

The Legal Efficacy of the PenOp® Product under Singapore Law

Daniel Seng*

Rajah & Tann

DISCLAIMER: This is a general dissertation concerning the general legal efficacy of the PenOp Product under Singapore law, without reference to its use with or implementation in any other particular document, system, service or product. Nothing in this dissertation should be considered to be a product endorsement or a legal opinion. Please note that the technical details concerning the PenOp Product is taken from the write-ups supplied and this writer has assumed that these details are correct and accurate in drawing the requisite inferences. The reader is encouraged to seek his own professional advice, including legal and technical advice, and should not rely on this dissertation in relation to any specific circumstance or implementation of the PenOp Product.

TABLE OF CONTENTS

1	Summary of the Technology behind the PenOp Signature.....	2
2	Signatures for use in the Electronic Environment	5
3	Legal Validity of the PenOp® Signature as a Signature.....	5
3.1	Validity of Electronic Signatures	5
3.2	“Symbols in Digital Form”	6
3.3	“Authenticating or Approving”	6
3.4	“Logically Associated”.....	7
3.5	PenOp Signature as an Electronic Signature	8
3.6	Additional Characteristics of PenOp Signatures.....	8
3.7	PenOp Signature as a Secure Electronic Signature	9
4	Legal Validity of Documents signed with a PenOp® Signature	10
5	Conclusion	11

* Daniel Seng is a partner in the Singapore firm of advocates and solicitors Rajah & Tann and Head of the Technology Practice Group of the firm. He is also concurrently Adjunct Fellow with the Faculty of Law, National University of Singapore where he teaches Information Technology Law and Telecommunications Law.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 2 -

1 Summary of the Technology behind the PenOp Signature

- 1.1 The PenOp Signature system utilizes both digital technology as well as biometrics technology to digitally record a user's signature which is then applied to the electronic document on which the user signs. The entire process is electronic – no paper is involved.¹
- 1.2 There are two components in the PenOp Signature system. The first component, the Signature Capture Service (“SCS”), is responsible for digitally recording the user's signature. To do so, in conjunction with the application software into which the SCS is integrated, the SCS will generate a prompt (known as the Gravity Prompt) on the digitizer or the computer screen to indicate the purpose for which the signature is required. (The SCS will also present the user with an “Approve” button for approving the signature. More will be said about that later.) The Gravity Prompt will prompt the user to execute his signature. The user “signs” on a small, pressure-sensitive pad called a digitizer,² or on a special stylus upon a window on a specially equipped computer screen,³ as if he would sign on paper. As an image appears that traces the movement of the digitizer's stylus, the SCS will capture the graphic image⁴ of the signature electronically.⁵
- 1.3 In addition, the SCS also picks up 90 different pieces of data about each person's signature, including measurements such as:
 - the angle of the pen to the writing surface,
 - the acceleration and deceleration during strokes,
 - the horizontal and vertical velocity of writing,
 - the number of times the pen is picked up and put down,
 - the actual placement of lifting and lowering of the pen,
 - the order in which the strokes are made,
 - the time taken to complete the signature,
 - the visible curvature of the strokes, and
 - the relative pressure applied throughout signing.⁶

¹ See comment by Michael Betts, Senior Vice President for Information Technology, American General Life & Accident Insurance Co, as reported in the Wall Street Journal, “When the Pen May Be Mightier Than the Keyboard”, 6 August 1998 Reprint, column 3.

² *Ibid*, column 1.

³ Paper by Benjamin Wright, “The Legality of the PenOp Signature”, page 5, para 3 and page 7, para 3.

⁴ *Supra* 3, page 5, para 7.

⁵ *Supra* 1, page 1, column 3.

