

Modernize the External Elements of the Contract Management Process

Contract Lifecycle Management Adjacent Technologies

***A User Guide: Tools, Tips, and Legal Framework for Implementing
Electronic Signature, PDF Forms and Registered Email Services to Speed
Contract Signoff and Notice Delivery in Today's Global Marketplace.***

Prepared by RPost for
Automation & Tools Workshop at the
International Association of Commercial & Contract Management
Annual Conference

Table of Contents

Chapter 1. OVERVIEW	1
Chapter 2. SERVICE BREADTH	3
2.1 AUTOMATION AND IMPLEMENTATION: SIMPLE AND INSTANT.....	3
2.2 ELEMENT 1: PRE-CONTRACT INFORMATION, CREDIT, OPERATIONS & APPLICATIONS FORMS.....	6
2.3 ELEMENT 2: CONTRACT NEGOTIATION CORRESPONDENCE	12
2.4 ELEMENT 3: CONTRACT SIGNOFF	15
2.5 ELEMENT 4: LEGAL AND CONTRACT NOTICES	19
2.6 ELEMENT 5: RECORDING INTERIM AMENDMENTS	23
2.7 ELEMENT 6: SENDER SIGNATURES ON PURCHASE ORDERS, DOCUMENTS, & COUNTERSIGNING .	23
Chapter 3. USER AND IMPLEMENTATION TIPS.....	26
3.1 USER TIPS: ENCRYPTION, REFERENCE CODES, COLLABORATION, AND MORE.....	26
3.2 IMPLEMENTATION TIPS AND CONSIDERATIONS	29
Chapter 4. LEGAL ELECTRONIC SIGNATURES	30
4.1 AUTHENTICATION, FORENSIC AUDIT TRAIL FOR HIGH EVIDENTIAL WEIGHT	30
4.2 PRACTICAL FRAMEWORK FOR CHOOSING ELECTRONIC SIGNATURE TOOLS FOR USE INTERNATIONALLY	31
Chapter 5. SUPPLIER LEADERSHIP	53

This user guide will teach you how to:

- Maximize administrative efficiencies around the contracting process,
- Reduce task cycle time, and
- Provide for the highest legal evidential weight of contracts and their associated correspondence and notices in jurisdictions internationally.

Chapter 1

OVERVIEW

Today, most organizations manage contracts and records with associated correspondence using standard email, fax, scanners, and records management tools, having developed their own processes for organization and efficiency. Some rely on Contract Lifecycle Management (CLM) systems which offer a platform to manage tasks, standard terms, approvals, and associated contract records.

Whether an organization uses standard email and document management programs or one of a number of CLM platforms, there are a number of functions that occur adjacent to these systems. If one was to move these to electronic form with robust tools, and implement with automation, one should enjoy significant new administrative efficiencies, cost savings, contract preparation cycle time reduction, and legal spend and litigation risk reduction.

Some of these technologies are familiar – **electronic signature services for contract execution, Registered Email messages for notices, PDF forms automation** – but many have hesitated to deploy for lack of understanding around the legal aspects or implementation simplicity.

This user guide takes a practical approach to demonstrating technologies that may be run within (i.e. operated within the user interface of) desktop or mobile messaging systems, enterprise resource management (ERP) systems, customer relationship management (CRM) systems, and with CLM systems. Essentially, these tools can be operated within any system that has an email send function without any technical integration.

The tools reviewed in this Guide present the contract manager with the opportunity to demonstrate early success with a quantifiable return on investment in contract management modernization efforts. This Guide presents best practice technology tools, tips, and a legal framework for conducting these processes with robust electronic methods that can be implemented in minutes within any CLM, CRM, ERP or email platform in minutes, without IT support.

This guide reviews the following elements in detail, which touch not only a number of the specific functional areas of the contracting process, but also the important implementation, automation, legal and records implications of moving a process to electronic means.

1. Integration and Automation Simplicity
2. Service Breadth:
 - a. **Pre-Contract Information**, Credit, and Application Forms Fill & Sign with Data Extraction
 - b. **Contract Negotiation** Correspondence Records of Recipient Off-Platform Dialog
 - c. **Contract Signoff** with Serial and Parallel Multi-Party Signing Options
 - d. **Legal and Contract Notices** by Electronic Delivery
 - e. **Recording Interim Amendments** by Email and Reply Email
 - f. **Sender Signatures** on Purchase Orders, Documents, and Countersigning Simplicity
 - g. **Additional Built-In Tools**: Contextual Private Notes, Encryption for Privacy, Contract Reference Codes, Document Metadata Cleansing, and more.
3. Legal Electronic Signatures, Authentication, and Forensic Audit Trail for High Evidential Weight
4. Service Selection for International Use
5. Importance of Supplier Leadership

Generally, these tools are implemented within the contract management phases 3, 5, and 6, noted below:

Figure 1: Contract Management Process Overview



Chapter 2

SERVICE BREADTH

2.1 AUTOMATION AND IMPLEMENTATION: SIMPLE AND INSTANT

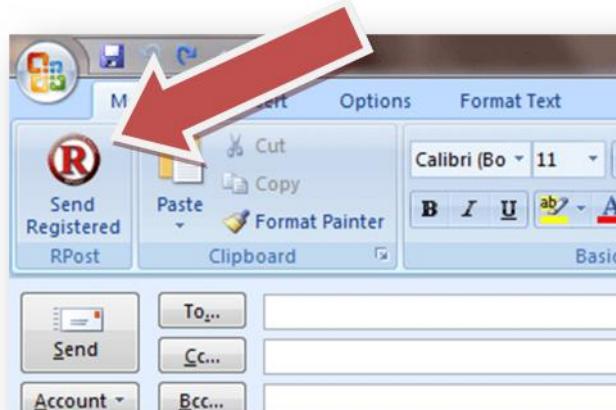
Today, most organizations manage contracts and records with associated correspondence using standard email or fax. All of the technology tools discussed in this guide can be implemented with either a light software add-in to existing software which practitioners are using today within the contract management function, or by simply formatting messages or documents in a particular way. None of these require ‘integration’ that would result in IT resources, or if IT is involved to facilitate the implementation, one would only use at most, very limited time of an IT desktop administrator.

RPost offers free service for individuals (up to three users per company domain) for use in limited monthly amounts (up to 10 times per month). For higher volume or corporate plans, please contact RPost at sales@rpost.com.

The preferred methods of implementing are as follows:

1. If using **Microsoft Outlook** (other program add-ins available in RPost’s [Apps Marketplace](#) for correspondence, RPost recommends its Microsoft Outlook plug-in that runs within the ‘Compose Mail’ user interface adding a “SEND REGISTERED” button next to the “SEND” button. This Microsoft add-in can be installed and used in limited monthly volumes for free, with a two minute download with click-to-install wizard, and runs within the native Microsoft Outlook desktop program. [Click here](#) to download now

Figure 2: Microsoft Outlook User Interface for RMail Desktop App



1. If using any contract management, enterprise resource management, customer relationship management, or other platform, as long as there is a ‘Compose Email’ interface, the sender can simply format the message in a particular way. **To use the services discussed in this guide, one could simply add **.rpost.org** as an extension to the recipient email address as shown below**, and a tag either to the message header or subject line to designate specific services discussed in this guide.

Figure 3: Sending RPost Messages from CLM or Other Email Interfaces with No Installation



2. Automation can then be accomplished using mail merge or batch sending functions of the email program, with the email addresses pulled with the version with the **.rpost.org** extension from the database.
3. RPost also makes available Application Programming Interfaces (APIs) for those that want to further automate or build these capabilities into any custom user interfaces.
4. RPost may be already enabled or available to turn on at the mail gateway or mail appliance level using mail server settings. Some mail systems that are easily configured for the RPost services are Sendmail Sentrion and MessageSystems MTA platforms. If enabled at the gateway, senders can send for RPost services by adding specific subject line content (for example, adding the text “(ESIGNOFF)” in the subject).
5. RPost offers a web-based used interface for accessing all of the services discussed in this guide. User accounts can be set up by simply selecting a password for use with your current email account. [Click here](#) to activate user account.

Figure 4: Sending RPost Messages from the Web Associated with Sender's Corporate Email Account



6. RPost offers access to these services integrated into other online document and sales management systems such as Salesforce.com and Box.net. Contact RPost for more details or visit the RPost Apps Marketplace - www.rpost.com/apps-marketplace.

2.2 ELEMENT 1: PRE-CONTRACT INFORMATION, CREDIT, OPERATIONS & APPLICATIONS FORMS

In the beginning of a business relationship, often there are forms that need to be completed – some are more complex than others.

Using RPost PDF Forms technology, one can simply add a special RPost PDF page to any form, regardless of how complex the form; then post that form for download, or simply email the form to users.

The RPost PDF Form enables the form owner (the sender of the form), without any extended PDF licensing other than use within a standard Reader, and without need for expensive servers, prepare the form within PDF Reader (the recipient of the form for completion or signature) with the following capabilities.

There are lots of variations available, but three common scenarios for sending R-PDF Forms are as follows. In the discussion noted below, the Owner is the form sender and the user is the person submitting the form (i.e. asked to complete or sign the form).

1. The owner sends a regular PDF form (perhaps pre-populated with some data) through the RPost system and RPost adds a signature page en route to the recipient. The recipient can complete the rest of the form and click to sign. RPost authenticates the user, obtains their electronic signature, and embeds onto the form and returns the records to the Owner and user.
- 2) The Owner sends many copies of a prepared R-PDF form to many destinations or puts it on a web site for download. The recipient can complete the form and click to sign. RPost authenticates the user, obtains their electronic signature, and embeds onto the form and returns the records to the Owner and user.
- 3) The Owners gets a prepared form and they have to enter in their own return address (and any workflow addresses for further automation) and the address of the signer, then they click "Send for Signature" on the second page.

R-PDF Form Signoff Records: In all cases noted above, the Owner (and optionally additional workflow addresses) receives a PKI digitally signed, user signed, and time-stamped PDF form with an XML data file to auto-populate form data into database systems.

Consider the following based on your needs:

Scenario (1) is optimal where the form is auto-generated or auto-populated with data.

Scenario (2) is best for web or broad distribution.

Scenario (3) is best for one-on-one transactions -- e.g. broker and buyer.

For example:

To start, the owner can take any PDF form that they have, they can fill it out partially and save. When they are ready to get it completed or signed they send it by email to the address of the signer and append .rpost.contracts.org. the recipient address (or use one of RPost's apps).

Alternatively, the Owner can start with an R-PDF form, one that contains an extra RPost signoff page, and on that page add the Owner and Signer's email addresses, and then click "Send for Signature". Their Outlook (or other native email program) opens up with the partially filled in form attached addressed to the relevant destinations and off it goes.

In summary:

Form Owner conducts one of the processes noted above to send the PDF form to the User (the signer).

Form User:

- a. Complete fill in the form,
- b. Encrypt the transmission of the form data back to the owner
- c. Draw their signature with their mouse, pen device, or stylus with the signature placed on the signature line of the form after a signer authentication process,

Form Owner:

- d. Receive a PKI digitally signed and time-stamped copy of the form with the form fields completed,
- e. Manually or through automated systems, pre-populate some form fields prior to sending to the recipient for signoff or form completion, and
- f. Extract form data in an automated fashion by use of an associated XML data file. This data can then be put into any standard CRM, ERP, or other database.

Figure 5: RPost Signature Panel (the Extra RPost Enabling Page) Added to the End of Any PDF Form

