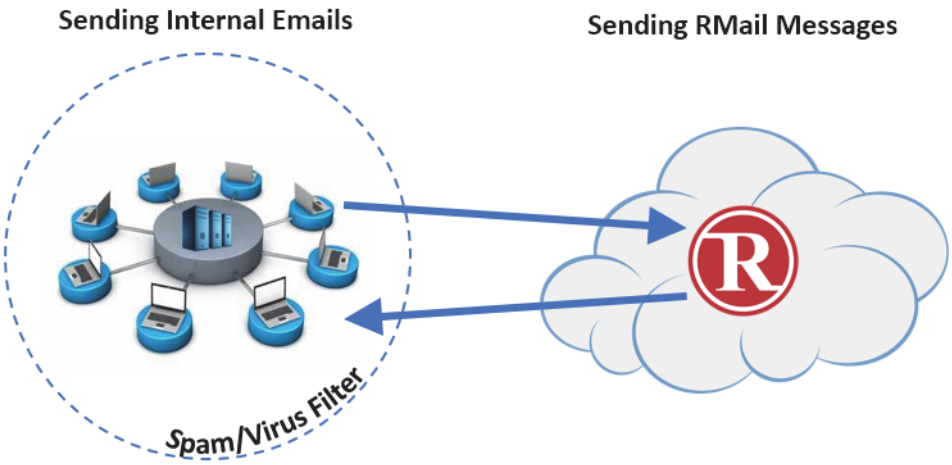
RMail Whitelist and Safe Sender Information

Thank you for your interest in the RPost Registered Email™ technology and RMail® services.

Emails sent using RMail services route through the RPost Cloud outside of your company's email network, for processing, delivery, and receipt generation. As such, the recipient's email system may properly identify a received RMail message as being from an external sender (the RPost Cloud).

If a sender and recipient share the same email server, this may confuse some recipient's email systems as these systems may see the "From" address as being from a sender within the recipient's same email domain while at the same time, it may see that the message came from an external server, the RPost Cloud server. Depending on the recipient email settings, this may cause the recipient's system to create a false alert.

RMail Message Pathway



If your mail system is providing false alerts such as "Unknown sender", or similar, when receiving RMail messages from people within the sender/receiver domain, you may choose to set the RMail system as a safe sender in your spam/virus filters.

Note: We always recommend that you whitelist the RPost sending and receiving domains and/or IP addresses.

Whitelist& SPF Information

If whitelisting is required, please have the network administrator set the following domains and/or IPs as safe senders ensure proper SPF sender authorization for RMail messages.

Domains:	**Inbound IPs from RMail to Recipient:** (Servers sending emails to Recipients)	**Outbound IPs from Customer to RPost** (if blocked) (Servers receiving mails from Customers)
r1.rpost.net	**52.58.131.9**	**52.28.241.216**
rpost.com	**52.58.136.115**	**52.29.244.65**
rpost.net	**52.29.207.240**	**52.29.207.240**
	52.28.232.174	**52.28.232.174**
	54.215.254.223	

SPF, DKIM & DMARC – Email Authentication

In addition to whitelisting, RPost recommends that customers implement the SPF and DKIM authentication mechanisms. These technologies utilize DNS TXT records to store their information. This information is used along with IP address and SMTP header information to establish authorization for the sender of the message.

In order to implement SPF & DKIM, the customer administrator must have access to a tool that can create and modify DNS records for the sender domain as well as the authorization to do so.

SPF – Sender Policy Framework

Typically, customer email sending domains will already have an SPF record configured. The SPF record provides authorization for a list of IP address and/or MX records to send on behalf of a domain.

SPF records can authorize the domain in the *envelope from* header (the Return-Path header) or the *message from* header (preferable). In order to utilize the *message from* header, customers must authorize RPost in their SPF record.

To authorize RPost as a sender the following text should be included in the sender SPF record.

include:*spf.rpost.net*

This is an example of an SPF record:

mydomain.com. IN TXT "v=spf1 include:spf.rpost.net ~all"

The following wizard can be used to create SPF records: https://www.spfwizard.net

This website provides a comprehensive source of SPF information: http://www.openspf.org

DKIM – Domain Keys Identified Mail

DKIM uses asymmetric encryption and hash algorithms to authenticate the message sender and validate the integrity of message content.

The authentication system verifies the validity of the message sender in the *message from* header.

To set up a DKIM record to authorize RPost as a sender, customers must contact RPost. RPost will configure the customer domain(s) on RPost sending servers send a unique public key to be included the customer DKIM DNS record.

This is an example of the setup instructions. Note: This is only an example, each domain must have a unique public/private key pair.

DKIM Setup Instructions

You need to add the following entry into your DNS server for **rmail._domainkey.mydomain.com**.

Selector Record

rmail._domainkey.mydomain.com IN TXT

"k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCsj5L2PNEDnUvqJjHfy69dFbrlZCXhSOvtA1K4HlS7IgVpR+JH8/xUPp
1Hmv2So6tSdmdlWdHDbJZzxtLdrHc7wkpcp4JWOu//BeeCzEOf+9n0DuV490qNDc2HXn4x9Mi4gqg5Wh7K7gTsK5rP+DitA
bKOI5TqwVIdHhPi6exu5wIDAQAB"
(The above is the BIND DNS server syntax, and other DNS servers may not require the ' to escape the ";".)

After setting up your DNS record, you can check the status of the **Selector** record at
http://www.dnswatch.info/dns/dnslookup?la=en&host=rmail._domainkey.mydomain.com&type=TXT&submit=Resolve