

Email Authentication: Actions you need to take today

By Leslie Price, Director of Deliverability Services

Executive Summary:

Since our initial whitepaper provided in September 2004, ISPs have continued to collaborate to identify and implement authentication methods. For an introduction to authentication methods, refer to our whitepaper dated September 9, 2004 that can be found at www.returnpath.biz. This updated brief provides brief descriptors of the systems in use, and action steps that every email sender should be taking.



Email Authentication: Actions you need to take today



Authentication Defined:

Authentication is a way for the receiver of an email (and the ISP) to authenticate the identity of the sender. If the identity of the sender can not be authenticated, then ISPs may reject the messages, or put the message through additional filters to determine if it should be delivered to the recipient. Without authentication, your chances of being filtered or blocked by ISPs that are authenticating senders are increased. ISPs are pursuing two primary methods of authentication: cryptographic based and IP based.

Crypto Based Authentication Methods Update:

Cryptographic methods use public key encryption techniques to “sign” each message in a way that is impossible to spoof and proves that the message came from the purported sending domain. Yahoo!’s Domain Keys is the method with the most traction. Currently:

- Yahoo! is signing and checking Yahoo! mail.
- Yahoo!, Earthlink, Gmail, and BT Internet are the largest ISPs that are in the process of implementing a cryptographic solution.
- While your email will not be rejected if it is not encrypted, you can get strong anti-spoofing benefits at the ISPs that are checking for domain keys. The benefits of protecting your reputation are further increased if your domain is widely spoofed.
- MTA vendors are incorporating domain keys signing and checking into their products.
- Senders interested in domain keys should talk to their MTA vendor about availability.

IP Based Authentication Methods Update:

Sender Policy Framework (SPF) and Sender ID are IP-based approaches and tie a purported responsible sending domain back to a set of IP addresses that are permitted to send mail for the domain. Both require publishing text records in the DNS (Domain Name Service) record for

every one of the sender’s domain(s). Messages from a “purported” domain are authenticated by comparing the IP address of the server that is actually sending the message to the list of IP addresses which are permitted to send for that domain.

Microsoft finalized the requirements for Sender ID in October of 2004. Essentially, SPF and Sender ID have “merged” and Sender ID is now compatible with SPF. Specifically:

- Sender ID requirements include checks for both SPF and Sender ID records.
- ISPs can now choose which identity they want to authenticate – the envelope “from” (authenticated by the SPF record) or the Purported Responsible Address (PRA), the email address of the sending entity as reflected in the message header (authenticated by the Sender ID record).
- If a sender has published SPF records, then the sender is also Sender ID compliant.
- In the absence of a Sender ID record, the sender’s SPF record is checked. Approval is contingent on approval of the SPF record.
- AOL has stated that they support Sender ID, but currently, this is accomplished by checking SPF records.

Impact on Marketers:

- AOL is no longer beta testing SPF. Requests to be added to the Dynamic Senders List require that the sender have a valid SPF record in place. Senders must have SPF in place when registering for this whitelist. The sender registers their domain(s), and the sender’s IP listings are based on the SPF record.
- Some smaller ISPs have begun rejecting mail based on SPF failures. The service provider, GoDaddy, rejects mail that is not SPF compliant. Spam Assassin 3.0 includes an SPF check that is configurable to reject mail if it is not SPF compliant.
- MSN and Hotmail plan to display a banner in any email that can not be authenticated. If the mail does not explicitly pass the Sender ID check, the banner clearly states that the source of the email can not be verified. This information may also be used as an input to the Smart Screen filtering process.

Action Steps: If you haven't done so already, publish an IP based record:

Requirements for both SPF and Sender ID have been finalized, and most major ISPs are testing the use of the records for authentication. ***If you haven't published your record, it should be a priority to do so.*** Return Path recommends the following process:

1. Perform an audit of all the domains AND sub-domains that you use

These should be "fully qualified" domains. Include domains for all types of mail that you send (marketing, sales, customer service, transactional and corporate mail to name a few) whether you send the mail using an Email Service Provider (ESP) or in-house. Each domain or sub-domain must be authenticated.

The audit should include:

- All "Header From" domains (the domains that show up in Outlook or AOL as the sending address)
- All Return-Path or other bounce domains that are in the header
- If you use the "Sender" header, a list of all sender headers
- Outbound server domains
- A listing of the sources that are permitted to mail from each of these domains
- Sources may include individual IP addresses, classes of IP addresses, and server names.

Determine if you need a Sender ID record in addition to your SPF record:

- If the list of your "Header From" domains is exactly the same as the list of your Return-Path/bounce domains, then you probably only need to publish an SPF record.
- If the list of your "Header From" domains is different from the list of your Return-Path/bounce domains, then you may need to publish a Sender ID record that provides the PRA record information for your authorized senders.
- If you send through an ESP or a third party, make sure you know what domains the mail from the third party uses in both the from and the bounce address. If either of those are domains under your control, you must authorize the third parties' use of your domain in your SPF/Sender ID record.

2. Work with your IT team to publish the appropriate record

The complete list of domains, sub-domains, and sources should be provided to your IT Department to publish the record.

There are several good wizards for building records including: <http://www.spf.pobox.com/wizard.html>.

Once the record is generated, it needs to be published. Generally, the individual in your IT group who control DNS records will publish the record.

3. Validate your SPF and/or Sender ID record

There are several validator software programs to ensure that the record you have published is valid including:
<http://www.dnsstuff.com/pages/spf.htm>
<http://spftools.infinitepenguins.net/check.php>

4. Check your log files for problems

Once published, check your SMTP log files for problems associated with an invalid record. You should see codes that indicate that the IP address you are mailing from can not be authenticated. Specifically, look for 500-level error codes for errors that might indicate a delivery issue associated with an authentication problem.

5. Maintain a valid record

Be prepared to update records as your environment or the authentication landscape changes. Changes to your system (i.e. new domains or IP addresses) may require changes or additions to your record.

Building on Authentication with Reputation:

The value of authentication programs is in its ability to identify and confirm the sender of the message. However, authentication does not ensure that the sender uses best practices for address collection, content, mail strategy, and bounce handling.

The next step in identifying and eliminating spam is to measure and report on a marketer's reputation. Measuring and reporting reputation will occur when the practices of authenticated senders are tracked, compiled, and provided to receivers (ISPs) who in turn determine if the marketer's record is sufficient to pass the mail to the recipient.

Achieving and maintaining a strong reputation means taking proactive steps to monitor deliverability, identify and correct root causes of failure, follow best practices and always respond to customer feedback.