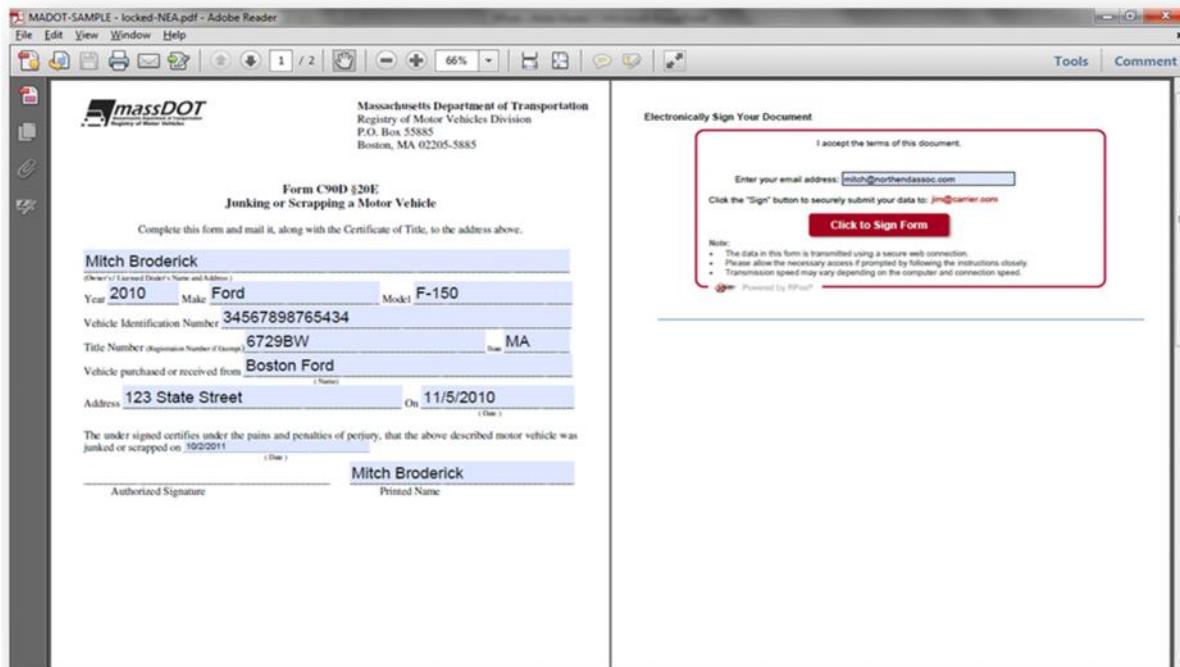


Figure 6: RPost Signature Panel in Detail

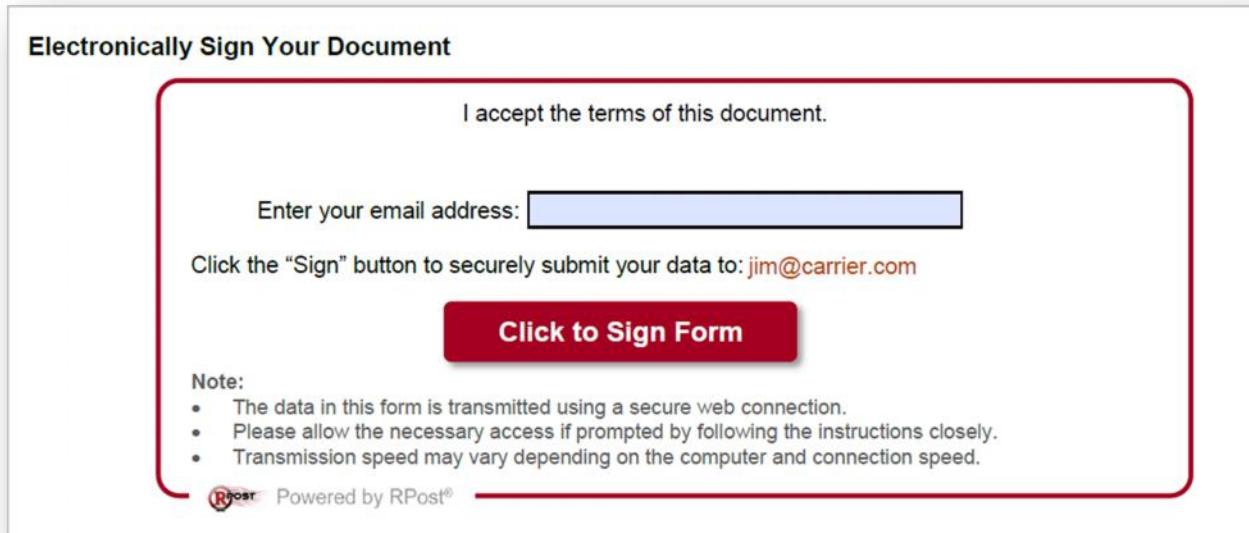
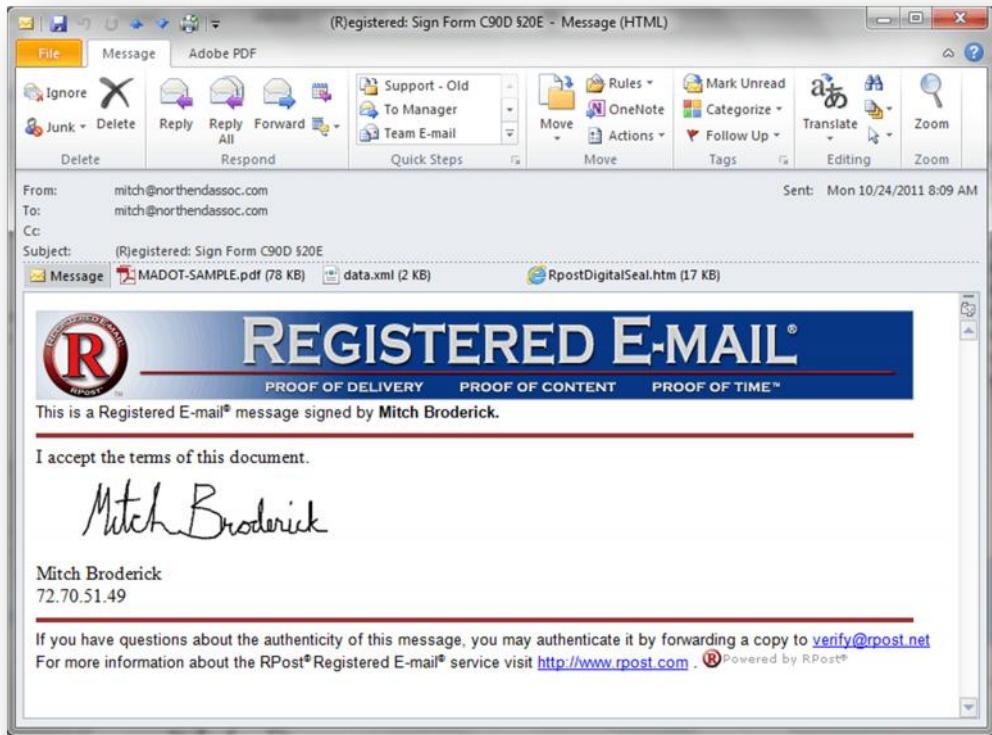


Figure 7: Sender and Signer Receive a Registered Email Message with the PDF Form Attached and Signed, which Includes the Form Data in XML Format



The signed PDF contains:

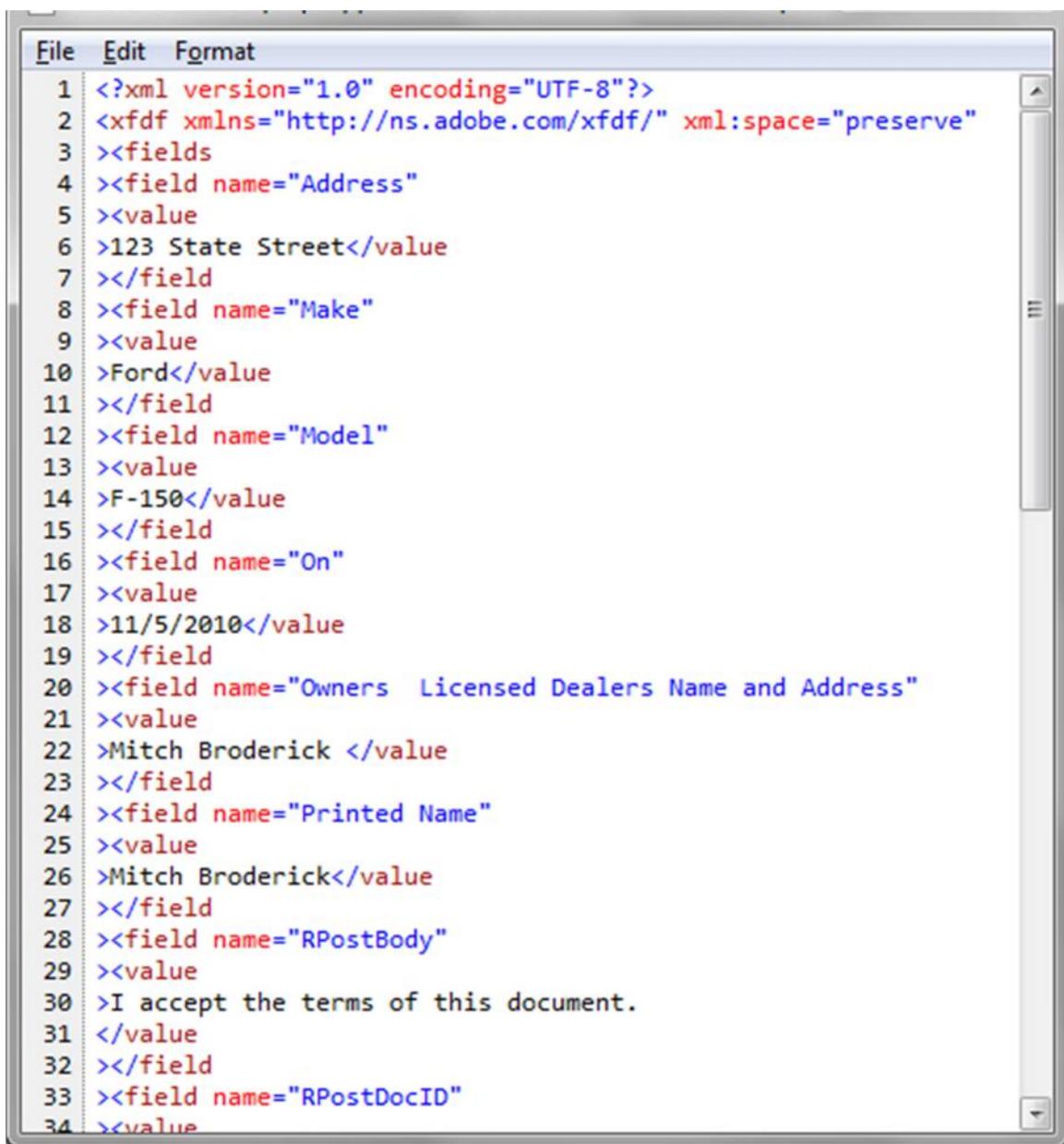
1. **Digital Signature:** Maintains the integrity of the document to avoid altering or tampering with a PDF writer or graphics program.
2. **Legal Electronic Signature:** Records agreement with both a handwritten signature scripted with the mouse, pen device, or stylus and stamp on the bottom right corner of all pages of the document.
3. **Official and Non-Repudiable Time-stamp:** Records official time stamps of the transaction on the PDF document in form that can be verified for content integrity.
4. **Searchable Text:** The signed form can be indexed by standard search tools in records management systems, eliminating the need for OCR recognition.

Figure 8: Signed PDF Using RPost R-PDF Forms Technology

The screenshot shows a PDF document titled "Form C90D §20E Junking or Scrapping a Motor Vehicle". At the top, it says "Certified by RPost Inc SecuRMail <support@rpost.com>, VeriSign, Inc., certificate issued by VeriSign Class 1 Individual Subscriber CA - G3." The form is from the Massachusetts Department of Transportation, Registry of Motor Vehicles Division, P.O. Box 55885, Boston, MA 02205-5885. It includes fields for the owner's name (Mitch Broderick), vehicle details (Year 2010, Make Ford, Model F-150, VIN 34567898765434, Title Number 6729BW, State MA), purchase information (Boston Ford), and the date (123 State Street, On 11/5/2010). A statement certifies the vehicle was junked or scrapped on 10/2/2011. The signature field contains a handwritten signature of Mitch Broderick and the printed name Mitch Broderick. A digital signature stamp at the bottom right indicates it was signed by Mitch Broderick on 10/24/2011 at 5:59:56 PM (UTC).

The email also contains the form data in XML format for easy integration into a contract management system or database. This eliminates the need for an employee to transcribe the data from a fax or a scan into a database. Neither the form Owner nor the form User need PDF extended rights or Adobe® Livecycle® server licenses.