⁶ *Supra* 1, see insert to the photograph.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 3 -

- 1.4 These are known as the biometric data or “act-of-signing statistics”⁷ of that signature.
- 1.5 Such statistics are just as useful, if not more so, than the graphic image of the signature. An enrollment session can be conducted whereby through the use of the SCS, different people can execute their properly authenticated and authorized signatures. Each signatory’s signature is then captured in a file known as an electronic signature card⁸ which will also store the biometric data for that signature.⁹ All these files can be collated and securely held in a database (a “Signatory Database”). Subsequently, a putative signature of any person in the database can be verified by comparing the biometric data for the second signature with the stored biometric data in the database. This is where the second component of the PenOp System or the Signature Verification Service (“SVS”) component comes in. Using a scientific comparison of these statistics, the SVS will be able to assess the authenticity of the second signature through a “signature match percentage” *eg* 50 percent or 72 percent.¹⁰ This percentage can be reported to a client application which can then be configured to accept or reject the signature based on a pre-designated signature matching threshold *eg* 75 percent.¹¹
- 1.6 Only the real signatory of his signature will be able to produce a second signature whose biometric data will match the captured statistics in the Signatory Database, or pass the designated signature matching threshold.¹² This is because signatures captured using the PenOp system rely on the same scientific theory as handwritten signatures on paper:¹³ that it is possible to form an opinion as to the identity or genuineness of signatures through scientific analyses of handwriting.¹⁴ Although the scientific theories behind PenOp signatures have yet to be tested in court, because PenOp signatures are signatures executed, stored and measured in a controlled and systematic way, a learned jurist, Wright, has opined that this new type of signature analysis may prove in the long term to be more reliable than traditional handwriting/questioned document analysis.¹⁵
- 1.7 This signature and the biometric data that are captured electronically are in turn mathematically “linked” to the electronic document for which the signature is applied. When the user, after signing his signature, taps the “Approve” button, to signify his approval of the inscription event, a first checksum¹⁶ is computed of the signed electronic

⁷ *Supra* 3, page 5, para 4.

⁸ *Supra* 21, page 1, column 2.

⁹ Wright, *supra* 3, page 6, para 2.

¹⁰ *Ibid*, page 6, para 2.

¹¹ *Ibid*, page 7, para 5.

¹² Though note that so much biometric information is picked up that each inscription of an individual’s signature is different from every other inscription of a signature by that same individual. See Wright, *supra* 3, page 31, para 1.

¹³ Wright, *supra* 3, page 21, para 3.

¹⁴ In Singapore, it is accepted law that expert opinion as to the identity or genuineness of handwriting can be taken when the court has to form an opinion as to the identity or genuineness of handwriting. See S 47(1) and illustration (c), Evidence Act (Cap 97). *Cf s* 75, Evidence Act (Cap 97).

¹⁵ Wright, *supra* 3, page 22, para 2.

¹⁶ See the explanation in the main text on “checksums” and “hash functions” referred to at *infra* 28.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 4 -

document, and of the following set of data (termed the “Inscription Information”), comprising:

- this checksum,
- the signature biometrics,
- the date and time of signing,
- the identity of the machine on which the signing occurred,
- the claimed ID of the user,
- the signature prompt/Gravity Prompt, and
- the graphical image of the user’s signature.

1.8 A second checksum is computed of this set of data, which is then encrypted¹⁷ together with this second checksum.¹⁸ This encrypted string of data, known as a Biometric Token™, represents the inscription event.¹⁹ A proper electronic record archiving system that securely stores both the electronic record and the Biometric Token™²⁰ can be used by the PenOp Signature system to create an audit trail of:

- who (through the use of the PenOp SVS component)
- signed what (calculating the checksum for the archived electronic document and matching it against the first checksum)
- when (the date/time information captured in the encrypted Biometric Token™), and
- why (the Gravity Prompt, which will contain the information presented in the prompt).²¹

1.9 All in all, the Biometric Token™, which is for all intents and purposes *the* PenOp Signature, is the amalgamation of several types of data:

- the graphic image of the inscribed signature of the signatory
- the biometric information or act-of-signing statistics of the signature
- the Inscription Information, and
- the link between the digitized signature and the electronic document for which the signature was executed.

