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 **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.

INTRODUCTION

Registered E-mail® is a service provided by RPost International Limited. The company markets the RPost service as one that "provides legal and verifiable evidence of the content and time any e-mail (and any attachments) has been sent and received by anyone, anywhere in the world".

Because legal systems vary throughout the world, RPost's claim of "legal" proof must be judged against prevailing legal systems. Such is the case for any UK implementation of RPost services given that the company's instructional materials are geared primarily for a US market with its "legal" claims focused primarily upon the US court system and enabling statutes.

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. The appropriate sections (8 and 9) of the Act related to the admissibility of documentary evidence are as follows:

8. (1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved:

(a) by the production of that document, or

(b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.

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.

(2) It is immaterial for this purpose how many removes there are between a copy and the original.

9. (1) A document that is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.

(2) A document should be taken to form part of the records of a business or public authority if there is produced to a court a certificate to that effect signed by an officer of the business or authority to which the records belong. (reference - Civil Evidence Act 1995)

Therefore, 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. There are no specific requirements included in the Civil Evidence Act that need to be met to address issues of legal admissibility. In practice, the only challenge to legal admissibility will come from the judge during the hearing of a particular case.

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.

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. Such scrutiny will relate to the authenticity, integrity and availability of information processed in an electronic format. It is thus critical that the court be satisfied that such electronic information is both reliable and accurate.

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. Some common misconceptions follow:

1. **READ RECEIPT:**

   Many MS Outlook users believe they already have delivery proof capability within e-mail system. The tracking options require the recipient of an e-mail to confirm receipt. Typically, such requests are ignored. Further, it is relatively easy to forge a read receipt. Where a receipt is received, it does not include any confirmation of the content of the e-mail.

2. **SENT FOLDER / ARCHIVE:**

   Many users believe that their "sent items" folder or "archive" provide a record of their correspondence. Whilst it can provide a record of what they claim to have sent, it does not protect them from a recipient claiming they did not get the e-mail, nor that the e-mail contained different information or attachments when they received it.

3. **PRINTED E-MAIL RECORDS:**

   Many organisations believe that a printed e-mail (from the inbox, sent folder, or other folder) is an effective way to authenticate the contents of an e-mail. However, if the contents of an e-mail are questioned, the e-mail may be withheld from evidence unless the holder of the printed e-mail can authenticate that correspondence via another means.

4. **BOUNCE NOTICE:**

   Many users believe that if they do not receive a "bounce" notice, then that e-mail was delivered to the recipient. As many e-mail systems turn off these "bounce" notices due to spam and blacklisting concerns, such a belief may be ill-founded.

Within the UK, the British Standards Institution (BSI) 'Legal Admissibility' Code of Practice (BIP 0008) is where one turns for assistance in demonstrating the authenticity of information in an electronic form. For e-mail applications, the most appropriate section of the Code is BIP 0008-2:2005, Chapter 6.

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. Every Registered E-mail message generates an automatically returned Registered Receipt™ e-mail that contains the contents of the original e-mail and any attachments, held in an encrypted form incorporated into the receipt (note, RPost does not store a copy of the e-mail or receipt, or encrypted data associated with the e-mail or receipt). The encryption key can only be deciphered by RPost, thus securing the contents of the receipt. The receipt also confirms the delivery status and official time stamp of both sending and receiving of the original e-mail message. The Registered Receipt e-mail is a digital snapshot of the server-to-server conversation that surrounds the sending and receiving (or possible non-receipt) of the e-mail and itself can be used to regenerate an authenticated original e-mail (and all attachments) should a subsequent challenge arise. The delivery status will reflect a minimum of "delivery to mail-server" (or "delivery failure") but could show "delivery to mailbox" and "opened" wherever possible.

It should be noted that an absence of a receipt, or an absence of a "date and time of opening" entry does not prove that the e-mail was never received / opened.

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. Thus, even where the content of a stored e-mail has been changed (either inadvertently or maliciously), the e-mail can be independently authenticated by forwarding the Registered Receipt e-mail to RPost where it is unlocked and used for verification purposes. 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.

ISSUES RELATED TO PERSONAL DATA

Within the UK, the processing of personal data is governed by the Data Protection Act 1998. This Act details conditions under which personal data can be legally processed. One of the conditions (the Eighth Data protection principle) 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.

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

SUMMARY

RPost's Registered E-mail® service automatically delivers a Registered E-mail® receipt to the sender containing delivery details of the original message, proof of content and official time stamp. The RPost Registered E-mail® service also enables a stored message to be authenticated at a later date, anywhere a challenge may occur with respect to delivery, time or the content of a Registered E-mail® message. This service functions independent of any action by the recipient.

The authentication / verification of a Registered E-mail® message will include the date and time of sending and receiving, the title and contents of the e-mail message, and all attachments. This registration and authentication / verification process is performed by RPost without storing the original e-mail message as the complete transaction is recorded and imbedded digitally within the Registered Receipt e-mail that is returned to the sender for safekeeping.

As this authentication process is available independently to both the sender and the recipient of a Registered E-mail® message, any contention as to the original contents of the e-mail can be resolved without doubt. By RPost's inclusion of a trusted time stamp with the original Registered E-mail® message, the date and time of the sending and receiving of a message can be demonstrated without doubt.

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

About the Author

Alan Shipman is the Managing Director and Principal Consultant for Group 5 Training Limited, the leading independent consortium of technical experts and consultants providing practical guidance on the implementation of Information Management Systems. Group 5 Training specialise in the application of the BSI-DISC Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP0008), for achieving real business benefits, with particular emphasis on management policies and operational procedures. Alan has been involved in Document Imaging Standards for over 20 years. He is Chairman of the BSI Document Imaging Applications committee, and is convenor of the International Standards Organisation (ISO) Document Imaging Quality sub-committee. He is a member of the UKAIIM Standards Committee, having previously chaired the committee for over 5 years. Alan also chairs the BSI Data Protection Committee which is responsible for BIP0012 - the Guide to the Implementation of the Data Protection Act.

About RPost

RPost® has set the global standard for Legal Proof™ for e-mail. RPost's patented services provide the sender with legally valid evidence of precisely what e-mail content and attachments were sent and received, by whom and when. RPost services include an integrated set of eContracting, e-signature, security and privacy/encryption tools. RPost has strategic business relationships with leading technology and service providers to provide RPost services to their existing clients, including Pitney Bowes, Google/Postini, AT&T, Orange (FranceTel) and BTInfonet, among others. Available in seven languages, RPost's Registered E-mail® services have also been used daily by the United States Government since 2003 and have been endorsed and marketed by many of the influential bar associations. RPost has offices in worldwide, for more information about RPost, please visit www.rpost.com. "Registered E-mail" is a registered trademark owned by RPost.