Figure 9: Signed PDF Form Includes the Form Data in XML Format



The screenshot shows a window titled "File Edit Format" containing XML code. The code defines various fields and their values, such as Address, Make, Model, and Owners Licensed Dealers Name and Address. It also includes a signature field for Mitch Broderick and a checkbox for accepting terms.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <xfdf xmlns="http://ns.adobe.com/xfdf/" xml:space="preserve"
3 ><fields
4 ><field name="Address"
5 ><value
6 >123 State Street</value
7 ></field
8 ><field name="Make"
9 ><value
10 >Ford</value
11 ></field
12 ><field name="Model"
13 ><value
14 >F-150</value
15 ></field
16 ><field name="On"
17 ><value
18 >11/5/2010</value
19 ></field
20 ><field name="Owners Licensed Dealers Name and Address"
21 ><value
22 >Mitch Broderick </value
23 ></field
24 ><field name="Printed Name"
25 ><value
26 >Mitch Broderick</value
27 ></field
28 ><field name="RPostBody"
29 ><value
30 >I accept the terms of this document.
31 ></value
32 ></field
33 ><field name="RPostDocID"
34 ><value
```

2.3 ELEMENT 2: CONTRACT NEGOTIATION CORRESPONDENCE

During the contract negotiation by contract specialists, there are often a number of “Rounds” where the contract draft is sent from Outlook or a contract management platform to the other party, and comments are returned. There can be several rounds.

Should a contract dispute arise in the future, even though these drafts are not signed and are not binding, litigators would likely look to these drafts to provide further clarification as to the intent of certain clauses or the interpretation of certain terms. As such, it is important to retain records of the correspondence sent to the other party, and importantly, record the correspondence in the replies from the other party.

The simplest way to accomplish this is to use the RPost Register Reply™ service. This service can be used from any CLM, CRM, ERP (by adding the **.rpost.org** extension to the recipient email address and a subject line prefix of “**(R+)**”) or standard email program (by clicking the added RPost “Send Registered” button and selecting the “Register Reply” service option).

Figure 10: Recipient’s View of a Register Reply Email in their Inbox if Sender Chooses to Include RPost Markings



This service provides the original sender with a Registered Receipt™ forensic email record of delivery, content associated with the delivery, and time-stamp of sending and receipt; as well as the reply content (including attachments) and time associated with the original outbound and reply emails. This Registered Receipt email can be authenticated at any time in the future and serves as an irrefutable and

court admissible legal record of the correspondence. The recipient needs nothing on their end and does nothing differently other than replying to the original email message using any standard email program. The receipt can be easily tagged with a Contract Reference number or other identifier, and stored in archives searchable by the reference number.

When the recipient replies, they simply press the reply button. The recipient does not need to do anything different or have any software. All attachments are recorded in the process. Attachments appear as they normal do with standard email.

Figure 11: View of Recipient Composing a Reply to the Sender's Register Reply Email

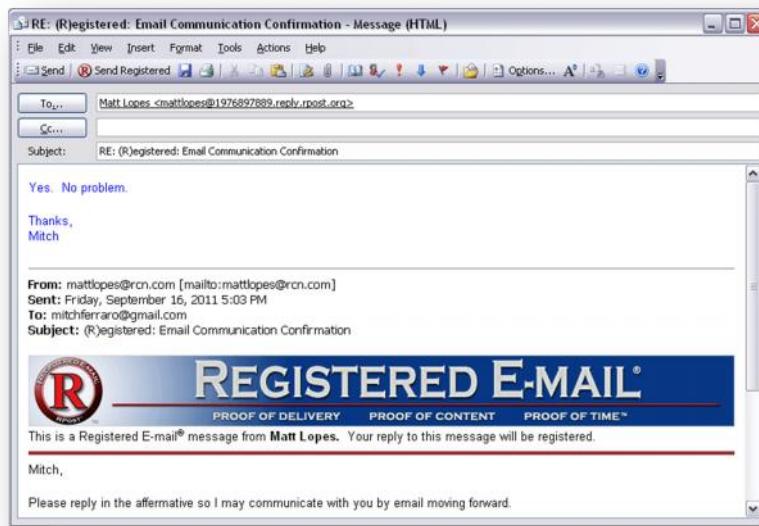
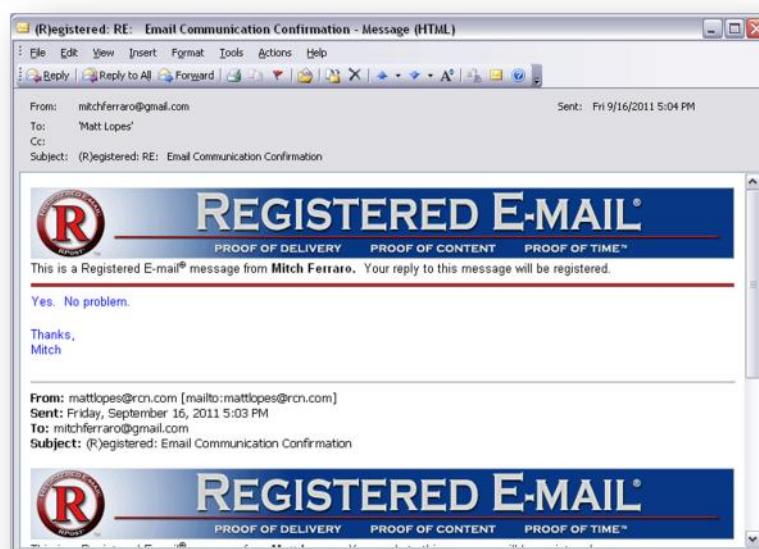
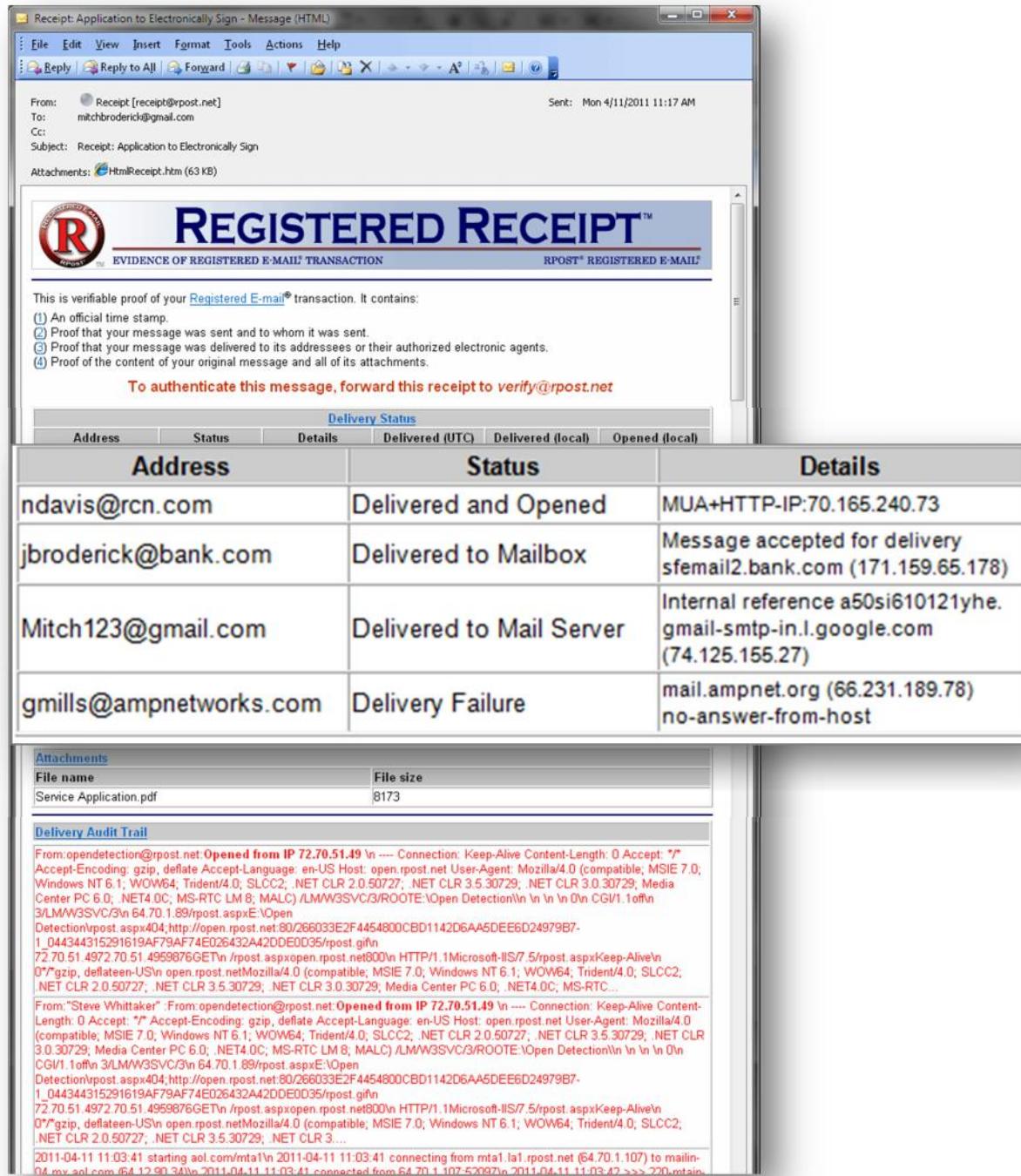


Figure 12: Sender's Inbox View of the Recipient's Reply to their Register Reply Email



The chain continues, and the resulting record contains all of the back-and-forth correspondence as long as the parties use the standard REPLY button in their native email program.

Figure 13: Resulting Audit Trail and Forensic Record of Content, Time-stamps, and Delivery Histories: the Registered Receipt Email Record Returned Only to the Original Sender



2.4 ELEMENT 3: CONTRACT SIGNOFF

After negotiation of the contract terms, a final contract often goes through a final review process for internal approvals, and then is prepared for signature by all parties.

Moving this signature process to electronic can significantly reduce the cycle time of the signoff process which can have benefits depending on the type of contract. RPost offers two services designed to obtain legally valid recipient signatures on the contracts, returning a forensic record of the signoff event, time-stamps, associated content and attachments, IP addresses of the signing parties, with digital signature and other cryptographic authentication capabilities.

The two versions of the service, Email eSignOff service and Hand eSignOff service may be used. The Email eSignOff being the fastest and simplest way to obtain recipient signoff on attached contracts or agreements typed into message body text.

Note, the RPost PDF Forms discussed earlier in this Guide, can be used for contract signoff as well.

The Hand eSignOff service creates a final contract image that has a comfortable and visually familiar look of a traditional pen-and-ink signed contract that is normally later scanned or faxed. This service should have the same legal standing in any country that accepts faxed signatures or scanned images of hand signed contracts as legally valid.

The simplest way to send a contract (as an attached .DOC, .XLS, .PPT, .PDF and newer format files) is to use the RPost service from any CLM, CRM, ERP by adding the **.rpost.org** extension to the recipient email address and a subject line prefix of “**(RPX)**” or standard email program by clicking the RPost “Send Registered” button and selecting the “Email eSignOff” or “Hand eSignOff” service option.

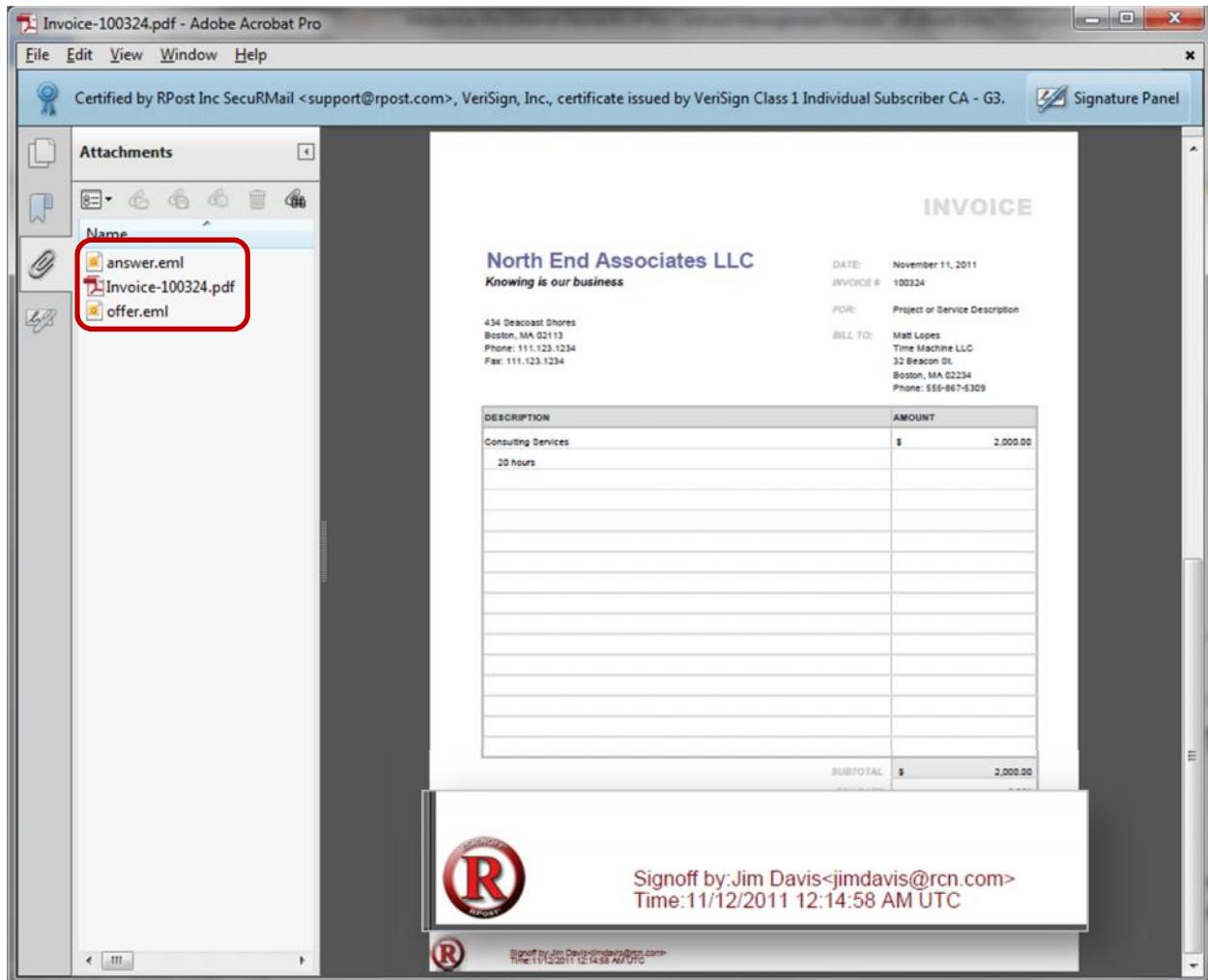
The Email eSignOff service is entirely unique in the marketplace and is by far the fastest way to obtain a legal electronic signature or indication of acceptance of terms on a document or message body sent by email. This service obtains the recipient indication of consent and acceptance of terms with a simple click by the recipient in the received email message body. The signed agreement contains, embedded in the PDF, the original email sent to the signer (offer.eml) and the email response to the sender (answer.eml).

Both “Email eSignOff” and “Hand eSignOff” service options both auto-optimize the signoff technology based on whether the originating document is a custom PDF or Office document or a PDF form. If a PDF form, the RPost service will automatically revert to the R-PDF Forms process.

When to Use:

- Email eSignoff: Desire speed, simplicity or simple and quick signoff on purchase orders or other standard agreements
- Hand eSignOff: Documents that are custom, court or government declarations, or one-off contracts where the sender wants a signoff record that looks like a traditional pen-and-ink faxed or scanned contract.

Figure 14: Example Email eSignOff Contract



The Hand eSignOff service obtains the recipient handwritten, mouse-drawn signature with a simple click by the recipient in the received email message body followed by a few mouse-strokes in an image of the contract that then displays in a web browser.

Figure 15: Hand eSignOff Process



Figure 16: Hand eSignOff Document View in Web Browser After First Party Signs, During Multi-Party Signoff Process



If multiple parties need to sign the same document, with the Hand eSignOff service, one can simply address multiple recipients in the “TO” field of the outbound email with contract attached, and both (or multiple recipient parties) will be then e-signing the same document image. The multiple hand signature service provides the final signed agreement containing the signatures of all parties the message was sent to for signing.

Figure 17: Hand eSignOff Document

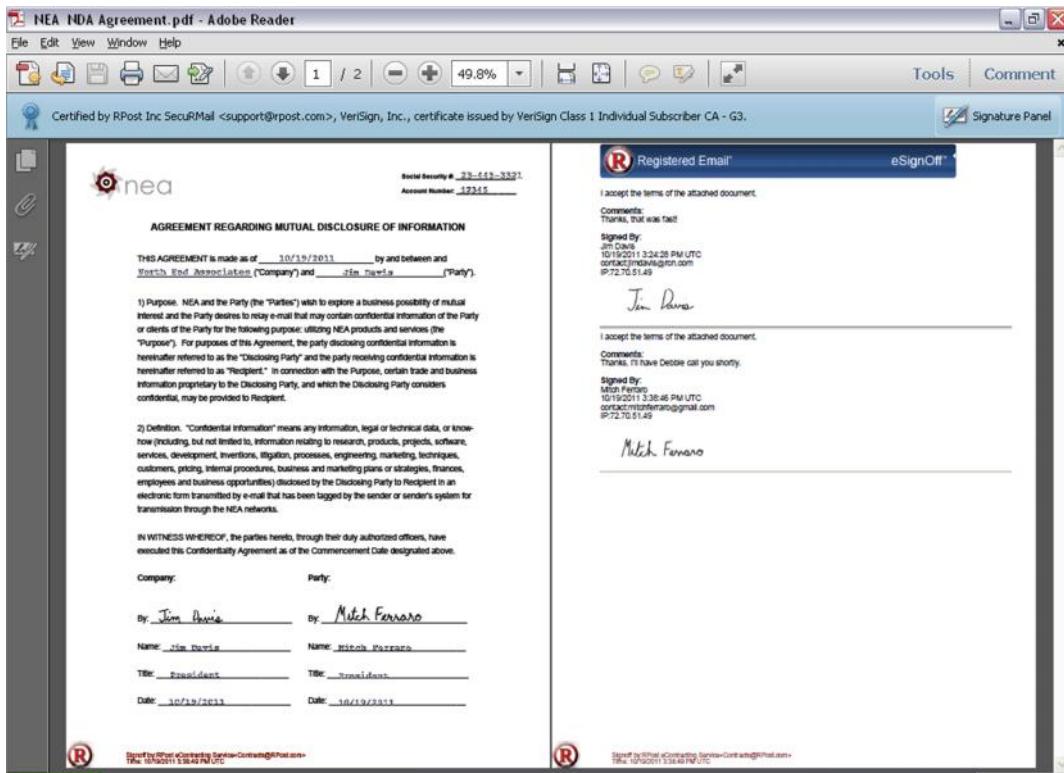


Figure 18: Summary of eContracting Services

Service Summary for Service Used to Obtain Recipient Consent or Signoff			
Register Reply Service: Recording the reply or response of a Registered Email message or form in the email body. Best for recording the back and forth communications or negotiations.		✓	
eSignOff Service by Email: Sending agreement for a quick recipient signature by email; no option for recipient to add text to agreement. Best for a fast, easy signature process for high volume contracts without content add-ons.		✓	
eSignOff Service by Hand: Sending agreement for recipient signature, allowing the signer to add text with the keyboard and mouse-script a signature directly to the agreement. Best for sending automatically generated or individually tailored agreements where the recipient is required to insert some text to the agreement before signing.		✓	✓
RPost PDF Form: Signing a complex form using only a free PDF reader to complete and sign a PDF form. Best for complex forms (completed or signed) when sent by email or posted on website.		✓	✓

Optional Encryption Available
Multiple Signers Available

All of these services also return to the sender a Registered Receipt email record which includes a more detailed forensic audit trail of the signoff process. The details of the Registered Receipt are discussed earlier in this document.

2.5 ELEMENT 4: LEGAL AND CONTRACT NOTICES

Every contract signed has a notice provision. There are notices that are sent during the life of the contract, such as changes in terms, pricing, specifications, quantities, and timing; as well as notices of renewal, default, termination, among others.

Typically, notices are not effective until received; and if the timing of notice is financially important, one should ensure that they send these legal contract notices using a method that will have a record of time and content received that is generated independent of recipient actions.

A July 2010 poll of IACCM members representing more than 75 member companies provided insight into the trends in moving legal notices to electronic delivery. In this poll, most (71%) have hesitated moving legal notices to electronic delivery as they report that they have been in disputes where the recipient has denied receipt of a business critical email. Further, the overwhelming majority (80%) report that they are most concerned with retaining proof of compliance with notice requirements, over time or cost savings (15% and 4% respectively). Jeffer Mangels Butler & Mitchell LLP and IACCM have produced a document that serves as a useful guide, entitled, “Moving Legal and Contract Notices from Paper to Electronic Delivery: A Corporate Counsel Guide.” [Click to download.](#)

For contract notices, the time of receipt of the notice is often important. The [legal time of receipt for email](#) is well defined in the United States by the Uniform Electronic Transactions Act, (notice by email if receipt of the email content can be confirmed, with time of receipt being the uniform time the email enters the information processing system that the recipient has designated or uses for the purpose of receiving email); and in different countries based on the United Nations’ model law that has become the framework for many electronic transaction law definitions. A legal analysis later in this document contains more reference materials.

To accomplish court admissible and irrefutable proof of content and uniform time of receipt of a legal contract notice, one should send these using the RPost [Registered Email®](#) service.

The simplest way to send these notices by the Registered Email service from any CLM, CRM, ERP is by adding the **.rpost.org** extension to the recipient email address. Alternatively, from standard email programs, one can install the RPost plug-in and then clicking the “Send Registered” button.

This service provides the original sender with a Registered Receipt™ email record of delivery, content (including attachments) associated with the delivery and time-stamp of sending and receipt. This Registered Receipt email can be authenticated at any time in the future and serves as an irrefutable and court admissible legal record of the correspondence.

The recipient needs nothing on their end and does nothing different other than reply to the original email message using any standard email program.

When evaluating the risk of potential of claims of non-compliance with contract notice provisions, one considers three points, with that risk mitigated by use of the Registered Email service.

1. **a claim of non-receipt of the notice entirely**, (i.e. where the electronic message is sent from sender to recipient but the recipient denies having received it),
2. **time of receipt is challenged**, (i.e. where sender and recipient claim time of receipt is different, and the notice is time-dependant), and
3. **electronic message content is challenged** (i.e. sender and receiver dispute the validity or inclusion of certain content including attachment content).

SUMMARY OF KEY LEGAL PRINCIPLES ASSOCIATED WITH THE REGISTERED EMAIL SERVICE

Legal opinions assert that RPost's Registered Email meets the following seven legal principles that would likely yield a legally valid and court admissible piece of evidence to satisfy notice provisions in contracts, should the recipient challenge that proper notice had been provided. These legal principles are summarized as follows.

RPost's Registered Email service returns a Registered Receipt email that:

1. **DELIVERY PROOF:** Provides a record of sending and receiving in accordance with the Uniform Electronic Transactions Act (UETA) by recording the recipient's server's receipt;
2. **CONTENT PROOF:** Uses cryptographic techniques to mathematically associate and preserve as tamper-detectable the contents of email and their attachments so as to satisfy process requirements designed under UETA, the Electronic Signatures in Global and National Commerce Act (ESIGN), and in evidence law to establish evidence of content;
3. **OFFICIAL TIME STAMP:** Links to a trusted and objective time source providing essential and credible evidence in disputes in which the time an email was sent or received is material to the case;
4. **ADMISSIBLE EVIDENCE:** Retains the records so that they are court-admissible as to their fact of delivery, as to their legal time of delivery and as to authenticity of content;
5. **FUNCTIONAL EQUIVALENCE:** Serves, under UETA and ESIGN, as the functional equivalent of paper mail, to be used in lieu of certified mail, registered mail, return receipt mail, private express mail services and similar types of paper mail services;
6. **ELECTRONIC ORIGINAL:** Provides a true electronic original of the message content, message attachments, and transmission meta-data including the delivery audit trail; and

7. **CONSENT:** Records consent, as under electronic law the recipient of the electronic transmission must have consented to the use of electronic format as opposed to paper; with a record of the recipient's consent retained as a reproducible legal record to prove consent if challenged.

