PAOGA®
Privacy & Trust in the Digital Age

Rite-Choice

White Paper

Legal Certainty & Evidential Weight

Author: **Peter Howes**
Date: August 2011

Contents

Disclaimer

The following information provided is without engagement and is intended solely to provide a general overview of the issues surrounding legal certainty and evidential weight without any pretension to completeness or accuracy of detail.

This Statement is not designed to clarify the details of individual legal regulations or all aspects of the subject addressed and does not replace legal advice in individual cases. Before making any business decisions you should consult your legal advisor. The legal regulations may have changed since this text was published.

About the author

- Peter Howes is a BSI Management Committee member who has contributed to the BSI Codes of Practice for Evidential Weight and Legal Admissibility of Electronic Information since 1994; this has been adopted as the Standard BS10008:2008. He is also Joint Author of the associated Compliance Workbooks.
- As an accredited trainer for the ISEB Foundation in IT Law qualification has a proven in-depth knowledge of the English legal framework, both Civil and Criminal.
- Since 1996, Peter has worked with the British Standards Institution to develop and deliver a wide range of workshops on Email Records Management, Email and the Law, Information Security and the Law, Legal Admissibility and associated topics.
- Peter, Director – Rite-Choice Ltd, has advised major organisations on the application of the BSI Codes to information both “born digital” and converted to digital form from paper, microfiche and film. These organisations include HBOS (Halifax Bank of Scotland), Companies House, Ernst and Young, Brown & Root, Canon, Deutsche Bank, ABN AMRO, Iron Mountain and the Metropolitan Police Service.

LinkedIn profile

1. Executive Summary

PAOGA can justifiably claim that it will be able to provide a legally compliant and effective replacement of signed documents, such as contracts.

This paper explains the important terms “Legal Certainty” and “Evidential Weight” in the context of PAOGA and how PAOGA will be able to deliver legal certainty and meet the evidential requirements to resist challenges for documents in electronic form in the event of those documents being used in the resolution of disputes.

It must be accepted that PAOGA is still in the course of development and that is why the future tense is used in the preceding two paragraphs.

For the expectation of legal certainty and evidential weight to be realised there are a number of items that will be completed by PAOGA during the final development phase. These items are required for PAOGA to comply with the accepted best practice for evidential weight. The most important issues to be addressed are: -

- a record of PAOGA compliance commitments (evidential weight best practice and other industry certifications to be sought),
- formal documentation (policy, design, processes and procedures),
- user documentation (to include user expectations and responsibilities as well as PAOGA service commitments), and,
- definition, design and implementation of specific aspects of PAOGA (audit trail and user roles/responsibilities).

PAOGA are committed to addressing these issues prior to general release.

2. Purpose of this Report

This report is intended to assist understanding of how PAOGA will be able to substantiate claims that it can provide the legally compliant and fully effective replacement of signed documents, such as contracts, in electronic form providing certainty and meeting evidential requirements in the event of those electronic documents being used in the resolution of disputes[1].

This is dependent on two legal aspects: -

- Legal Certainty, and,
- Strong, unimpeachable Evidential Weight

To achieve the evidential and certainty goals PAOGA will enable its users (individuals and entities) to create networks of trust relationships using cryptographic techniques. Unlike other existing trust services in the marketplace, PAOGA does not rely on a trusted Certificate Authority (CA) hierarchy. Comparison of these different trust models is outside the scope of this document.

[1] Most information used in dispute resolution is accepted without challenge with regard to authenticity or integrity. However, it is becoming increasingly common for the credibility of records to be questioned. As a consequence, and also because of the not unnatural public cynicism regarding the security of today’s technology based services in the light of incessant news coverage of compromises, it is imperative that PAOGA protects information against compromise and is able to resist challenges as to the authenticity and integrity of that information.

3. Objectives of PAOGA

PAOGA has identified the advantages of a trust model for certainty and confidentiality that is controlled by the individual and customised to suit each relationship they have rather than being a choice from a potentially unsuitable, limited, pre-defined, rigid set as with existing trust services.

Specifically, PAOGA is targeting the areas of personal and business information storage and exchange with certainty and confidentiality based upon use of electronic signatures and encryption and is developing a suite of applications in this space built on an individually controlled trust model rather than reliance on the pre-set, constrained approach[2] of existing trusted service providers.

In common with existing trusted services; PAOGA uses existing, proven, widely adopted, open standards throughout, rather than inventing new cryptographic technologies. This use of standards by PAOGA covers digital certificates, encryption algorithms, digital signatures, time-stamps.