¹⁷ The details of the encryption methodology are not disclosed. The security of the encryption methodology will have an important bearing on the security of the Biometric Token™.

¹⁸ Wright, *supra* 3, page 5, paras 5 to 7.

¹⁹ Wright, *supra* 3, page 5, para 8.

²⁰ Wright, *supra* 3, page 26, paras 6 to 7.

²¹ PenOp Brochure entitled “Signature Series”, page 1, column 2.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 5 -

2 Signatures for use in the Electronic Environment

- 2.1 Although electronic documents have been around for some time, the law has only just started to come to terms with and to accept electronic documents. The lack of legal rules in this area is largely because it is only recently that technology has been properly applied to solve the problem of document security and signed electronic documents.²² Technological progress in this area has been driven by the recent prevalence of electronic transactions. In the faceless, borderless world of the Internet, a merchant cannot be sure, and cannot prove, that he is transacting with a person who claims to be who he is. Details, particulars and addresses can be fabricated, and other information such as credit card numbers can be stolen from credit card holders, or intercepted from insecure e-commerce servers or e-commerce communications, or even generated *ad hoc* from easily available computer programs found on the Internet. This makes it possible for the alleged purchasers of e-commerce commodities to dispute the transactions. For this reason, the technological spotlight has recently been cast on electronic signatures.
- 2.2 In the traditional paper-based environment of commerce, transactions are usually completed in one of two ways: the merchant either parts with his goods for cash on delivery, or the merchant procures the signature of his customer to some document, be it the invoice or the delivery order, whether in advance of the order or upon delivery. There is no reason why the same safeguards afforded by signatures cannot be applied to the electronic environment. Hence the advent of “electronic signatures”. If a merchant can procure the electronic signature of his customer to an electronic order for goods, where a dispute arises, the merchant will have a higher level of assurance that he will be able to prove in court that this was the order of his customer. Conversely, it will be more difficult for the customer to dispute the transaction, because he will be confronted with his own electronic signature. Supposing the merchant implements the PenOp system for capturing his customer’s signature. Is the PenOp signature accorded legal recognition in Singapore?

3 Legal Validity of the PenOp® Signature as a Signature

3.1 Validity of Electronic Signatures

- 3.1.1 Although PenOp signatures are generally described in the technical sense as electronic signatures, and even seen as alternatives to digital signatures,²³ this technical description is no assurance that PenOp signatures are legally recognized as signatures in law. Whether PenOp signatures are signatures in law calls for a close analysis of the rules of law relating to electronic evidence and documentary signatures.
- 3.1.2 Prior to the coming into force of the Electronic Transactions Act (No 25 of 1998) (“SETA”) on 10 July 1998,²⁴ there were certain uncertainties in Singapore law in relation

²² Daniel Seng, “Computer Output as Evidence”, [1997] Singapore Journal of Legal Studies 130, 184.

²³ *Supra* 1, page 2, entitled “Are Digital Signatures the Answer?”, column 1. But it is generally accepted that the term “digital signatures” refers to signature systems that make use of a type of cryptography known as asymmetric cryptosystems. In contrast, PenOp signatures rely on the science of signature dynamics. See also the discussion in the main text at *supra* 12.

²⁴ The SETA is available on the Internet at www.cca.gov.sg.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 6 -

to electronic signatures and electronic documents signed with electronic signatures. But with the passage of SETA, many uncertainties arising out of the use of electronic signatures and electronic documents have been addressed.

3.1.3 The starting point is the definition for “electronic signatures”. Section 2 of SETA reads:

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;

3.1.4 Section 8(1) of SETA provides that where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law. SETA also makes it clear that the courts are not foreclosed from relying on only the traditional methods to prove electronic signatures. The courts may rely on any manner of proof, including proof of execution of a symbol or proof of a security procedure for purposes of verifying that the electronic document that is signed is that of the signatory.²⁵

3.1.5 So is the PenOp Signature an “electronic signature” under SETA? Answering this question calls for a close analysis of the definition of an “electronic signature” under SETA.