In the United States, a clear definition as to what constitutes a '*legally received electronic message*' is within the Uniform Electronic Transactions Act (UETA). Assuming UETA applies to the transaction (note, although this reference is to United States law, this principle generally holds internationally as this is based upon a United Nations model law that has been used as the foundation for most electronic transaction laws worldwide), an email is deemed "received" under UETA pursuant to Sections 15(b) and (e), which state the following:

15 (b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when: (1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and (2) it is in a form capable of being processed by that system.

15 (e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

Similar to when mail is sent, the recipient is deemed to have "received" the email, regardless of whether the recipient is aware of its receipt or retrieves the email, when it enters the recipient's "information processing system" or server, provided that the recipient has designated that system for use, uses it and can access the system.

Note, one should review and update all contract notice provisions to include notice by email, if receipt of the email can be confirmed. Some may wish to be more precise and re-state the definitions noted in section 15 of UETA above, to pre-empt any potential issues related to definitions of time of delivery.

Figure 19: Recommended Modern Contract Notice Provision Excerpt

"...notice by email if receipt of the email content can be confirmed, with time of receipt being the uniform time the email enters the information processing system that the recipient has designated or uses for the purpose of receiving email."

RPost's Registered Email service was identified as the top pick by the Jeffer Mangels Butler Mitchell LLP Corporate Counsel Guide to "Moving Legal and Contract Notices from Paper to Electronic Delivery" with commentary from the International Association of Commercial and Contract Managers. View online at: www.rpost.com/downloads/legal-notices-guide.pdf -- includes a requirements list with comparison of different service providers.

Figure 20: Excerpt from Requirements List for Electronic Services for Legal and Contract Notices

<i>Provider</i>	RPost
<i>Product Name</i>	<i>Registered Email®</i>
<i>Category</i>	<i>Email</i>
<i>Evaluation Features</i>	
Delivery Proof	Included
Open Tracking	Included
Content Proof	Included
Official Timestamp	Included
Admissible Evidence	Included
Functional Equivalence	Included
Electronic Original	Included
Self-Authentication	Included
Portability of Evidence	Included
Legal Opinion	Included
Patented Technology	Included
User Simplicity	Included
Ability to Automate	Included
E-discovery Facilitators	Included
Ease of Implementation	Included
Flexible Cost Models	Included
<i>Total</i>	100%

2.6 ELEMENT 5: RECORDING INTERIM AMENDMENTS

After a contract is active, in addition to legal notices, there are often requirements to amend certain terms and record agreement to such amendments. There is also a desire to do so without going through the entire process of updating the complete agreement.

Once a clause is agreed to be amended, one can effect this quickly by inserting in the body text of the email the original clause with the new superseding clause. By then sending this from the CLM system or from desktop email software such as Microsoft Outlook with the RPost add-in as a Register Reply email (as detailed in “ELEMENT 2” of this document), the recipient need only reply and type “Agreed” to affect a legal electronic signature. The RPost Register Reply service cryptographically associates the indications of acceptance with the message content of the reply, and provides Registered Receipt verifiable record.

This receipt (and received reply email) can be loaded into the contract management system as an interim record until such time as the full contract is updated reflecting all of the interim amendments. The proof and authentication process provided by the Registered Receipt is discussed earlier in this document.

2.7 ELEMENT 6: SENDER SIGNATURES ON PURCHASE ORDERS, MESSAGES AND DOCUMENTS, COUNTERSIGNING

There are situations where senders would like a simple and quick way to add their signature to email messages and attached documents. In these cases, leaving a bare image of one’s signature leaves one easily exposed to that signature being associated with other documents without the signer’s permission.

RPost offers its Digital Seal® service with handwritten signature options to:

- Time stamp the email and attached documents,
- Provide non-repudiation as to the content of the email body and attached documents,
- Sign the message body and all pages of associated documents (Word converts to PDF or PDF) as the sender, with hand scripted signature on the bottom of outbound email and attached PDF,
- Sign as sender, with mouse-script handwritten signature optionally saved by RPost system,
- Watermark all signatures with a timestamp, and
- Digitally sign the attached document (if it is a PDF or is converted to PDF format by RPost), with a PKI digital signature for timestamp and content integrity authentication.

Finally, there is a Registered Receipt email for the overall record of transmission with delivery, content proof, and timestamps of receipt, associated with the sender’s signature and documents. The proof and authentication process provided by the Registered Receipt is discussed earlier in this document.

Figure 21: Sender Scripts their Signature on Feature Dialog Box

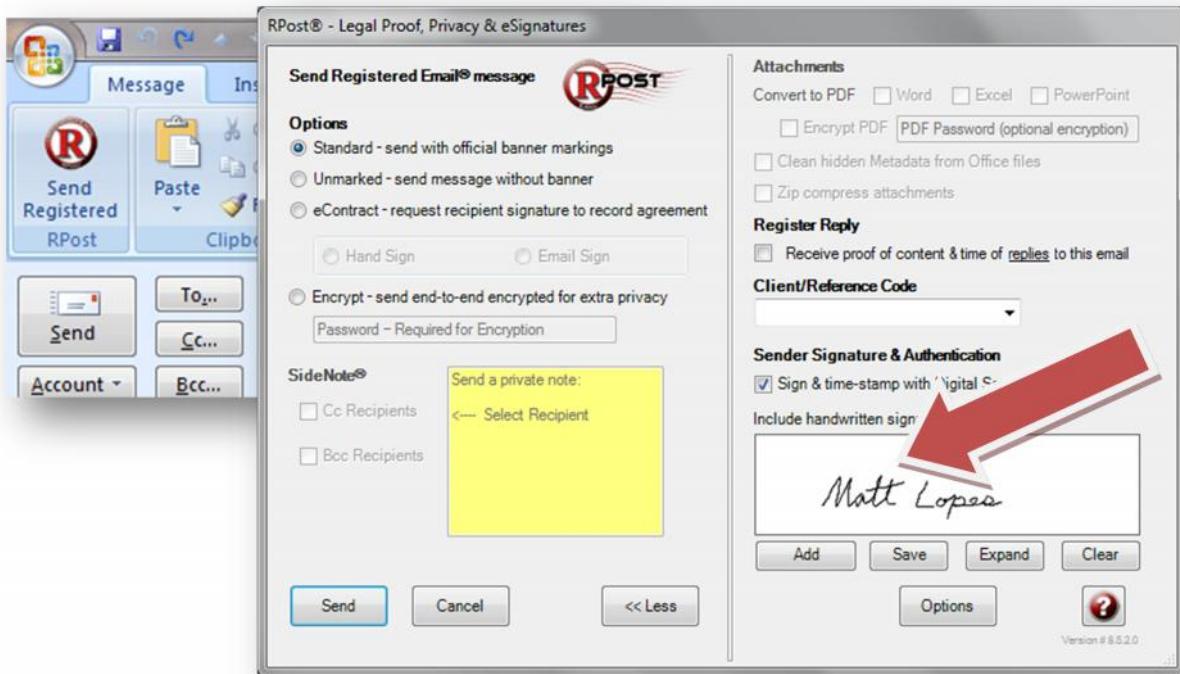
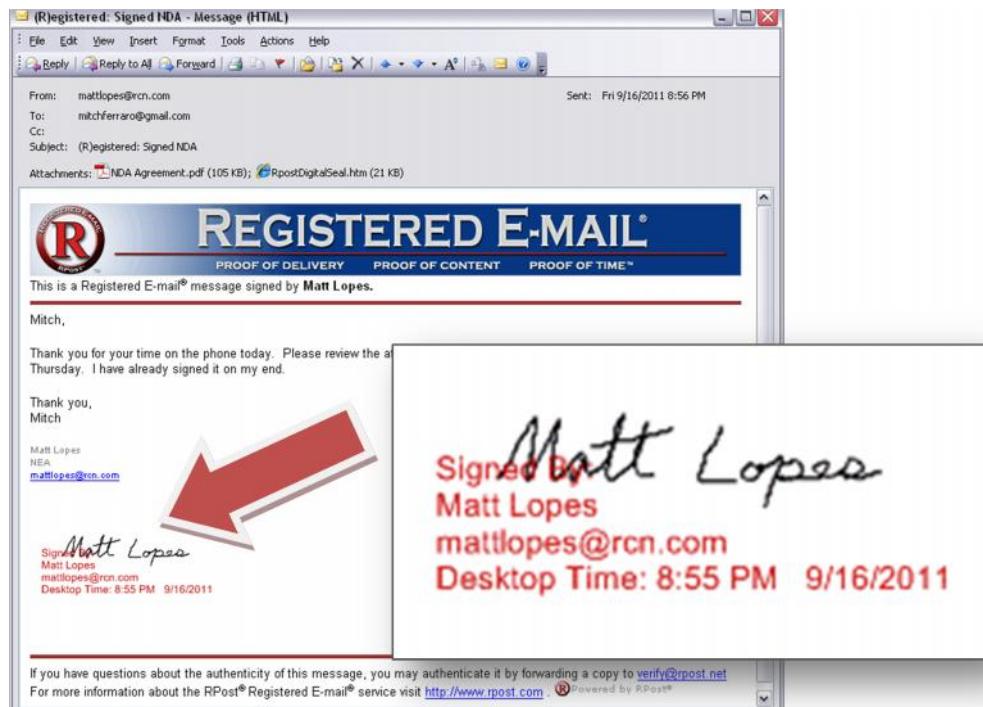
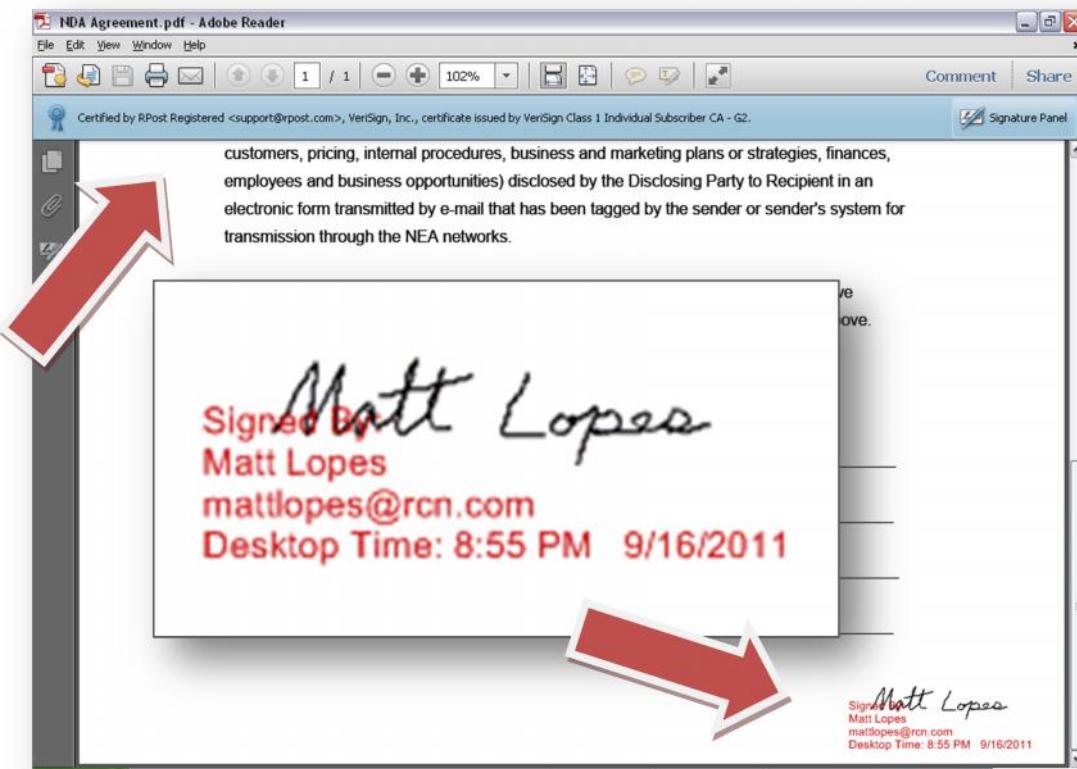


Figure 22: Registered Email Message Containing the Sender's Name, Signature and Time stamped Watermark (the Registered Email Banner is Optional)



All attached PDFs are digitally signed with a PKI certificate and electronically signed with the sender's name, signature and time stamp.

Figure 23: Attachment to an Email Sent with the Registered Email Service Digital Seal Feature and Sender's Signature



Chapter 3

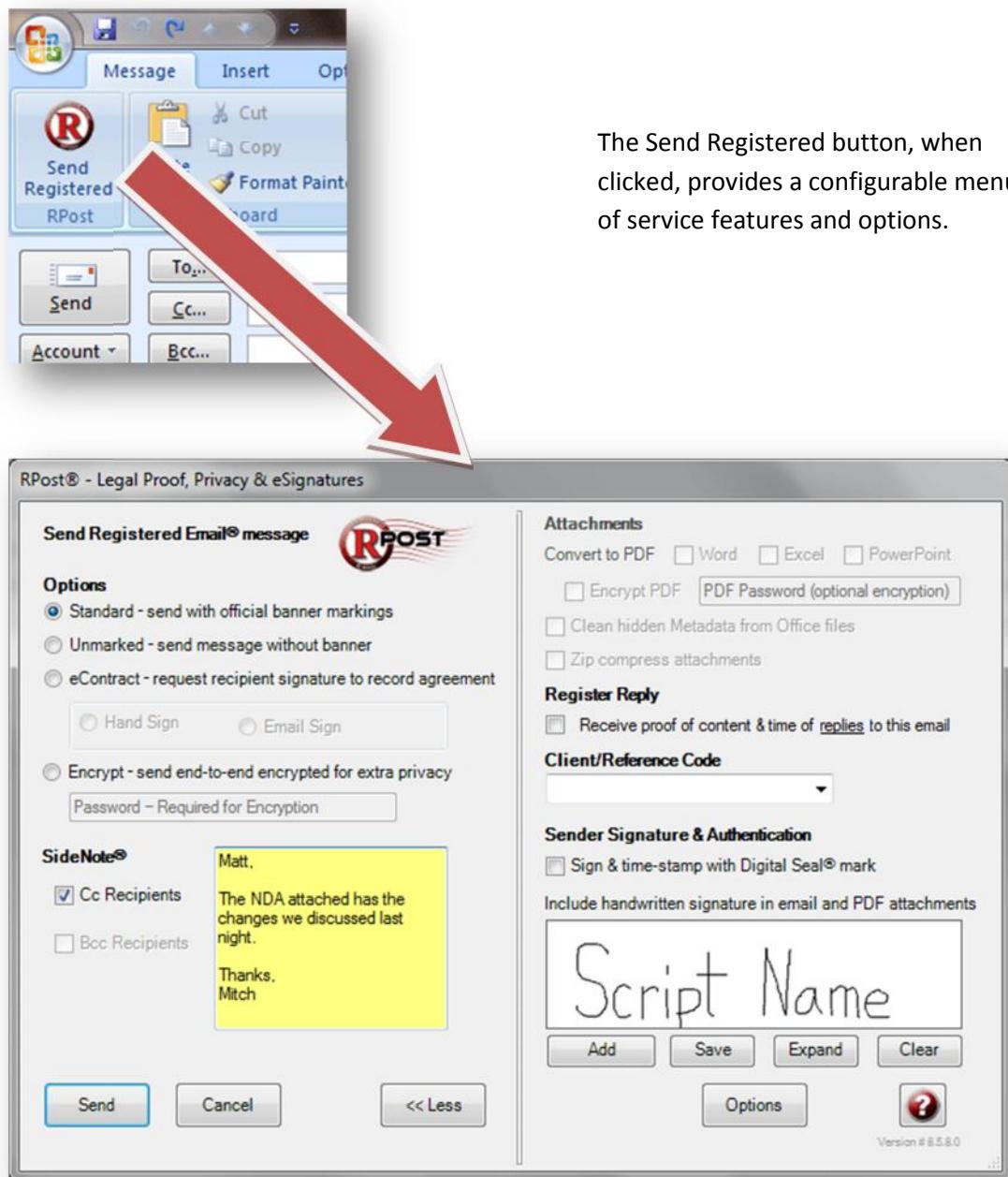
USER AND IMPLEMENTATION TIPS

3.1 USER TIPS: ENCRYPTION, REFERENCE CODES, COLLABORATION, AND MORE

RPost offers additional service, most elegantly accessed using RPost's Microsoft Outlook or other software add-ins.

1. **ENCRYPTION:** RPost does permit users, with all of the services described above, to conduct the correspondence or contract signoff in a secure, encrypted manner.
2. **META-DATA CLEANING:** RPost includes meta-data cleansing services, with the cleansing and processing occurring en route to the recipient. Many contract templates are re-used. Industry does call for cleansing the metadata associated with these documents prior to sending them to external parties as a best practices security requirement.
3. **REFERENCE NUMBERS:** Users who are using a Contract Reference number can, with these RPost services, tag the correspondence to that reference number and have the reference number appended to the subject of all the correspondence if desired.
4. **ACCESS FROM ANYWHERE:** Users can access the RPost services from one's desktop via common web browsers, Microsoft Outlook, or Lotus Notes, as well as from common mobile devices.

Figure 24: Full Featured Outlook User Interface



5. **SIDENOTE® COLLABORATION:** There are situations where a specialist might want to copy or blind copy the manager that originally requested the contract on certain correspondence – or perhaps a person who is supposed to follow-up by telephone or complete some other action triggered by the correspondence. For these additional communications, RPost offers its SideNote® service. This service permits the sender to add a private note for context in the same email, with that private note only visible to the copied or blind copied recipients, appearing as a “yellow-sticky note” at the top of their email.

Figure 25: “To” Recipient View of a SideNote Message

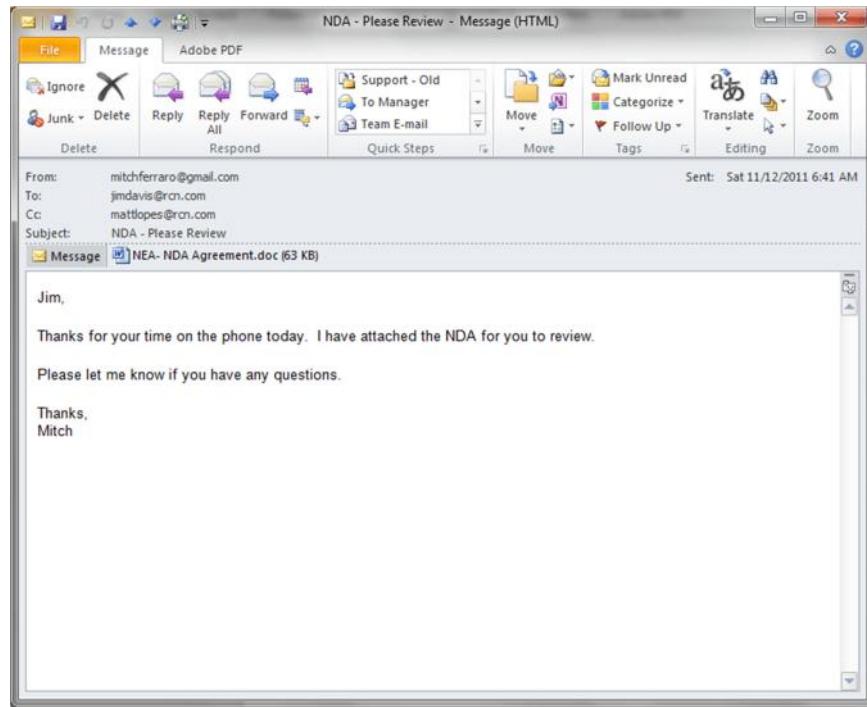
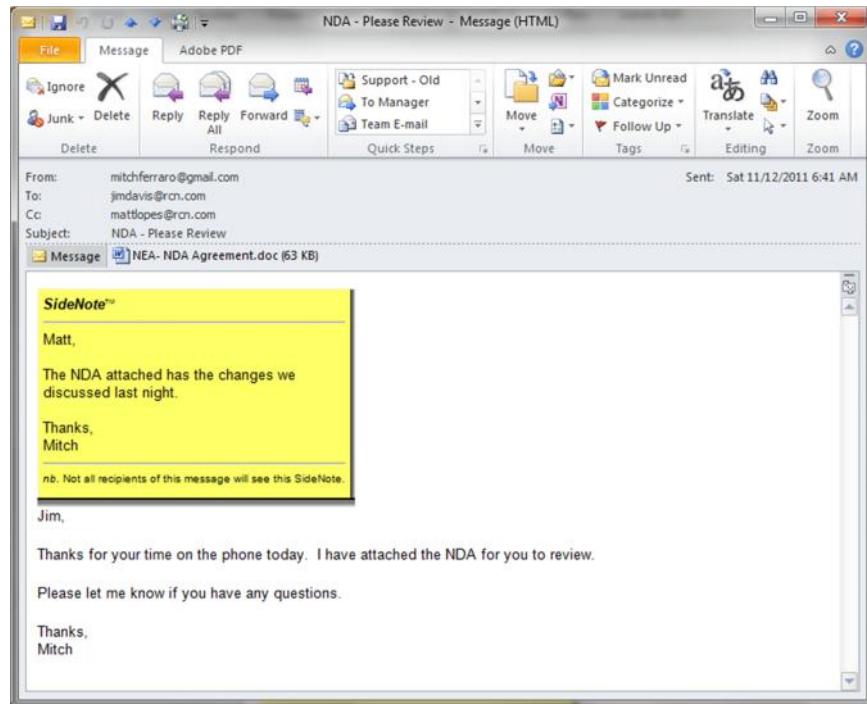


Figure 26: “Cc” Recipient View of a SideNote Message



3.2 IMPLEMENTATION TIPS AND CONSIDERATIONS

When considering use of RPost services versus alternatives, we recommend considering the following:

1. **Breadth of Services:** Choose service providers that have a breadth of service offerings so you do not need to switch providers or plan a new and separate implementation when those additional services will be implemented. RPost provides services that have the greatest breadth.
2. **Service User Interface:** Consider whether users prefer to send from within programs that they currently use. For example, if users use Microsoft Outlook to send document for signoff, consider the Outlook add-in used.
 - a. **How configurable is it? The RPost add-in is very configurable by IT or individual users.** This is important as your organization may want to have certain features locked in upon installation, disabled, or enabled, without any extra ‘customization’ costs. RPost software is fully configurable at installation or after if desired.
 - b. **Is it well written so as not to conflict with other add-ins? RPost software has been tested internationally in a variety of companies and there are no current known conflicts with other software.** Other add-ins may be poorly written, but are considered (if already used extensively) to be standard on the desktop. New add-ins may cause conflicts
 - c. **Does it use the underlying messaging infrastructure within your company or send data to the web via web services? RPost properly has settings so as to now bypass corporate security and records systems.** Records managers, if they have corporate security or archive services, may require outbound messages to route through the messaging servers so as to be included in security screening and enterprise archiving. Pushing documents directly to the web or web services may bypass these corporate security and records requirements.
 - d. **Does it clean up the sent folder so as not to leave unwanted traces of the services having been used? RPost properly cleans up traces from the Sent Folder.** Many Outlook add-ins do not take the necessary steps of removing traces from the SENT folder that can cause end user confusion or conflict with search and indexing.
 - e. **Does it leave unwanted traces of the services having been used, saved in the address auto-fill files? RPost properly cleans up traces in address auto-fill files.** Many Outlook add-ins do not take the necessary steps ensuring they do not leave traces in the address auto-fill files; which could otherwise result in messages being sent to the wrong person.
3. **Understand Ownership of Intellectual Property: RPost's technology has been granted 35 patents valid in 21 countries.** Choose a provider that has invested in intellectual property development; with ownership of technology licenses. Otherwise, ensure you are indemnified from intellectual property infringement damages and know the risk of a system that infringes others' patents being shut down.

Chapter 4

LEGAL ELECTRONIC SIGNATURES

4.1 AUTHENTICATION, FORENSIC AUDIT TRAIL FOR HIGH EVIDENTIAL WEIGHT

According to a July 2010 poll of members of the International Association of Commercial and Contract Managers, the most important consideration of an e-signature initiative is comfort with the legal process (71% of respondents identified this as most important) with cost savings and user training simplicity important but equally far less important (15% of respondents identified these each as most important).

All of the RPost services mentioned in this Guide, including the electronic signature services, operate on the Registered Email technology and therefore return a Registered Receipt email record to the sender.

The [Registered Receipt](#) email is the resulting evidentiary record returned to the sender and includes the underlying Internet forensics (server-level delivery audit trail, IP addresses, official uniform times), and uses mathematical methods and cryptography to associate the message content and attachments (back and forth) with the Internet forensics. This provides non-repudiation of delivery and non-repudiation of replies or signatures depending on the service selected. In other words, delivery, content, time received, and depending on service feature, sender author, content replied to, or signed contracts associated with, cannot be denied if one holds this receipt record.

This record is returned to the sender in the form of a Registered Receipt™ email. The Registered Receipt, at any time, can be independently (third-party) authenticated and if validated, will reconstruct the electronic originals – original message text, attachments, and Internet forensic records all in native format.

This record is portable so that, in a dispute resolution situation, the Receipt can be forwarded by email to any opposing party, counsel, arbitrator, mediator or judicial officer, and that party can, independent of any cooperation or complexity, simply forward the Receipt to an RPost verify email address (verify@rpost.net) to have the Receipt authenticated with original content returned to the party requesting authentication.

Locke Lord Bissell and Liddell LLP confirms this for the United States in their [legal opinion](#), where they describe this Registered Receipt email as providing the sender with delivery proof, content proof, and an official time stamp; packaged as court admissible evidence, providing the functional equivalence to records returned through certified mail, registered mail, return receipt mail, private express mail services, fax logs and similar types of paper mail services; and provides a true electronic original of the

message content, message attachments and transmission meta-data including the delivery audit trail. Alan Shipman, author of the British Standards Institute ‘Legal admissibility’ Code of Practice – BIP 0008 – confirms these points for the United Kingdom in a [legal opinion for the United Kingdom/Europe](#), mapping the Registered Receipt email record to BIP 0008 and European Electronic Commerce Directive (2000/31/EC).

The form in which RPost packages this Registered Receipt email is such that the RPost system does not store any information (yet the Receipt can re-construct the electronic original content when authenticated). RPost does not store copies of these receipts by default and RPost is [Safe Harbor Certified](#).

4.2 PRACTICAL FRAMEWORK FOR CHOOSING ELECTRONIC SIGNATURE TOOLS FOR USE INTERNATIONALLY

NOTE: RPOST DOES NOT PROVIDE LEGAL OPINIONS NOR SHOULD RPOST MARKETING MATERIALS BE RELIED UPON FOR LEGAL DECISIONS. RPOST CAN REFER TO OUTSIDE COUNSEL WHO CAN BE CONTRACTED FOR SPECIFIC LEGAL OPINIONS AND MAKES OUTSIDE COUNSEL RPOST CONTRACTED LEGAL OPINIONS AVAILABLE FROM TIME TO TIME.

SUMMARY

The following decision-framework may be applied to instruct staff as to which method of confirmation of agreement could be used in different situations and international geographic regions.

In general,