However, because PAOGA does not rely on the same trusted Certificate Authority (CA) hierarchy as with alternative trust services it is not vulnerable, as they are, to compromise of a CA or the CA hierarchy.

4. Legal Requirements and How PAOGA Meets Them

a. Legal Certainty

A major strength and weakness of the English legal system is its reliance, where no precedent exists, on interpretation by the presiding official, usually a Judge or Magistrate. A consequence of such interpretation is that the conclusions in a particular case can appear to contradict either common sense or previous experience.

Interpretation also affects perceptions when considering a term such as “legal certainty”.

“Legal certainty” is a well established concept that can be defined in civil law as the predictability as to how the officials will react in a particular circumstance; for common law it can be regarded as facilitating the ability of the citizen to organise their affairs in a manner that does not break the law.

Whilst the English legal system is based on common law, the civil law approach to “legal certainty” is of particular relevance when considering the significance of using a particular technology, such as that employed by PAOGA, to deliver against a claim to provide “legal certainty”. The law[3] is quite clear that electronic signatures associated with electronic

[2] Trust Service Providers are constrained by their design and as a consequence create a small set of functional products that meet their service level agreements and risk models (normally detailed in their Certificate Policy and Certification Practice Statement – see IETF RFC 3647).

[3] Electronic Communications Act 2000 – Part II Section 7
Electronic signatures and related certificates.

(1)In any legal proceedings—

(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and

(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.

documents based on the use of cryptographic techniques, such as those utilised by PAOGA, are legally admissible and have the same validity as a “wet signature on paper”.

Without this clarity, eCommerce would not have developed as far as it has. But, as has been well demonstrated, the current state of the market leaves unanswered questions regarding the authenticity of an electronic signature. It is this uncertainty that has led to a somewhat piecemeal approach in adjudication that means that the behaviour of officials cannot always be reliably predicted creating some doubt as to “legal certainty” even though the law is clear and unambiguous.

Before delving somewhat deeper into this area it is worth considering whether, or not, a wet signature on paper has “legal certainty”.

Experience shows that handwriting a signature in ink on a piece of paper is a well tried approach that has been well tested in disputes over the centuries and that the officials in a case will treat it quite predictably – so does it pass the civil test of “legal certainty”? Maybe, but does this mean that the handwritten signature on a piece of paper is always accepted as absolute proof of a particular point or contract? Absolutely not!

The reality is that the signed paper document will be admitted and used as evidence and will then be given the evidential weight it warrants.

b. Evidential Weight

In any dispute, whether at Court, in a Tribunal or before the dispute goes to a formalized resolution it has to be remembered that the dispute is an adversarial process where weakest links are exploited.

If evidence or statements can be discredited then the representation of the party discredited will be undermined. When evidence is discredited its value will be diminished, sometimes totally. The key to preventing evidence being discredited is to prove its authenticity and integrity - this will maximise its evidential weight.

Evidential weight is “how trustworthy is this particular piece of evidence” and should not be confused with “how valuable is this piece of evidence”. Clearly the most valuable piece of evidence will be considered less compelling to the outcome of the dispute if its provenance can be discredited. All evidence can have its evidential weight diminished by challenge that is not robustly resisted. This is true of evidence given by an individual or contained in documents submitted as evidence.

Documents that are submitted as evidence are regarded as “hearsay” evidence as opposed to evidence given orally. If the authenticity or integrity of such hearsay evidence is challenged the originator of the document is unlikely to be present or able to resist the challenge unless there is other evidence that supports the authenticity or integrity of the document in question. Interestingly, the term “document” has a wide definition that includes electronically stored information.

The legal framework that is pertinent to any discussion of evidential weight is bounded by 2 pieces of primary legislation.

- Civil Evidence Act 1995[4] - where the standard of proof for the case is “Balance of Probability”, and
- Police and Criminal Evidence Act 1984[5] - where the standard of proof is “Beyond Reasonable Doubt”.

[4] Civil Evidence Act 1995

The Civil Evidence Act 1995 and associated Civil Procedure Rules make it clear that evidence should be weighted and that the authenticity and integrity of documents submitted as evidence is accepted unless formally challenged[6].

Until recently the situation with regard to criminal proceedings was less clear. However, the "Justice for All" White Paper 2002[7] (Section 4.52/4.53) led to a change to the basis upon which evidence is viewed in criminal proceedings away from an environment whereby much evidence was deemed inadmissible. It observed that the then current *"rules of evidence, which determine what evidence the court can take into account, are difficult to understand and complex to apply in practice. There has been growing public concern that evidence relevant to the search for truth is being wrongly excluded. Magistrates, judges and juries should be trusted to give appropriate evidence the weight it deserves when they exercise their judgment"*.

