RPost's Registered E-mail® services and Evidence issues within the United Kingdom Legal System

By Alan Shipman, Author, British Standards Institute
'Legal admissibility' Code of Practice – BIP 0008

London, England ABSTRACT OF OPINION February 2008

ABSTRACT

RPost® service delivers a Registered E-mail® message to the recipient and returns verifiable evidence of the precise content (message body and all attachments) and official time the e-mail was sent and received by each recipient. The service accomplishes this without storing e-mail messages and without any extra recipient action or special settings or software on the recipient side.

This review of the admissibility and evidential weight of RPost's Registered E-mail® service in the United Kingdom presents the following conclusions:

(1) DELIVERY PROOF: RPost's Registered E-mail® service provides a record of sending and receiving in accordance with the European Electronic Commerce Directive (2000/31/EC) by recording the recipient's server's receipt thereof;

(2) CONTENT PROOF: The encryption and tamper-detectability of RPost's Registered E-mail® service preserves the contents of e-mails and their attachments so as to satisfy process requirements designed under the European Electronic Commerce Directive (2000/31/EC) and evidence law and to establish evidence of content;

(3) OFFICIAL TIME STAMP: RPost's link to a trusted and objective time source provides essential and credible evidence in disputes in which the time an e-mail was sent or received is material to the case;

(4) ADMISSIBLE EVIDENCE: RPost's Registered E-mail® service receipts are admissible as to their fact of delivery, as to their trusted time of delivery and as to the authenticity of their content;

(5) FUNCTIONAL EQUIVALENCE: RPost's Registered E-mail® service, under European Electronic Commerce Directive (2000/31/EC), can serve as the functional equivalent of paper mail, to be used in lieu of certified mail, registered mail, return receipt mail, private express mail services, fax logs and similar types of paper mail services;

(6) ELECTRONIC ORIGINAL: RPost's Authentication Receipt™ provides a methodology for demonstrating the trustworthiness of the electronic original, including the message content, attachments and transmission meta-data including the delivery audit trail;

(7) SELF-AUTHENTICATING EVIDENCE: The RPost system provides the ability to have e-mail evidence authenticated without relying on complexities of a system-wide authentication or chain of custody reviews within the sender's and/or recipient's IT infrastructure.

(8) THE UK LEGAL ADMISSIBILITY POSITION: Within the UK, the majority of instances where the contents of an e-mail will be used as evidence are those dealing with civil litigation. The appropriate legal system for civil litigation is defined by the Civil Evidence Act 1995, which states that any 'statement contained in a document' – and this will include statements in e-mails – is hereby shown to be admissible as evidence into a UK civil court. Therefore, one should focus on "authentication" of the e-mail that is to be used as evidence in civil litigation, in light of how a judge might need to accept such authentication. The party with the most evidential weight often has the upper hand and it is here that the strength of RPost's "legal" proof capability is likely to prevail.

(9) EVIDENTIAL WEIGHT: Once legal admissibility is determined (e.g. can statements within an e-mail be admitted into court as evidence), the evidential weight of the information contained within the document must then be scrutinized. The ability to be able to prove the integrity of content of an e-mail (including any attachments) and its time of delivery are becoming increasingly important. There are common misconceptions around standard e-mail systems which can easily be exploited by one party or another to deny or dispute the integrity of an e-mail.

(10) CODE OF PRACTICE COMPLIANCE PROVISION: The Code of Practice (BIP 0008-2:2005, 6.7) discusses the advantages of e-mail systems that include a proof-of-delivery option. The Code notes that "whilst the receipt of such a confirmation message may be trustworthy, the absence of such a receipt may not be reliable evidence as to either delivery or non-delivery. It is important to note that the RPost "proof of delivery" capability speaks directly to this provision.

(11) AUTHENTICATION: To further enhance the potential evidential weight of an e-mail, the RPost system provides a mechanism for demonstrating the authenticity of a stored e-mail. This authentication can take place any time after the Registered Receipt e-mail has been received by the sender – the original message can be re-authenticated at any time. Where doubt occurs with an authenticated e-mail, a re-authentication could be performed 'in front of the court' if necessary to provide the strongest test possible of the validity of the evidence contained within the e-mail under question.

(12) ISSUES RELATED TO PERSONAL DATA: Within the UK, the processing of personal data is governed by the Data Protection Act 1998. This Act states that personal data may not be processed outside the European Economic Area unless certain conditions apply. In the case of RPost, some e-mail traffic may be diverted to computer systems installed within the USA. Thus, in order to retain legal processing status under the Data Protection Act 1998, RPost has signed up to the EC 'Safe Harbor' process[1], which will allow the free flow of information containing personal data from the EEA through the RPost servers.

Alan Shipman
Managing Director, Group 5 Training Limited
Author, British Standards Institute 'Legal admissibility' Code of Practice – BIP 0008
February 2008

For more information on RPost services, visit www.rpost.com

[1] http://www.export.gov/safeharbor/SH_Overview.asp