1. The Group of Twenty (G-20 major economies), most other advanced nations, and many other less developed countries have passed electronic signature laws. In most countries, the rules of evidence apply, and electronic signatures are legally admissible in court as evidence of the parties’ agreement. The stronger the evidential weight -- the content, time, transmission authentication and other auditable information around the signature process -- the more likely to withstand challenge to evidence of agreement, validity of signature or record of consent, or admissibility in court.
2. Some countries have more liberal electronic signature laws; some countries prefer specific digital signature technologies but do not preclude use of evidence of signoff by use of other technologies. It is generally required that parties agree to sign electronically generally, and may be useful to add consent in the agreement to “use of RPost electronic signatures service to record agreement and RPost Registered Email service for proof of successful transmission of notices by email.”
3. Some examples of countries where electronic signature laws have been passed include Argentina, Australia, Austria, Belgium, Belize, Bermuda, Brazil, Canada, Cayman Islands, Costa Rica, Chile, China, Colombia, Czech Republic, Denmark, Finland, France, Germany, Hungary, Hong Kong, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Macao, Malaysia, Mexico, New Zealand, Norway, Peru, Philippines, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, South Africa, South Korea,

Sweden, Spain, Switzerland, Taiwan, Thailand, Turkey, UAE, United Kingdom, United States, Uruguay, among other countries. This list is not comprehensive.

4. Since the United States (see reference [legal analysis](#)) and the United Kingdom have liberal and well defined electronic signature laws, and in the United Kingdom, there is a British Standards Institute Code of Practice for court admissibility of email as evidence (see [reference](#)), it may be useful to either choose United States or United Kingdom as the governing law in your agreements.

5. RPost does have customers that use its Registered Email and electronic signature services in most countries of the world. In general, these companies:

- a. Select which RPost electronic signature or email evidence service is appropriate for use for their purposes,
- b. Record consent in the agreement to use of RPost electronic signatures service and RPost Registered Email service for proof of successful transmission of notices by email, and
- c. Cite US or UK as governing law for their agreements.

There are other RPost customers that, when parties cannot agree to venue of law or language of the agreement for whatever reasons, yet wish to continue to conduct business, use RPost Registered Email services to record proof of notice of terms and specify in the agreement that continued use of services or continued business conduct shall be governed by the terms of business so noticed and with evidence of such notice having been received by the RPost Registered Email® receipt record.

Again, the above and following framework may provide useful guidance. This is not intended to be or replace legal advice. RPost does not offer or provide legal advice. Information RPost provides is for discussion purposes only and you should rely on your own legal counsel for your specific purposes or your specific legal advice.

Figure 27: Framework for Use of Electronic Signatures in International Commerce

Framework for Use of Electronic Signatures in International Commerce	Region A (United States, United Kingdom...)	Region B (Countries where contract signatures are exchanged by fax...)
Agreement to Methods (Situation A) The parties have agreed to a dispute resolution venue, language and legal jurisdiction in the course of drafting their business agreement.	<u>Preferred Methods</u> Register Reply™ service Email eSignOff® service (RPost Services - A) Hand eSignOff® service RPost PDF Forms service (RPost Services - B) Registered Email® service Digital Seal® service (RPost Services - C)	<u>Preferred Methods</u> Hand eSignOff® service RPost PDF Forms service (RPost Services - B) Registered Email® service Digital Seal® service (RPost Services - C)
Notify of Intent to Conduct Business Based on Terms (Situation B) The parties are not permitted or prefer not to sign the other parties' agreement due to language, law venue, or other considerations, but wish to continue to conduct business.	<u>Preferred Methods</u> Registered Email® service Digital Seal® service (RPost Services - C)	<u>Preferred Methods</u> Registered Email® service Digital Seal® service (RPost Services - C)

SUMMARY OF APPLICABLE RPOST SERVICES

There are three main RPost services that are used by RPost customers today, in countries around the world, for the purposes of recording agreement on terms for which one conducts business with clients, suppliers, and business associates. Depending on the jurisdiction and situation, one may opt to use one of these services:

RPost Service A:

Email eSignOff service - Sign by email with reply.

Register Reply service. Prove time and content that a notice with business terms was received, by Registered Email message, with recording of the associated content in the reply email back to the sender, packaged together in the form of the Registered Receipt email non-reputable record.

RPost Service B:

Hand eSignOff service - Sign by hand with mouse, pen device, or stylus.

RPost PDF Forms eSignOff service - Sign by hand with mouse, pen device, or stylus

RPost Service C:

Registered Email service with Digital Seal service - Prove time and content that a notice with business terms was received, by Registered Email message. One accepts the fact that continued business activity after receipt of terms indicates mutual consent to conduct business under those terms.

SUMMARY OF REGION AND SITUATION DEFINITIONS

Region A: Countries that generally define a legal electronic signature as a sound, symbol or mark; made with intent to sign, logically associated with the content. Some examples of countries in this region include the United States, Canada, Singapore, and the United Kingdom.

Region B: Countries where contract signatures are exchanged by fax, contracts are customarily scanned and stored electronically (PDF, microfilm, Tiff, etc.), or one can rely on the general rules of evidence – the party whose evidence holds greater weight will generally prevail in an evidentiary dispute as to what has been agreed to by the parties. Note, some of the countries in this region will have passed electronic transaction laws that specify a specific type of technology or method of using that technology that if used will certainly constitute a legal electronic signature (i.e. public key infrastructure digital certificates) or specify identification of signing parties, while others will not have. For the framework of this analysis, one could consider all countries that have passed e-signature laws as part of this region, whether or not they specify use of a digital certificate technology, certain certificate authorities, or requirements to

verify identity of sender and/or receiver. A useful partial list of countries with reference to specific country laws is available at [Wikipedia](#); which references the following country electronic signature / transaction laws: Argentina, Bermuda, Brazil, Canada, China, European Union and the European Economic Area, India, Japan, Malaysia, Moldova, New Zealand, Peru, Russian Federation, South Africa, Switzerland, United States, Uruguay, and Turkey.

Situation A: The parties have agreed to a dispute resolution venue, language and legal jurisdiction in the course of drafting their business agreement.

Situation B: The parties are not permitted or prefer not to sign the other parties' agreement due to language, law venue, or other considerations, but wish to continue to conduct business.

Refer to this full analysis and supporting reference material for more detail. Note, there are always exceptions and one should consider, for example, the type of business being conducted, whether or not the business is being conducted with a government agency that has dictated their own rules specific to that agency, the specific definitions of electronic signature and legal time of receipt of email.

SUMMARY OF RPOST SERVICES RELEVANT TO THIS ANALYSIS

RPost makes its services available as an office suite – RPost Office – or individually by service line – [Registered Email](#), [e-Signature](#), or [Email Encryption](#) services.

All RPost service transactions, regardless of service line, return a “[Registered Receipt™](#)” email to the sender as the ultimate record, that can re-construct the other workflow records (i.e. PDFs, etc.) that the RPost service may also generate to memorialize agreement (depending on the RPost service referenced).

Registered Receipt Email

The [Registered Receipt](#) email is the resulting evidentiary record returned to the sender and includes the underlying Internet forensics (server-level delivery audit trail, IP addresses, official uniform times), and uses mathematical methods and cryptography to associate the message content and attachments (back and forth) with the Internet forensics. This provides non-repudiation of delivery and non-repudiation of replies or signatures depending on the service selected. In other words, delivery, content, time received, and depending on service feature, sender author, content replied to, or signed contracts associated with, cannot be denied if one holds this receipt record.

A more detailed description of the Registered Receipt email record is in other sections of this Guide.

RPost Service A: Sign by indication in received email.

Register Reply™ service: This service records the message content, time of delivery, reply content with any text that is typed (such as “I agree”) as indication of acceptance, and reply time. This record is

returned to the sender as an email message for workflow purposes, and as a Registered Receipt for evidentiary purposes.

Email eSignOff® service: This service records the message content, time of delivery, and permits the recipient to click in the email body as an indication of acceptance; then packages a PKI digitally signed PDF record with a watermarks seal and timestamp on each page, recording the content of any attached agreements and the correspondence in the message body. This record, returned to the sender as a PDF, may be used for workflow purposes and can be independently verified for non-repudiation of agreement between parties.

Relevance to this Analysis: Both of these versions of the RPost service provide a verifiable record with high evidential weight, of the recipient's electronic signature on a set of terms attached to an email or in the body of an email – the electronic signature being the symbol or mark; made with intent to sign, logically associated with the content. These services apply to Situation A in Region A.

RPost Service B: Sign by hand with mouse, pen device, or stylus.

Hand eSignOff® service: This service electronically applies the recipient or multiparty recipients' handwritten (mouse scripted) signatures to a contract. The sender attaches any contract to an email and just sends as normal – no contract or form set up is needed. The recipient can review the contract in their web browser and with a few mouse-strokes, handwrite a mouse-scripted signature that becomes electronically sealed to the contract. The process is simple and hassle-free for the user and the end result (the signed-off contract) has the precise look of a traditional pen-and-ink signature on a contract, with the added benefits of RPost's Registered Receipt forensics for future authentication. This service records the message content, time of delivery, and permits the recipient to click in the email body as an indication of acceptance; then packages a PKI digitally signed PDF record with a watermarks seal and timestamp on each page, recording the content of any attached agreements and the correspondence in the message body. This record, returned to the sender as a PDF, may be used for workflow purposes and can be independently verified for non-repudiation of agreement between parties.

PDF Forms eSignOff® service: This service electronically applies the recipient or multiparty recipients' handwritten (mouse scripted) signatures to a complex PDF form with the rest of the service similar to the Hand eSignOff® service described above.

Relevance to this Analysis: This version of the RPost service provides a verifiable record with high evidential weight, of the recipient's handwritten signature on a set of terms attached to an email or in the body of an email. Here, the biometric signature can be forensically identifiable to an individual who is signing in the same manner a handwriting expert might do for a pen-and-ink signature on paper. One may view this resulting signature on "electronic paper" or a PDF, no different in terms of legal standing as pen-and-ink signature on paper that is then transmitted by fax, or a pen-and-ink signature on paper that is then scanned and stored as a PDF electronic record. As such, one may view the important legal consideration for use within a territory as whether that territory accepts fax signatures; or provides electronic records the same legal standing as paper records – a fundamental element of all of the e-signature laws noted in Region B. Further, with the RPost service, the resulting PDF record is PKI

digitally signed -- a technology that is specified in some of the Region B electronic statutes. These services apply to at least Situation A in Region A or B.

RPost Service C: Prove time and content that a notice with business terms was received, by Registered Email message. Accept that continued business activity after receipt of terms indicates mutual consent to conduct business under those terms.

There are two service components to this service – Registered Email® service and Digital Seal® service -- that may be used together to provide non-repudiation of sender, non-repudiation of delivery, non-repudiation of received content and attachments, and non-repudiation of times associated with receipt. When used together, you have full accountability for both parties (sender and receiver).

Digital Seal® service. This service cryptographically provides the recipient of an email with a simple means to verify and prove sender, prove original transmitted message content and attachments, and prove official uniform time of transmission analogous to a postmark. This includes options for “**Sender Hand Sign**” available using some of RPost’s web, mobile, and desktop apps, which would add similar evidentiary characteristics as the Hand eSignOff® service described above.

Registered Email® service: RPost pioneered the concept of proof for email in 2000 by inventing its email proof service entitled, “Registered Email®”. This service from the outset, was designed to provide the sender with legally valid and court admissible evidence of email correspondence occurring from the sender’s desktop email or directly from applications. Registered Email services provide the sender with verifiable evidence of delivery, content, and timing of any contract notice sent by email, in a form that can re-construct the electronic original, without requiring recipients to download any software, click links, or visit special websites to open and read messages.

