



Sender ID Framework

Implementation Guide

What is Sender ID?

The Sender ID Framework is a type of email sender authentication. Sender authentication does not currently exist in today's standard SMTP logic for email—making it easy for spammers to disguise their identity and locale. Similar proposed sender authentication technologies include Sender Policy Framework (SPF), required of AOL's whitelist senders in August of '04, and Yahoo Domain Keys, still in testing by Yahoo.

Without sender authentication email users have seen huge increases in email domain spoofing (falsifying the "from" address/domain) and phishing (fraudulent spam that attempts to capture private information or credit card numbers).

Sender ID hopes to be the industry standard sender authentication scheme to counter e-mail domain spoofing and to provide greater protection against phishing schemes. This specification is the combined result of Microsoft's Caller ID for E-Mail proposal, Meng Wong's Sender Policy Framework (SPF), and a third specification called the Submitter Optimization. These three draft technical specifications were recently submitted to the Internet Engineering Task Force (IETF) and other industry organizations for review and comment.

Why is Sender ID a Good Thing?

1. It helps prevent domain forgery and Phishing. Phishing is the practice some spammers employ to trick email recipients into divulging personal information, such as credit card numbers or account passwords, by sending email pretending to be from a legitimate source, such as a user's bank, credit card company or online merchant. Sender ID doesn't explicitly prevent spam or phishing scams, but it does make them easier to detect because it provides a more reliable answer to the question: "Who sent the message?"

2. It is a critical first step to our fight against Spam, and reducing false positive filtering of legitimate email. Though not a silver bullet in itself, Sender ID at least adds protection against domain forgery which runs rampant in the spamming community. It paves the way for "Accreditation" and "Reputation" services (like Bonded Sender) to ultimately solve the spam problem. Sender ID merely says "who" sent the message, whereas accreditation and reputation say "who they are", "where they are", and "what their history as a sender is." This allows the email receiving community (ISP's, spam filtering companies, blacklists) to know more about a sender before making an inbox, bulk folder, or block decision.

3. Reputation will ultimately follow a brand, not just an IP. Of course it depends which color glasses you look at this issue through, but ultimately more accountability for the emails we all send will be a good thing. Following guidelines for permission name capture, best practices for content, frequency, and list hygiene is the best way to preserve that reputation.

How does Sender ID Work?

Email senders (like your company) publish an Email Policy Document (SPF record) in their Domain Naming System (DNS) record. This record allows a company to tell the world which IP addresses are allowed to send email for their domain. **In the case of an Email Service Provider (ESP) like ExactTarget, our clients also need to publish these records since we are transmitting your email from our IP address but under your domain name.** When receivers (ISP's, companies, etc.) receive the email, they'll check the Sender ID record to ensure that the domain in the email "from" address is valid for the IP address that sent the message.

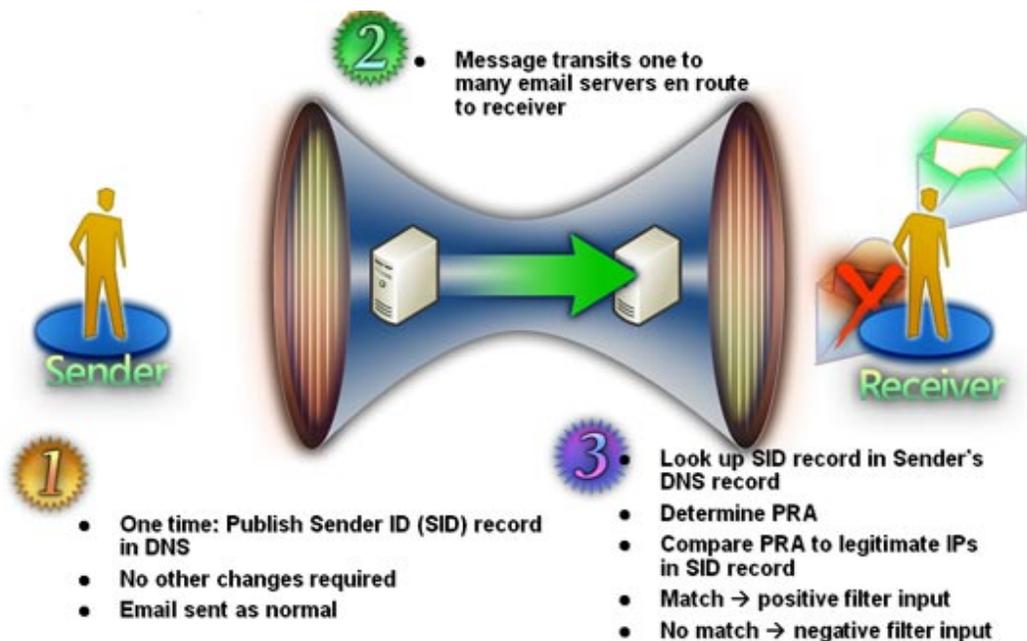
In the case of an ExactTarget client, like your organization, the Sender ID process will check your domain since it is in the "from address" of the email. The ISP will then check to see that your Sender ID records specify ExactTarget as a legitimate "outsourced domain." Once this check is passed, then a final check of our Sender ID records takes place to ensure the IP they received the email from has been authorized to send mail for exacttarget.com.