This is an important facet of the Criminal Justice Act (2003)[8]. The provisions of the Act, supported by the Criminal Procedure Rules[9], enable magistrates, judges and juries to hear all the relevant evidence and afford it the weight it deserves.

The Youth Justice and Criminal Evidence Act 1999[10] removed an admissibility restriction on use of evidence from computer records as detailed in Section 69 of the Police and Criminal Evidence Act 1984.

So, an electronic or paper document will be legally admissible. Does this mean that either the handwritten signature on a piece of paper or electronic signature on an electronic document is always accepted as absolute proof of a particular point or contract?

The reality is that the signed document will be admitted and used as evidence and will then be given the evidential weight it warrants.

That evidential weight will be diminished if a party in the dispute can demonstrate that the document may have been superseded by a newer version, may have been tampered with or cast doubt as to whether the signature is not the authentic signature of the individual in question. Paper documents can get changed[11], even after they have been signed and counterfeit signatures are not uncommon.

Therefore, whilst there may be "legal certainty" regarding the document, the way it is treated as evidence is dependent on its evidential weight. In that regard there is no difference between paper and an electronic document that has been electronically signed[12] using techniques such as those within PAOGA.

[5] Police and Criminal Evidence Act 1984

[6] Civil Procedure Rules – Part 32.19

[7] Justice for All White Paper originally published by the Home Office, available from CPS website.

[8] Criminal Justice Act 2003 Part 11 Chapter 2 Section 117

[9] Criminal Procedure Rules Part 34 – Hearsay Evidence

[10] Youth Justice and Criminal Evidence Act 1999 Chapter VI Section 60

[11] An example of this was a change to a handwritten police log of events during the shooting on Stockwell Underground Station on 22 July 2005 that came to light during the Inquest.

[12] The PAOGA electronic signature is an "advanced electronic signature" under the terms of the Electronic Signatures Regulations 2002 Section 2.

The law states that such an electronic document will be admissible and it is then up to the specifics of the technology based solution to ensure that the evidential weight is maximised and that the electronic document's integrity and authenticity is resistant to challenge.

The technological approach adopted by PAOGA would appear to meet these objectives and this would be best demonstrated by formal adoption of the recognised best practice[13]. Such a demonstrable compliance with best practice cannot be completed until the system is complete and fully documented; however, PAOGA are committed to achieve and then maintain compliance[14]. This will ensure that users of the system can be assured of the "legal certainty" of the system and will have the evidence to resist a challenge as to the authenticity and integrity of electronic documents stored and communicated using PAOGA[15].

It is important to realise that the electronic signatures applied with PAOGA demonstrate strongly that a document has not been changed; in this respect it can be argued that an electronically signed document is less susceptible to challenge than a paper document.

As a result, any challenge regarding an electronic document is likely to focus on whether the signature was applied by the individual or someone else[16]. If an individual's Private Key is accessible to others then this could be the basis of a successful challenge to authenticity. In this regard, PAOGA differs from many trust models in that the user's Private Key is never known by PAOGA and so cannot be compromised by PAOGA or PAOGA staff[17].

Clearly there is potentially an issue with systems, including PAOGA, if the Certificate Store on the user's system is compromised. PAOGA have addressed this by using a discrete Certificate Store[18] that can be held separately and is significantly more secure than the equivalent standard operating systems.

[13] Best practice for this maximisation of evidential weight is the British Standards Institution publication BS 10008:2008 Evidential weight and legal admissibility of electronic information. Specification and associated guidance codes and compliance workbook.

[14] This must be formally confirmed and recorded by PAOGA.

[15] It should be noted that the PAOGA components are a part of a wider system that includes the procedures that the user employs. If these procedures are imprecise, poorly defined or not followed then the evidential weight of the content could be reduced. An example of this is if, for instance, the user keeps their password on a piece of paper beside their PC then another person could sign documents that the proper person had no involvement in and the evidential trail that links identity to the document would be compromised.

[16] There are examples where this type of argument has been used in Court by an individual to deny they were responsible for a commitment apparently made in their name; there are also examples where such repudiation has been unsuccessful.

[17] Clearly, there is a risk if a user makes their Private Keys known or accessible to another, wittingly or unwittingly. Users must be made aware of their responsibilities to keep their private Keys confidential and the implications of them not doing so.

[18] The PAOGA Certificate Store can be held on, for example, a USB memory stick and additionally can be secured with password, PIN or one-time code sent via SMS. The user option of none of these additional security options is not recommended.