In certain countries, governments have adopted RPost’s Registered Email service as a national mail product of their national postal operator -- such as the governments of Bermuda, Iceland, Colombia, Cayman Islands, among others. Governments and international government organizations use RPost’s Registered Email service in this capacity for correspondence and notices to nearly every country of the world today.

Relevance to this Analysis: This version of the RPost service provides for full accountability of the transmission of specific business terms from one party to any other, without any requirements or action on the recipient. As such, this service can be comfortably used for any contract related notice where the sender may wish to be able to prove at a later time, the time and content that notice was received. In the context of business agreements, there are situations where two parties are not permitted to (by law or policy) or prefer not to sign the other parties’ agreement due to language, law venue, or other considerations, but wish to continue to conduct business. With this RPost service, the sender may accomplish proof of agreement to business terms without any recipient signature through the Registered Receipt proof of time and content that a notice with business terms was received by Registered Email message; and then by accepting the fact that business activity continued after receipt of terms. This continuity of business after receipt of terms (provided that the notice specifies in some manner that ‘should business continue after receipt of terms, then the terms received are the prevailing

terms governing the continuance of the business') may indicate mutual consent to conduct business under those terms. These services apply to at least Situation A or B in Region A or B.

BACKGROUND

While RPost does not provide its own legal opinions [nor should this analysis or its marketing materials be taken as such], attached are two independent reviews that speak to the strength and integrity of the RPost claim of providing legal and court-admissible proof for e-mail, in compliance with electronic law with respect to electronic document delivery.

- *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 [Click here.](#)
- Confidential Memorandum – *Legal Review of RPost Registered E-mail service in context of Electronic Law relative to Authentication / Admissibility Requirements* by Jon Neiditz, et al of Locke Lord Bissell & Liddell, LLP. [Click here.](#)

Amongst other provisions, the three areas of electronic law that RPost sees as most useful for RPost customers are the following concepts:

Definition A. Validity and Definition of Electronic Signatures

Definition B. Concept of Functional Equivalence

Definition C. Time of Legal Receipt of E-mail

Definition D. Court Admissible Electronic Record

There above are four concepts in these legal opinions that are relevant to this analysis. In particular, Service A relies heavily on definition A (see below); Service B relies heavily on Definition B (see below); and Service C relies heavily on Definition C (see below). All services rely on the Registered Receipt email mapping to Definition D (see below).

US and European Electronic Law

In the United States the enforceability of electronic transactions is governed by the Electronic Signatures in Global and National Commerce Act (ESIGN), a federal law enacted in 2000 that largely preempts inconsistent state law, and the Uniform Electronic Transactions Act (UETA), a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws in 1999. In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999 and the Electronic Commerce Directive adopted in 2000.

The force of these statutes is to remove barriers to the use of electronic transactions and to stipulate that electronic records and electronic signatures cannot be denied legal effectiveness solely on the ground that they are in electronic form.

ESIGN states that, notwithstanding any other rule of law, “a signature, contract, or other record relating to [a] transaction....may not be denied legal effect, validity, or enforceability solely because it is in electronic form.”

UETA provides that “a record or signature, contract, or other record relating to [a] transaction...may not be denied legal effect, validity, or enforceability solely because it is in electronic form.” UETA goes further, affirmatively stating that “if a law requires a record to be in writing, an electronic record satisfies the law,” and “if a law requires a signature, an electronic signature satisfies the law.”

The European Union Electronic Signature Directive requires member states to “ensure that an electronic signature is not denied legal effectiveness...solely on the grounds that it is in electronic form.”

A. Validity and Definition of Electronic Signatures:

- See Locke Lord Bissell & Liddell memo page 7, “Issues and Conclusions” #7 for a discussion of electronic signatures relative to US law.
- See Locke Lord Bissell & Liddell memo pages 16 thru 20 for a more detailed discussion of “Functional Equivalent of Electronic Signatures and Notices.”

B. Concept of Functional Equivalence:

- See Alan Shipman white paper attached that speaks throughout to the point of functional equivalence in discussing electronic transactions.
- See Locke Lord Bissell & Liddell memo attached pages 7 thru 29 with a specific reference to “Functional Equivalent of Electronic Signatures and Notices” on page 16.

C. Definition of Legal Delivery by E-mail:

- See Alan Shipman white paper page 4 “Code of Practice Compliance Provisions” as he discusses proof of delivery.
- See Locke Lord Bissell & Liddell memo attached page 6 “Issues and Conclusions” for reference to “sent” and “received” e-mail under US law. Pages 10 thru 13 speak to evidence of “sending” and “receipt” of e-mail.

EXAMPLE OF COUNTRY SPECIFIC LAWS: AUSTRALIA

The following is an example of how one might view the e-sign laws in Australia in relation to RPost services.

Note: e-commerce provisions in Australia differ with each State and Territory having its own Electronic Transactions Act. While they generally track the Commonwealth Electronic Transactions Act of 1999, they each have differences in definitions and have some additional sections. Further, there are some unrelated laws that affect the Electronic Transactions Act: (a) Consumer Protections (b) Trade Practices

Act of 1974, (c) Australian Security and Investment Commission Act 2001, (d) Privacy Act of 1984, and the (e) Cybercrime Act of 2001.

Focusing on the Commonwealth Electronic Transactions Act of 1999, RPost considers the following sections to be most relevant in reviewing its service capabilities for compliance and utility.

A. Validity and Definition of Electronic Signatures (see below)

B. Concept of Functional Equivalence (see below)

C. Definition of Legal Delivery by E-mail (see below)

A. SECTION 10: Signature

Excerpt: If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if: (a) in all cases--a method is used to identify the person and to indicate the person's approval of the information communicated; and (b) in all cases--having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and...

Relevance to this Analysis: Since the Australian law cites "in all cases--a method is used to identify the person..." as being a requirement, we would interpret this such that Service B would be more applicable in Australia as providing a method (handwriting comparison) that can be used to identify the person.

B. SECTION 8: Validity of electronic transactions

Excerpt: For the purposes of a law of the Commonwealth, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.

Relevance to this Analysis: This section is useful for Service A, B, or C.

C. SECTION 14: Time and place of dispatch and receipt of electronic communications

Excerpts:

Time of dispatch (1): For the purposes of a law of the Commonwealth, if an electronic communication enters a single information system outside the control of the originator, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the dispatch of the electronic communication occurs when it enters that information system.

Time of receipt (3): For the purposes of a law of the Commonwealth, if the addressee of an electronic communication has designated an information system for the purpose of receiving electronic communications, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication enters that information system.

Relevance to this Analysis: This section is useful for Service C for proof time received for contract notice or receipt of business terms.

(Commonwealth Electronic Transactions Act of 1999 available online at:
http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/)

EXAMPLE OF COUNTRY SPECIFIC LAWS: SINGAPORE

The following is an example of how one might view the e-sign laws in Singapore in relation to RPost services.

In July 1998, the Electronic Transactions Act (ETA) (Cap 88) of Singapore was enacted to provide a legal foundation for electronic signatures, and to give predictability and certainty to contracts formed electronically. The Singapore ETA follows closely the UNCITRAL Model Law on Electronic Commerce, which sets the framework for electronic laws in many countries.

It is important to note that the Act explicitly permits parties to vary the rules in the Act if both parties agree to the variation or procedure, as stated: "Variation by agreement: As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision [of the general ELECTRONIC RECORDS AND SIGNATURES and the ELECTRONIC CONTRACTS sections] may be varied by agreement [between the parties]."

It is also important to note that the Act does not apply to the creation of wills, trusts, execution of powers of attorney, documents of title, negotiable instruments, sale or transfer of real estate ("immovable property"). Although, the Act explicitly states that the Minister may amend to limit these carve-outs at any time, thereby expanding applicability of the law.

Focusing on the Electronic Transactions Act of 1998, sections II and IV in particular, RPost considers the following sections to be most relevant in reviewing its service capabilities for compliance and utility.

A. Validity and Definition of Electronic Signatures

B. Concept of Functional Equivalence

C. Definition of Legal Time of Sending and Receipt for Email

REFERENCE PART II and Part IV OF THE ACT

There are three sections that are important here. First, consider the **definition of an electronic signature** as: "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."

Relevance to this Analysis: This definition in Singapore is similar to the definition of electronic signature in the U.S. law and one could review the Locke Lord Bissell & Liddell opinion for further analysis. One might interpret this, such that Service A or B would be apply in Singapore.

Note in Section 6, Legal Recognition of Electronic Records, the law clearly declares the **validity of electronic signatures**: "...information shall not be denied legal effect, validity or enforceability solely on

the ground that it is in the form of an electronic record." The **validity of electronic transactions** are discussed in Section 11.1, where the law clearly states in reference to electronic transactions, that the "offer and the acceptance of an offer may be expressed by means of electronic records."

Sections 7 and 8.1 discuss the **concepts of functional equivalence**. In Section 7, Requirement for Writing, the law states that, "where a rule of law requires information to be written...an electronic record satisfies that rule of law..." In Section 8.1, Electronic Signatures, the law states 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." In Section 11.2, the law discusses the **concepts of functional equivalence in relation to electronic transactions**, and declares that, "where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose."

With regards to situations where one party or a type of transaction may require some form of associating the electronic signature with the party signing, Section 8.2 clearly permits such association to be provided for if, for example, the service provider or system for embedding the electronic signature can "show that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party." This could be accomplished by, for example, a service provider recording the email address of the party (of which the party would have had to have had the user name and password to access the received document for signature) along with the time stamp and internet protocol address of when and where the party accessed the document to electronically sign.

If one is interested in confirming intent by both parties to conduct a transaction in electronic form, Section 12 permits recordation of the intent by electronic means: "As between the originator and the addressee of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record."

Relevance to this Analysis: This section is useful for Service A, B, or C.

Section 15 defines **the legal time and place of dispatch and receipt for email**.

The **legal time of sending** is defined in Section 15.1 as "when it [the email] enters an information system outside the control of the originator..." In the context of the RPost system, the legal time of sending would be the time the email was inducted for processing by the RPost system.

The **legal time of receipt** for email is defined in Section 15.2(a)(i) as occurring "at the time when the electronic record enters the designated information system [provided by the recipient]." In the context of the RPost system, the "designated information system" would be the server of record listed in the Internet mail exchange (MX) records associated with the recipient email address. The legal time of receipt for an email would be the time the email was determined to have been accepted by the information processing system of the recipient.

Relevance to this Analysis: This section is useful for Service C for proof time received for contract notice or receipt of business terms.

EXAMPLE OF COUNTRY SPECIFIC LAWS: BERMUDA

E-commerce provisions are generally defined by Bermuda's Electronic Transactions Act of 1999.

The aspects of the Bermuda e-commerce laws most relevant to RPost customers appear to coincide with US and European e-commerce laws. It is likely, therefore, that an independent party retained to produce a formal legal opinion would conclude that RPost's services track the requirements of electronic transaction laws as follows.

Focusing on the Electronic Transactions Act of 1999, RPost considers the following sections to be most relevant in reviewing its service capabilities for compliance and utility.

A. Validity and Definition of Electronic Signatures

B. Concept of Functional Equivalence

C. Definition of Legal Time Sent and Received for E-mail