3.2 “Symbols in Digital Form”

3.2.1 I have concluded that the PenOp signature in the form of the Biometric Token™ is an “electronic signature”. First, the digitized graphic image of the signature, together with the other encrypted information, will be such “*symbols in digital form*” that are, at the very least, logically associated with the electronic document (the electronic record²⁶).

3.3 “Authenticating or Approving”

3.3.1 Secondly, through the use of the Gravity prompt, as well as the “Approve” button, the signatory executes the PenOp signature. The SCS component thereby requires the signatory to undertake a conscious decision to execute his PenOp signature upon the relevant electronic document. In such circumstances, it will be difficult to contend that he did not intend to be bound by his inscription on the document. This meets the requirement in the definition that such a signature must be applied to the electronic document “*with the intention of authenticating or approving the electronic record.*”

3.3.2 It is useful to examine these two aspects of the SCS component again in more detail. The Gravity Prompt informs the signatory as to the nature of the document for which he is signing. So the signatory has to consciously apply his mind to the act of inscribing his signature on the digitizer or the screen. Since the Gravity Prompt will confront the signatory before he inscribes his signature, a properly designed and reasonably informative Gravity Prompt will make it difficult for any signatory to contend that he did not know what he was signing.

²⁵ S 8(2), SETA.

²⁶ An “electronic record” is defined as “a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another.” See s 2, SETA.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 7 -

3.3.3 Furthermore, the signatory, after signing the document, is given a last opportunity to “Approve” or “Reject” the signature *before*²⁷ it is applied to the electronic document. He has to “Approve” the signature before it is electronically and “logically associated” with that electronic document. The signatory is actually given the opportunity to reject his signature.

3.3.4 It is the combination of both the Gravity prompt and the “Approve” button that makes it difficult, if not impossible, for the signatory to subsequently repudiate the transaction by claiming that he never applied his mind to either the signature or the document for which he is signing.

3.4 “Logically Associated”

3.4.1 Thirdly, the PenOp signature is “logically associated with the electronic document for which it was signed.” It is this link between the signature and the document that makes the PenOp signature a legally effective “electronic signature”. This linkage is achieved by way of two mechanisms:

- The first is the computation of a checksum of the electronic document which is sought to be “signed” (the “first checksum”). The checksum as described by PenOp is a “hash function”,²⁸ which produces a unique mathematical result (the “hash result”) from the same electronic record. This result and the function that produced it have two very important security characteristics:
 - (a) Any slightest change to the electronic record will produce a different checksum or “hash result”.²⁹
 - (b) Similarly, it is computationally infeasible³⁰ that two electronic records can be found that produce the same hash result using the same function.³¹
- The second is the computation of another checksum for all the biometric data for the signature and the first checksum. The biometric data and the first checksums are then encrypted, together with this second checksum, to form the Biometric Token™.³² Because the Biometric Token™ is both encrypted and protected by checksums, a proper implementation of this system means that any slightest change to the biometric data can be detected.

3.4.2 If the properly implemented PenOp system³³ has these characteristics, this gives the party relying on PenOp signatures the assurance that the electronic document that is signed is the same document to which the PenOp signature is applied. This assurance arises because it becomes computationally infeasible to alter or modify the PenOp-signed

²⁷ Wright, *supra* 3, page 7, para 3.

²⁸ There is no description of the actual checksum formula that is used, although as is set out by Wright, *supra* 3, page 40, endnote 1, the checksum has a probability of error of about 1 in 2^{80} or 10^{24} .

²⁹ Wright, *supra* 3, page 5, para 5.

³⁰ This translates into the probability of error, as set out in *supra* 28.

³¹ See the definition of “hash result” in s 2, SETA.

³² Wright, *supra* 3, page 5, para 8.

³³ Wright, *supra* 3, pages 26-27.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 8 -

document, or to attribute another document to the PenOp Signature, and yet ensure that the same checksum (as stored in the Biometric Token™) will be produced for the modified document.³⁴ This provides a high level of assurance that the PenOp Signature is “logically associated” with the electronic document for which it was signed.

