed and submitted without verification by the recipient tax authority that the signature is genuine. In such situations, the nature of the legal act being executed by the signatory does not require on-line verification. Verification would only become an issue in the event of a subsequent dispute. Similarly, where a transaction involves payment, the recipient is likely to be much more concerned with the transfer of funds than whether the signature can be verified as genuine or not!

'Tested Telexes' as an electronic signature

In the case *Standard Bank London Ltd. v The Bank of Tokyo Ltd* (1995), the English courts were required to consider the extent to which a recipient could reasonably rely on a particular form of electronic signature. In the absence of a regulatory requirement, the court simply accepted expert testimony that 'tested telexes' were an accepted form of electronic signature in use in the banking industry.

However, the central issue concerned the nature of the obligation placed upon a recipient of such an electronic signature to *verify* its authenticity. The courts held that only "wilful blindness" by the recipient would have given rise to the imposition of liability in the event of fraud. In all other circumstances, the burden of risk clearly lies with the user of the electronic signature technique. The decision can be seen as encouragement to the use of electronic signatures, since the lower the burden placed upon a recipient to check the authenticity of a signature the more acceptable such techniques are likely to be.

However, if one objective of implementing an electronic signature system is to enhance the security present in existing paper-based procedures, then some form of verification service should be considered. Where an organisation *is* concerned to achieve signature verification, either contemporaneous to the act of signing or upon receipt of a signed document, PenOp provides a Signature Verification Service.

This service enables a user to compare a signature against a sample of previously recorded signatures. The system will check the signature and provide a score representing a statistical measurement of similarity between zero (poor) and a hundred (good). The organisation relying on such verification is able to set the threshold of acceptability appropriate to the underlying transaction.

The verification sample should contain a number of signatures designed to allow for a realistic degree of variance. The sample may be obtained through a variety of methods:

- during a single enrolment session, such as the point at which an account is opened ('session-based enrolment');
- collected over a period of time through a series of interactions ('absorption-based enrolment'),
- or carried out subsequent to a query relating to a particular signature event, such as a fraudulent tax return ('deferred enrolment').

The verification sample will need to be held on a system accessible by the relevant application. Where a communications profile is relatively closed, such as the submission of policy documents to an insurance company (ie. many-to-one) or internal compliance procedures (ie. one-to-many), the verification sample can be held by the party requiring verification. Where PenOp is being used in an open trading environment with a variety of 'unknown' trading partners, such as an Web-based procurement, then the verification sample could be held by an independent third party (commonly referred to as a Trusted Third Party, see further Annex 3).

Evidential value - PenOp's forensic characteristics

Disputes are inevitable in any environment. If such an event were to arise, it may be necessary to provide evidence before a court that the PenOp signature:

- was associated with a particular document, and
- the signature relates to a particular person;

In either case, it will be necessary to submit both archive records relating to the specific signature event²⁴; as well as an array of technical information relating to the operation of the PenOp system, as implemented within the client application.

Under English law there are no general regulations governing the type of medium to be used for archival recording. However, where regulations *explicitly* permit electronic record-keeping, such as electronic invoices, conditions are sometimes stipulated and the relevant public authority may have the right to be notified prior to organisation relying solely on such records²⁵. Regulatory authorities may also have statutory powers to investigate and audit an organisation's records maintained on a computer DIP system²⁶.

Evidential issues can be distinguished into two procedures:

- can computer-derived evidence be submitted into court for consideration (the issue of 'admissibility', and
- what weight will be given by the courts to such evidence (usually referred to as 'probative value').

Admissibility

In civil proceedings, under the Civil Evidence Act 1995, there are no special conditions governing the use of computer-derived evidence in court. However, in criminal proceedings, Section 69 of the Police and Criminal Evidence Act 1984 states that any statement produced by a computer will only be admitted into court subject to compliance with certain conditions. One of these conditions provides that "at all material times the computer was operating properly".

To satisfy a court that the conditions have been met, it is necessary to obtain either oral testimony or a signed statement from a person who occupies "a responsible position" in relation to the operation of the system, eg. PenOp as implemented within a client application. This is an affirmative duty which can be met by a person who is "familiar with the operation of the computer"²⁷. It would therefore be good practice for organisation's to designate such a person when the system is implemented.

²⁴ The signatory may be given the opportunity to retain a copy of the document signed, either in electronic or hard copy form.

²⁵ eg. Customs & Excise, under the Value Added Tax Act 1983: Schedule 7 expressly authorises the electronic recording of information for VAT purposes, provided that: (a) the inspector is informed in writing at least 1 month before; and (b) any conditions laid down by the inspector are followed (Schedule 7, s.3(2)).

²⁶ eg. Finance Act 1985.

²⁷ *R v Shepherd* [1993] 1 All ER 225.

Probative value

In terms of establishing a strong evidential link between a PenOp signature and the document to which it applies, an explanation of the Biometric Token mechanism would need to be provided (see Section 4 above).

In order to discharge any burden of proof with respect to the link between a person and his signature, a detailed examination and comparison would need to be carried out between the forensic characteristics recorded by the PenOp Signature Capture Service, during the act of signing, and any other signature examples, whether enrolled under the PenOp system or paper-based. Document examiners would be used to analyse the signatures and provide an expert opinion about the authenticity of any disputed signature.

PenOp records some ninety different statistical measurements arising from the act-of-signing, such as the speed of each stylus stroke and the relative positions of each mark. Such forensic data should provide sufficient information to enable a reliable comparative analysis to be carried out.

Concluding remarks

This report has focused on the extent to which the PenOp electronic signature product may be considered to be legally valid. Such validity has been assessed both in terms of complying with regulatory requirements for a 'signature' and as an evidential item.

In terms of 'signature' requirements, PenOp is able to show, with a high level of security, the key features of a legally valid signature: assent, identity and integrity. In addition, the manner in which PenOp records a hand-written signature will possibly facilitate its acceptance under English law compared with other techniques which depend on the substitution of the hand-written signature by data items.

In the absence of clear statutory or regulatory guidance on the issue, it is impossible to guarantee that a court will accept the validity of an electronic signature in every situation in which it may be used. However, the paucity of recent case law on the issue suggests that it is perhaps rare that the validity of a signature constitutes the basis for a dispute. Steps can also be taken to mitigate any risk, such as the incorporation of an express contractual term accepting the validity of electronic signatures. Any organisation incorporating PenOp into an application will need to review the relevant regulatory framework and make an independent assessment of the legal risks involved.

The implementation of PenOp within a particular environment will obviously vary according to each application. However, a PenOp electronic signature contains a range of components which can provide substantial forensic data evidencing the existence of a link between the person and his signature and between his signature and the document. If appropriately recorded and retained, such data should convey sufficient weight to meet any burden of proof required of it.

Within the next two years, it is anticipated, at both a national and European level, that legislation should be forthcoming explicitly addressing the legal validity of electronic signatures, in the context of promoting the development of electronic commerce and the 'Information Society'.