A. Validity and Definition of Electronic Signatures

The following are some excerpts from the Act:

definition section: "electronic signature means a signature in electronic form in, attached to, or logically associated with, information that is used by a signatory to indicate his adoption of the content of that information and meets the following requirements— (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using means that the signatory can maintain under his sole control; and (iv) it is linked to the information to which it relates in such a manner that any subsequent alteration of the information is revealed";

RPost's electronic signature services are comprised of two aspects; (a) obtaining the indication of acceptance from the signatory, and (b) providing the forensic evidence that that indication of acceptance was associated with the precise content of the signed material and at what time the material was signed. relating to point (a) RPost has a biometric signature option that satisfies the definition points (i), (ii), and (iii), and RPost uses cryptographic techniques that satisfy the definition point (iv).

these points of the RPost service noted above further satisfy the requirements of section (11) of the act, subsection (1), which states: (1) where the signature of a person is required by law, that requirement is met by an electronic record if— (a) a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic record; and (b) that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

it is important to note that in section (11) of the act, subsection (2), an electronic signature remains valid whether or not it is associated with an accredited (digital) certificate. this subsection states: an electronic record that meets the requirements of subsection (1)(a) and (b) shall not be denied legal effect, validity and enforceability solely on the ground that it— (a) is not an electronic signature; or (b) is not associated with an accredited certificate

Relevance to this Analysis: One might interpret this such that Service B would be more applicable in Bermuda as providing a method that can be used to identify the person. For sender signatures on documents, Service C (Digital Seal®) appears to also apply.

B. Concept of Functional Equivalence

The following excerpts from sections of the Act clearly state that electronic records, transactions, writings, and court evidence are proper in electronic form, and RPost's services clearly facilitate and provide for this proper use, or in fact better use (in terms of yielding greater evidential weight of resulting electronic evidence).

Excerpts follow:

Section 8. "Legal recognition of electronic records: 8 Information shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is— (a) in the form of an electronic record;"

Section 9. "Writing: 9 (1) Where information is required by law to be in writing or is described in any statutory provision as being written, that requirement or description is met by an electronic record if the information contained in the electronic record is accessible and is capable of retention for subsequent reference."

Section 15. "Formation and validity of contracts: 15 (1) In the context of formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records."

Section 14. "Admissibility and evidential weight of electronic records: 14 (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic record in evidence—(a) solely on the ground that it is an electronic record... (2) Information in the form of an electronic record will be given due evidential weight and in assessing the evidential weight of an electronic record, regard shall be had to— (a) the reliability of the manner in which the electronic record was generated, stored or communicated; (b) the reliability of the manner in which the integrity of the information was maintained;"

Relevance to this Analysis: This section is useful for Service A, B, or C.

C. Definition of Legal Time Sent and Received for E-mail

The RPost system provides a record of legal time of sending and receipt of an electronic record as defined by the Act. The following are the relevant excerpts from sections of the Act.

Section 18. Time and place of dispatch and receipt of electronic records:

Excerpts:

Time of dispatch: "(1) Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information processing system outside the control of the originator."

Time of Receipt: "(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows— (a) where the addressee has designated an information processing system for the purpose of receiving electronic records, receipt occurs— (i) at the time when the electronic record enters the designated information processing system; or (ii) if the electronic record is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic record comes to the attention of the addressee;"

Again, RPost services provide for what the Act calls for.

Note, section (10) of the Act discusses "legal delivery" as in legally serving papers on a person and this process would be conducted using RPost's Register Reply™ service with legal delivery in this case having been confirmed if receipt is acknowledged (and then recorded by the RPost system) by a reply e-mail.

Relevance to this Analysis: This section is useful for Service C for proof time received for contract notice or receipt of business terms.

EXAMPLE OF COUNTRY SPECIFIC LAWS: BELGIUM

Validity and Definition of Legal Aspects of Registered Email, Digital and Electronic Signatures Services.

1. Question

This analysis concerns the RPost service entitled "*Registered Email*" and the additional service entitled "*Electronic Signature*". The same services are offered on the Dutch web site rpost.nl under the names "*Aangetekende Email (Registered Email)*" and "*Digitale Handtekening (Digital Signature)*", respectively. This discussion is about verifying (1) which evidential value Belgian law allocates to emails that are sent within the context of the Registered Email service and (2) whether the RPost "*Digital Signature*" can qualify as an electronic signature in the sense of Belgian law.

2. Summary

Below is a summary of our conclusions regarding the questions as set out in point 1 above. Further below in this memorandum we outline the different elements that brought us to these conclusions.

- There are no particular regulations (as yet) regarding electronic registered mail in Belgium.

- There are now disputes on the value of proof of ordinary emails, especially when both parties do not agree as to the authenticity of the time of successful transmission and content transmitted. Ordinary emails are generally regarded as valid proof and as such accepted by the Belgian Courts.
- However, in recent jurisprudence ordinary emails have been refused as proof because there were indications that the email system by means of which the emails were sent, could possibly be manipulated.
- The Registered Email service of RPost offers added value to senders of important electronic messages given the fact that, as independent third party, RPost is able to authenticate the integrity of an email message, which includes authenticating the time of sending, time of successful transmission, content of the message and attachments, and the identity of the sender through the use of technical security measures.
- Moreover, the Registered Email service complies *prima facie* with the conditions as listed in the previous act on registered electronic mail, which has, however, been abrogated in the meantime. Seeing that this legislative initiative will presumably be resumed again in the near future, it is definitively to the advantage of RPost that its services already comply with the initially listed legal conditions.
- We therefore expect that the Registered Email service of RPost will be accepted as a reliable technique of proof by the Courts and that this will provide a stronger position of proof than an ordinary email where the value of proof shall extend to (i) the time at which it was sent (ii) the delivery of the message to the addressee and (iii) the contents of the email and all attachments. RPost additionally offers methods of identifying the sender and receiver which include options for sender account activation, recording IP addresses, adding or requesting mouse-scripted handwritten signatures applied to the record, or requiring personalized passwords to access the message.
- Given the fact that the integrity of a Registered Email message can always be disputed before Court, it is important to note that the sender of the Registered Email message, or receiver of the Registered Email message with the RPost Digital Seal file store the Registered Receipt or Digital Seal record so that they can email the record to RPost for authentication at any time, after which RPost returns an authentication report with the authenticated original message content, forensic record, and timestamps. This authentication process and resulting record can be presented to a Court in case of a dispute.
- An email or document as confirmed by an RPost Digital Signature, constitutes a legally valid and permissible means of proof in legal proceedings. In this regard, the “*Digital Seal*”, “*eSignOff*” and “*eContract*” services qualify as advanced electronic signatures in the sense of Belgian legislation on electronic signatures.

3. General description of the RPost services

Our advice and conclusions in this memorandum are based on the factual outline of the RPost services as set out by RPost during an on-line demo on 18 January 2012 and on the information available on the rpost.nl and rpost.com websites. A useful reference on RPost websites is a detailed review on [court admissibility of Registered Email services](#). While this focus is on US electronic transactions laws, many of the principles carry forward to the rules of evidence and our analysis.

a. Registered Email

RPost commercialises the Registered Email service as an electronic message with legally valid proof. Its value of proof would extend to the sending of the email, its delivery to the receiver, the official time at which it was sent and the content of the email as sent and received, including the attachments.

The user must first register to be able to use the Registered Email service. Such registration is effected either by way of an email, account set-up or payment based authentication process or by way of an agreement between RPost and the user whereby the user is identified and payment data are furnished. From a technical point of view, the user can use a web user interface or install a plug-in for Microsoft Outlook, Lotus Notes, or some mobile devices and programs. Hereby a “Send Registered” button will appear in its email program. When the user sends an email by using this button, this email is linked to a unique code which identifies the registered user. Receivers of such emails do not need special software to be able to receive such emails.

After a Registered Email has been sent, the sender first receives a confirmation of the fact that his or her email has been sent, together with the identification of the addressee and the time at which it is received by the RPost registration service. A receipt is then automatically generated in the sender's mailbox, in which the delivery status of every Registered Email message is verified.

RPost uses hashing algorithms to authenticate email content: a Triple DES encrypted copy of the message in combination with an SHA-1 hash is attached to the receipt. In this way the content of an email can be verified at a later point in time. The actual content of an email does not need to be filed or saved by RPost for this purpose because all processing takes place on the Internet (SaaS model), whereby RPost is responsible for processing the emails. By sending the receipt of a Registered Email message to RPost for verification, RPost can compare the hash code of the original email and the plain-text version to verify whether both versions correspond.

b. Digital Signature

RPost offers three different services that fall under the heading of Digital Signature: (i) a digital signature that the sender can attach to an email (“*Digital Seal*”), (ii) a digital signature that a receiver of an email can put under that message as acceptance thereof (“*eSignOff*”) and (iii) two or more digital signatures that can be attached to the same document (“*e-Contract*”).

The Digital Seal is attached to a Registered Email to certify the identity of the sender and the content of the message. This Digital Seal is based on PKI technology through which a compressed version of the email message, together with the identification of the sender, is included in an HTML file, which is attached to the email message. This HTML file can be presented to RPost for verification at any later

point in time. RPost can decrypt this file to verify the integrity of the content of the message and, at the request of the sender/signatory, to draft a report of this.

With the eSignOff service the receiver of an email can view and sign an entire document without the possibility to make any changes to its content. For this purpose the signatory just uses his mouse and "writes" his handwritten signature with the cursor in a field specially provided for this purpose. Through this the signatory's IP address is registered and added to the message. Here, too, a PKI digital signature is attached to the document to be able to show the identity of the signatory and the integrity of the message content in the future.

Finally, by using the e-Contract service, the initial sender can countersign an electronic message that has already been signed by the receiver with the eSignOff service. The sender then first sends an email message to the receiver with an eSignOff service request, the latter signs and RPost returns the message to the sender who, in his turn, signs the message. In this case, a time stamp is generated of both the sender's and receiver's signatures. As is the case with the Digital Seal and eSignOff services, this service is also based on PKI cryptography.

4. Value of proof of the Registered Email service for the purposes of Belgian law

a. No particular legislation regarding registered electronic mail

Belgian law does not, as yet, have any particular legislation in place on registered electronic mail. This means that for the purposes of assessing the value of proof of the RPost Registered Email service, we must turn to the Civil Code (see point b). The legal value of a registered electronic mail must therefore be assessed ad hoc, taking into account the quality of the service offered. When making this assessment we can actually take the definition of an "ordinary" registered mail in the Postal Act into account, i.e. "*a service that consists of guaranteeing, for a fixed rate, against risks of loss, theft or damage, whereby the sender, where appropriate at his request, receives proof of the submission and/or of the order of the postal mail to the addressee*".