3.5 PenOp Signature as an Electronic Signature

3.5.1 If the PenOp Signature exhibits all these characteristics, on this analysis, the PenOp signature is an “electronic signature”. The result is that under SETA, the PenOp Signature is a valid legal substitute for traditional, handwritten signatures.

3.5.2 It should however be cautioned here that SETA is not applicable to certain classes of documents or instruments. While the general purpose of SETA is to ensure that there is no discrimination against electronic signatures, a line is drawn between documents of title and most other documents. So by s 4 of SETA, the following matters cannot be signed or executed by way of an electronic signature:

- (a) the creation or execution of a will;
- (b) negotiable instruments;
- (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;
- (d) any contract for the sale or other disposition of immovable property, or any interest in such property;
- (e) the conveyance of immovable property or the transfer of any interest in immovable property; and
- (f) documents of title.

3.5.3 Most contracts *eg* e-commerce contracts for the provision of goods and services will fall outside of these exclusions, unless these transactions themselves deal with these excluded categories of matters. It should also be noted that provision is also made for the Minister to add or detract from this enumerated list of matters which cannot be signed electronically.³⁵ It is expected that as electronic signature technologies mature, with wider commercial acceptance of the technology will come the narrowing of this list of exclusions.³⁶

3.6 Additional Characteristics of PenOp Signatures

3.6.1 From the discussion above, it will be apparent that a properly implemented PenOp signature system also gives the assurance that the PenOp signature is itself not tampered with. This is because by virtue of, *inter alia*, the use of checksums, it becomes computationally infeasible to modify the PenOp signature itself, or to attribute another signature to the first document signed with the original PenOp signature.

³⁴ Of course, this is subject to a proper implementation of the PenOp system, as well as proper security of both the signed document as well as the Biometric Token™.

³⁵ S 4(2), SETA.

³⁶ Daniel Seng, *Legal Guide to the Electronic Transactions Act*, commentary on s 4(2), page 9.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 9 -

- 3.6.2 Thus, a properly implemented PenOp signature demonstrates two characteristics:
- (a) that it is possible to accurately determine whether the PenOp signature was signed by the alleged signatory, and
 - (b) that it is possible to accurately determine whether the initial electronic record that is signed using the PenOp signature has been altered since the PenOp signature was inscribed.³⁷
- 3.6.3 Most electronic signatures will not have these security features. Interestingly, these are the two very characteristics of digital signatures (as they are defined in SETA) as well.³⁸ This means that PenOp signatures, unlike most generic electronic signatures, compare very favourably with digital signatures.

3.7 PenOp Signature as a Secure Electronic Signature

- 3.7.1 With these two security features, under certain circumstances, a secure, properly implemented PenOp Signature becomes a “secure electronic signature” under SETA. A secure electronic signature is one which it can be verified that the signature, at the time it was made, was
- (a) unique to the person using it;
 - (b) capable of identifying such person;
 - (c) created in a manner or using a means under the sole control of the person using it; and
 - (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.³⁹
- 3.7.2 The PenOp signature will be unique to the person using it, since, as is explained above, by virtue of signature dynamics, it is infeasible to duplicate a signatory’s signature as well as the biometric data of the signature.⁴⁰ As such, by the application of the SVS component, it is possible to identify the person to whom the PenOp signature belongs.⁴¹ Subject to proper security safeguards being put in place to ensure that the signatory database is not accessed in an unauthorised way, if a matching PenOp signature is executed, the same biometric uniqueness of a person’s signature goes a considerable

³⁷ Note that as Wright points out, this is conditional upon properly and securely archiving the initial electronic document which has been signed. Without this initial electronic document, it is not possible to compute its checksum and compare it against the checksum stored in the Biometric Token™. See *supra* 3, page 26, para 6.