Steps:

1. Sender Publishes Sender ID records in DNS. Those having their mail sent by another domain must publish that company as an acceptable outsourced domain.
2. The email is sent and travels through the Internet.
3. Receiver (ISP) looks for Sender ID records for the Purported Responsible Address (PRA). The PRA is the domain in the "from" address that sent the email message. If the ISP's check records verify that the IP address from which the mail was received is part of the Sender ID record for the sender, then the message has "passed" the Sender ID check.

The diagram below should help explain the process.

Diagram 1: Sender ID Flow



How is SPF Different than Sender ID?

In June 2004 we publish Sender Policy Framework (SPF) records, which is a different sender authentication standard that was adopted by AOL, and enforced for all AOL whitelist partners (like ExactTarget) starting August '04. SPF and Sender ID are closely related. In fact they're based on the same concept of authenticating an IP address for a domain. However, whereas SPF merely authenticates the domain in the "return path" (bounce.exacttarget.com), found in our email headers, Sender ID also authenticates the "from" address that is visible to the user—your organization's "from address." In the case of Sender ID, the "from address" is referred to as the Purported Responsible Address (PRA), which is the email address that sent the email.

Examples of SPF and Sender ID checks are below.

Email Header Check with SPF:

ISP checks to see that the IP address in the header is authorized by the domain specified in the return path to send mail.

X-Apparently-To: chiphouse2000@yahoo.com via 66.218.78.147; Wed, 18 Aug 2004 08:33:22 -0700

X-Originating-IP: [207.67.38.85]

Return-Path: bounce-205875_html-736605137-463653@bounce.exacttarget.com

Received: from 207.67.38.45 (EHLO xtinmta026.exacttarget.com) (207.67.38.32) by mta113.mail.sc5.yahoo.com with SMTP; Wed, 18 Aug 2004 08:33:22 -0700

From: "Consolidated Widgets" <customercare@widgets.com>

To: chiphouse2000@yahoo.com

Subject: August Newsletter

Date: Wed, 18 Aug 2004 10:33:16 -0500

List-Unsubscribe: <mailto:leave-fcb01670706c03781a4c342838-fe29137373620478741777-fec410767662017e@leave.exacttarget.com>

Email Header Check with Sender ID:

ISP checks to ensure that IP address in header is authorized by "from" address to send email, and when return path is different than "from" address, the Sender ID records are checked for domain in the return path as well.

X-Apparently-To: chiphouse2000@yahoo.com via 66.218.78.147; Wed, 18 Aug 2004 08:33:22 -0700

X-Originating-IP: [207.67.38.85]

Return-Path: bounce-205875_html-736605137-463653@bounce.exacttarget.com

Received: from 207.67.38.45 (EHLO xtinmta026.exacttarget.com) (207.67.38.32) by mta113.mail.sc5.yahoo.com with SMTP; Wed, 18 Aug 2004 08:33:22 -0700