The Belgian legislator has however already considered the issue of registered electronic mail. Nevertheless, this has not yet resulted in particular legislation in this regard. As a matter of fact, a law on this subject was recently withdrawn only one month prior to taking effect. Because we expect that new legislative initiatives will possibly be taken in the (near) future, we give a brief outline of the legislative history in this regard (see point c).

b. Generally applicable Civil Code rules concerning evidence

The evidential value of emails does not generally pose any problems for Belgian Courts.¹ They generally accept regular (printed) emails as proof in the light of the general rules Civil Code concerning evidence², unless a party disputes their authenticity.

¹ E. VALGAEREN, "ICT en bewijsvoering – Het paard van Troje" ("ICT and provision of proof - The Trojan Horse"), in X., *De bewijsregeling in arbitrage* ("The rules on evidence in arbitration"), Bruylants, Brussels, 2009, 115

However, in a recent case the Court of Appeal in Ghent refused to accept the email submitted as evidence³. In the case referred, the emails in question were sent through an internal company email system. The Court ruled that the internal email system could be easily manipulated by the managers and that it could therefore not be reasonably shown that the emails had actually been sent by the so-called sender and that its content had not been changed.

One can expect that similar cases will occur in the future. Courts will in such cases ask parties to deliver proof which shows that a disputed email was actually sent and received and that its content remained unchanged. In this respect the judgement of the Court of Appeal can be seen as urging companies to use more reliable supplementary techniques of proof.

In this respect the RPost Registered Email service can fill the void. By using hashing algorithms, it enables one to verify when and by whom an email was sent, whether and when it was received, and what its original content was. Seeing that this verification is performed by an independent third party (as an independent third party RPost stands between the sender and the addressee of an email), the RPost service can be qualified as a supplementary technique of proof that renders added value of proof to an email in comparison to an ordinary email.

In this respect one must however keep in mind that the authenticity of an email message can always be disputed before Court. When the authenticity or integrity of a Registered Email message is disputed, the Courts may possibly ask an RPost-service user to submit the RPost-service security measures and technical provisions to prove the authenticity or integrity of such message. In this respect, RPost sufficiently documents how the integrity of a Registered Email message record can actually be authenticated.

c. Legislative initiatives regarding registered electronic mail

As of 2001, Belgian law includes a particular act concerning “electronic signatures and certification services”.⁴ On 13 December 2010 the Belgian Parliament ratified an act that made a series of amendments to the AES and provided a legal context for registered electronic mail.⁵

Herein a registered electronic mail was defined as follows: *“any service of electronic data transfer that consists of guaranteeing, for a fixed rate, against risks of loss, theft or damage of the data, whereby the sender, where appropriate at his request, receives proof of the submission and/or of the order of the mail to the addressee”*.⁶ Moreover, it also listed a number of conditions with which suppliers of registered

² Articles 1315 *et seq.* of the Civil Code.

³ Ghent 10 March 2008, *Computerr.* 2008, issue 171, 303 *et seq.*, notes by P. Van Eecke and E. Verbrugge.

⁴ Act of 9 July 2001 on the establishment of certain rules regarding a legal framework for electronic signatures and certification services, *Belgian Official Gazette* of 29 September 2001, 33070 (referred to hereafter as the “AES”)

⁵ Act of 13 December 2010 in amendment of the Act of 21 March 1991 on the reform of some economic public companies, of the Act of 17 January 2003 on the status of the regulator of the Belgian post and telecommunication sectors and to amend the Act of 9 July 2001 on the establishment of certain rules regarding a legal framework for electronic signatures and certification services, *Belgian Official Gazette* 31 December 2010, 83279.

⁶ Article 39(4) of the Act of 13 December 2010

electronic mail must comply. A registered electronic mail that was alleged to meet these conditions was then equated to a registered mail.⁷

However, on 31 May 2011, one month before the Act was supposed to take effect, (the coming into force was scheduled for 30 June 2011), the respective provisions of this Act were abrogated with immediate effect. These provisions were withdrawn because the Belgian legislator first wanted to submit them to the European Commission in the light of Directive 98/34/EG of the European Parliament and of the Council of 22 June 1998 regarding an information procedure in the field of standards and technical regulations.⁸

No decisions may be taken on these provisions during such consultation of the European Commission. This so-called standstill period came to an end on 27 October 2011 and the following has been communicated by the Commission to the Belgian State regarding the white paper in the meantime: "*The bill contributes to the development of electronic legal correspondence. More specifically, the goal is to create a coherent legal framework for registered electronic mail. The starting premise for this bill is that the rules should be pragmatic in nature, easy to put into practice and do not introduce compulsory formalities or procedural requirements.*"⁹

This means that, in principle, the Belgian legislator may continue its legislative initiative. However, this has not yet happened to date but it is expected that, having regard to the attention that nevertheless is given to this subject, a new legislative initiative will indeed be taken in the (near) future.

Pending such new legislative initiative, we have verified the Registered Email service against the conditions that the Act of 13 December 2010 imposes on service providers of registered electronic mail.¹⁰ These conditions seem to be met *prima facie*, as a result of which the RPost service in the meantime seems to comply with the conditions which the legislator has initially foreseen within the framework of the registered electronic mail and which we expect to be introduced once again by the legislator.

Finally, it seems to us that in any event, as far as functioning is concerned, an RPost Registered Email message is equivalent to a registered post mail since the technology used by RPost envisages the same functional qualities as the procedural requirements set for such registered post mail¹¹, viz. (i) guaranteeing against risks of loss, theft or damage and (ii) generating a receipt for the sender as proof of the submission and/or of the order of the mail.¹² Even if the formerly abrogated law were not to be

⁷ Article 41 of the Act of 13 December 2010

⁸ See Bill of 16 March 2010 on miscellaneous provisions regarding telecommunication, Amendment No. 9 by Mr Van den Bergh, 1247/003.

⁹ See Communication from the Commission - SG(2011) D/51793 at http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&sNlang=EN&iyear=2011&inum=392&lang=E_N&iBack=4

¹⁰ For an overview of these terms and conditions, see Article 52 of the Act of 13 December 2012 (we enclose a copy of this as Appendix to this memorandum).

¹¹ The principle of the functional equivalence was set as prerequisite principle in the Law of 11 March 2003 on certain legal aspects of information society services, *Belgian Official Gazette* of 17 March 2003.

¹² See the definition of a "ordinary" registered mail under the Postal Act in point a.

revived (in the short term), this is a relevant argument to allocate added value of proof to RPost's Registered Email services as opposed to an ordinary email.

5. Qualification of the Digital Signature as "Electronic Signature" in the sense of Belgian law

The Act introducing the use of telecommunication tools and the electronic signature in the judicial and extra-judicial procedure gave a new meaning to the classic concept of a signature under Belgian law¹³. In accordance with this Act a totality of electronic data that can be attributed to a particular person and that shows that the integrity of the content of the documents secured¹⁴ can meet the requirement of a signature. Therefore, it is possible to have electronic alternatives for a handwritten signature, on condition that the *authenticity of the sender* and the *integrity of the content* of the document can be proved.

The legislator subsequently introduced an extensive and technologically neutral definition for an electronic signature under Belgian law: "*electronic data that are attached to or logically associated with other electronic data and which are used as a means of authentication*".¹⁵ A distinction is made here between the "ordinary" electronic signature, the "advanced" electronic signature and the "qualified" electronic signature. Only the qualified electronic signature is automatically equated to a written signature. To be regarded as qualified, a signature must be created on the basis of a qualified certificate. However, in practice, the use of the qualified electronic signature is not very broadly established in Belgium. The number of certification service providers offering qualified electronic signatures is therefore also very limited¹⁶.

As stated above, besides the qualified electronic signature, there are also other types of electronic signatures recognised by the AES, i.e. the ordinary and advanced electronic signatures. However, these types are *not* automatically equated to a handwritten signature.

An ordinary electronic signature consists of data in electronic form, attached to or logically associated with other electronic data, which are used as a means of authentication.¹⁷ Moreover, advanced electronic signatures must meet the following additional requirements: (i) it is uniquely linked to the signatory, (ii) it enables one to identify the signatory, (iii) it is formed by means which the signatory can keep exclusively under his control (iv) it is linked to the data to which it relates in such a manner that any subsequent change to the data can be traced.¹⁸

¹³ The Act of 20 October 2000 Introducing the Use of Telecommunication Tools and the Electronic Signature in the Judicial and Extra-Judicial Procedure, *Belgian Official Gazette* of 22 December 2000, 42698

¹⁴ Article 1322(2) of the Civil Code

¹⁵ Article 2(1) of the AES.

¹⁶ For a list of the accredited certification service providers, please see http://economie.fgov.be/nl/ondernemingen/informatiemaatschappij/veiligheid_informatie/elektronische_handtekening/

¹⁷ Article 2(1) of the AES.

¹⁸ Article 2(2) of the AES.

The signatory's identity can be traced through the RPost Digital Signature service because the signatory's IP address is added to the message. This means that conditions (i) and (ii) above have been met. As regards the integrity requirement, a judge will naturally be inclined to attach more credibility to an electronically signed message when the party involved was not able to still change the content thereof. This is also guaranteed with the RPost Digital Signature because a compressed version of the message is attached to the email as HTML file, which means that condition (iv) is also met. Finally, the receiver can keep exclusive control of his mailbox and therefore there is also compliance with condition (iii).

In our opinion, the Digital Seal, eSignOff and eContract services will therefore qualify as "advanced" electronic signatures in the sense of the AES. These three technologies do, after all, fulfil the functions of identification, irrefutability *and* integrity.

Even if an advanced signature is not automatically equated to a written signature, the judge will, in any event, not be allowed to refuse an email or document with an advanced electronic signature as evidence merely because of the fact that the signature was created electronically or is not based on a qualified certificate.¹⁹ However, a judge does still remain at liberty to refuse legal effect to an electronic signature if he is of the opinion that other criteria are not met.

¹⁹ Article 4(5) of the AES.

Chapter 5

IMPORTANCE OF SUPPLIER LEADERSHIP

When choosing a technology supplier, one should look to a company that can support a consultative process of determine the optimal services, settings and feature characteristics to fit your situations – the requirements of today and as they evolve.

This technology supplier should have track record and history in the marketplace of servicing large organizations.

It is also important to understand intellectual property ownership, which shows the ability to continuously innovate, within the organization; which should lead to more product opportunities over time.

RPost® is just that kind of technology supplier – a partner to optimize any service deployment. RPost has set global standard for email proof, message encryption and electronic signature services. RPost's Registered Email® services enable both sender and recipient to prove, sign, encrypt, archive and collaborate across desktop, mobile and online email platforms, with far less cost, time, paper and risk. RPost services are designed for industries where the speed of contract execution, encryption or court admissible email records may be a business critical requirement.

Recipient of the 2011 World Mail Award for Security, endorsed as the top pick by the 2011 JMBM Corporate Counsel Guide for Converting Contract and Legal Notices to Electronic Delivery and the 2011 Council of Insurance Agents & Brokers' Buyers Guide for Email Encryption, RPost services are in use in nearly every country in the world, by the U.S. Government through AT&T's GSA schedule, within Global F500 companies, and endorsed by some of the most influential American Bar Associations.

RPost, founded in 2000, has been granted 35 patents with worldwide coverage and operates in 8 languages. In some countries, such as Bermuda and Colombia, among others, the governments have made the RPost service a national mail product of the country offered by the government postal service. In other countries, such as with the India Supreme Court, the court systems are using the RPost services themselves.

For further details, visit the 15 minute recorded video interview located at www.rpost.com in the ABOUT >> [FROM THE CHAIRMAN](#) section. www.rpost.com



For further information on RPost's eContract™ Solution visit www.rpost.com or www.econtract.com
Call +1-866-468-3315 or +1-310-356-6536 or email info@rpost.com

Also visit: **www.rpost.com** to download a free trial.

This communication, published by RPost, is intended as general information only and may not be relied upon as legal advice, which can only be given by a lawyer based upon all the relevant facts and circumstances of a particular situation.

Copyright © RPost. All Rights Reserved