³⁸ A “digital signature” is defined in s 2, SETA to mean “an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer’s public key can accurately determine — (a) whether the transformation was created using the private key that corresponds to the signer’s public key; and (b) whether the initial electronic record has been altered since the transformation was made;”

³⁹ S 17, SETA.

⁴⁰ See the main text at *supra* 12.

⁴¹ See the main text at *supra* 10.

The Legal Efficacy of the PenOp® Product under Singapore Law

- 10 -

distance towards proving that the PenOp signature was created by the person using it.⁴² Finally, as is explained above,⁴³ the PenOp signature is linked to the electronic document for which it was signed so that any changes to the document will invalidate the PenOp signature checksums.

- 3.7.3 If this verification process is achieved by way of a prescribed security procedure, or a commercially reasonable procedure agreed to by the parties involved, the PenOp signature becomes a secure electronic signature. The advantage is that under SETA, no presumptions are made as to the authenticity and integrity of electronic signatures.⁴⁴ So it is open to the signatory to dispute that his signature has been forged or tampered with, if he signs it with a “mere” electronic signature. However, with secure electronic signatures, unless evidence to the contrary is adduced, a secure electronic signature will be presumed to be the signature of the person to whom it correlates, and affixed by the person with the requisite intention of signing the electronic document.⁴⁵ So the tables are turned, and it is up to the signatory to show that the signature is not his. This, of course, will not be an easy prospect for the signatory, unless his case is genuine.

4 Legal Validity of Documents signed with a PenOp® Signature

- 4.1 If the PenOp signature is a secure electronic signature, another advantage accrues. The use of the PenOp signature may amount to a prescribed security procedure or a commercially reasonable security procedure⁴⁶ agreed to by the parties involved which has been properly applied to an electronic document to verify that the electronic document has not been altered since a specific point in time. (It should be borne in mind that the Biometric Token™ contains a record of the date/time on which the PenOp signature was inscribed.) If so, by the application of s 16(1) of SETA, the electronic document signed with a PenOp signature shall be treated as a “secure electronic record” from the time of the signature’s inscription.
- 4.2 The legal consequence is that a secure electronic record shall be presumed not to have been altered since the point in time to which its secure status relates.⁴⁷ This is a very important presumption. With this presumption, parties can, with confidence, handle, manage and act on an electronic document signed with a PenOp signature and which is so properly verified as being authentic. Parties will not have doubts as to the authorship of the electronic document, the date and time of the document, and the integrity of the document.⁴⁸ The admission and proof of a PenOp signed document in evidence will be greatly facilitated.⁴⁹

⁴² See, again, the main text at *supra* 12.

⁴³ See the main text under the heading “logically associated”, starting at *supra* 28.

⁴⁴ S 18(3), SETA.

⁴⁵ S 18(2), SETA.

⁴⁶ The test for a “commercially reasonable security procedure” is set out in s 16(2), SETA.

⁴⁷ S 18(1), SETA.

⁴⁸ See Daniel Seng, “Computer Output as Evidence”, *supra* 22, pages 162-163.

⁴⁹ Ss 35, 36, Evidence Act (Cap 93).

The Legal Efficacy of the PenOp® Product under Singapore Law

- 11 -

5 Conclusion

- 5.1 In conclusion, even though the legal validity of the PenOp system awaits testing in Singapore courts, a PenOp signature is most certainly an electronic signature, which generally has the same legal recognition as a signature in non-electronic form. In addition, a properly implemented PenOp signature system and proper and secure archives of the electronic documents to which it is applied, coupled with adequate security for the SVS signature database, makes the PenOp signature a secure electronic signature, and makes the documents to which it is applied secure electronic documents. This gives such signatures and documents the added presumption that they are authentic and accurate, and that their integrity and authenticity will not be easily disputed. With this technical and legal security afforded by the PenOp system, parties will be able to more confidently commit themselves to their obligations and undertakings in the electronic environment.

Daniel Seng
Partner & Head, Technology Practice Group
Rajah & Tann
16 December 1999