From: "Consolidated Widgets" <customercare@widgets.com>

To: chiphouse2000@yahoo.com

Subject: August Newsletter

Date: Wed, 18 Aug 2004 10:33:16 -0500

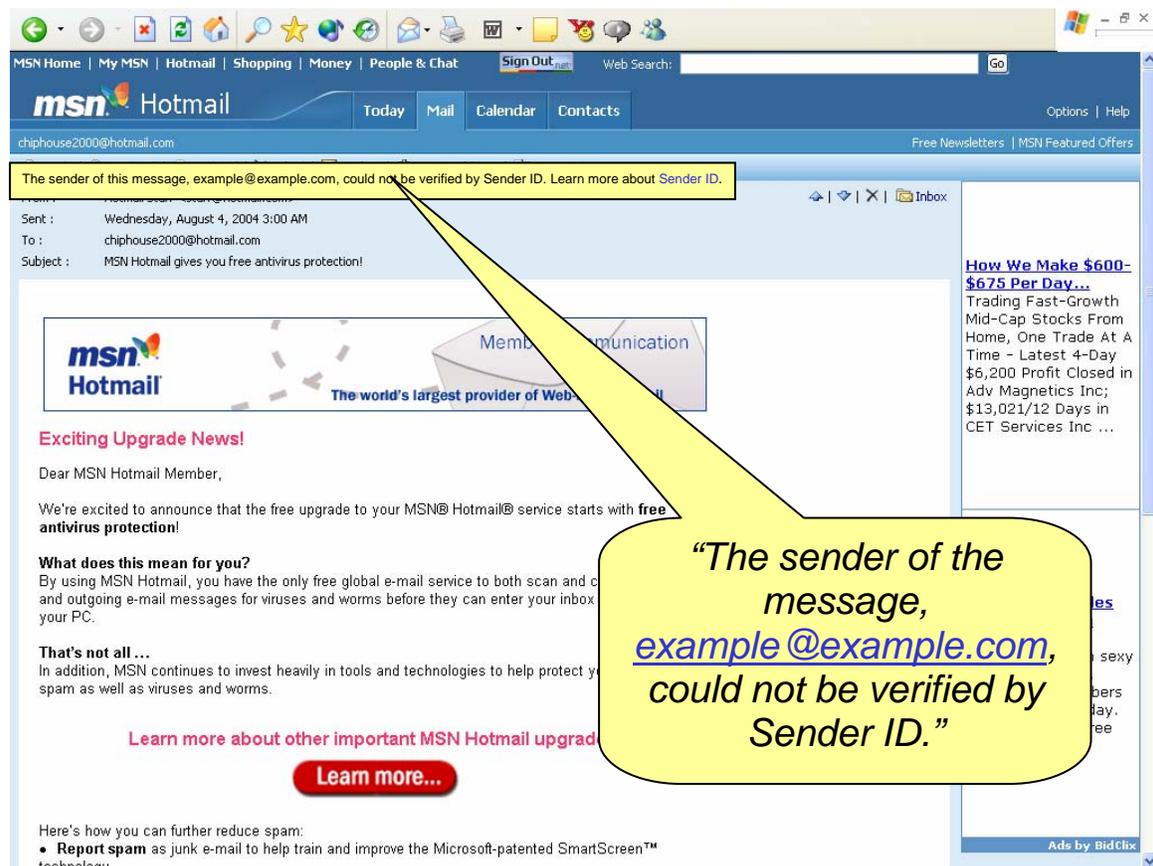
List-Unsubscribe: <mailto:leave-fcb01670706c03781a4c342838-fe29137373620478741777-fec410767662017e@leave.exacttarget.com>

What will Microsoft do with Sender ID Records?

Microsoft's goal is to begin checking Sender ID records for all inbound email to MSN and Hotmail by October of 2004. Initially they will not be blocking messages that don't have a Sender ID record, though they will eventually start filtering messages without Sender ID, thus increasing the chance the email is sent to the bulk folder rather than the inbox.

In the short-term, Hotmail will be merely labeling inbound email with a "pass" or "didn't pass" the Sender ID authentication process. Emails will be labeled in a yellow box at the top of the email. Email that doesn't pass Sender ID will be labeled with text saying, "*The sender of the message, example@example.com, could not be verified with Sender ID.*" See example below:

Example: Hotmail Screenshot of Sender ID in Action



Will other ISPs Check for Sender ID Records too?

This isn't an easy question, but the hopeful answer is "yes!" There may be a hold-up on this occurring quickly however due to Microsoft's pending patent on Sender ID, and the lack of support from AOL, the IETF and the open source community.

However, Microsoft hosted a conference in late August for all ISPs in the country who wanted to come and learn more about Sender ID and how to implement it. Hopefully it will gain some traction and get used broadly. Clearly one standard would be best for all of us.

Sender ID is still under review by the Internet Engineering Task Force (IETF) for consideration as an industry-wide standard for email authentication. We await more information on this, but we'll be moving forward with Sender ID, and if necessary, help you adopt an IETF standard later if need be.

Does your Organization have to do anything?

ExactTarget clients will need to publish Sender ID records. Online tools are already in place in a Beta format, courtesy of Microsoft at

<http://www.anti-spamtools.org/SenderIDEmailPolicyTool/Default.aspx>

This online tool allows organizations to key in their domain and the wizard will help them structure their Email Policy Document (SPF record). The organization can then cut and paste it into their DNS record.

DNS Records: Who owns them and how do they get changed?

The DNS records for your domain (e.g. - widgets.com) is typically managed by your technical staff (in-house) or with your ISP or hosting service. It is for this reason that you'll need to work with whoever hosts your DNS records to publish Sender ID records. ExactTarget has already published our records, but we need your organization to publish Sender ID records as well.

Resources like www.networksolutions.com, www.register.com, www.dnsstuff.com, www.tucows.com all allow you to research the "technical contact" for your domain(s). Do a "whois" search to identify this person. This is the person that will be able to publish your Sender ID record in the zone file for your domains that send email.

How does My Organization Create a Sender ID Record?

1. Find the correct technical contact at your organization by visiting www.networksolutions.com or similar site and searching the "whois" record for your domain.
2. Make sure this is the "Technical Contact" listed on your "Whois Record" for your domain
3. Work with your technical contact to establish all IP addresses and domains under which you send email.
4. Visit www.anti-spamtools.org to use the Sender ID Wizard and fill it out using the information you gathered on your IP addresses and domains. NOTE: This is still in beta due to the pending patent and IETF standards approval. However, we recommend you publish a record as soon as possible – you can modify it later if standards change.
5. Fill in "exacttarget.com" and "bounce.exacttarget.com" under the "outsourced domains" section of the wizard
6. Cut, paste and send your record to your Technical Contact to publish in your DNS record

What Does a Sender ID Record Look Like?

Here is a partial Sender ID record for the bounce.exacttarget.com. You can see it is still related to SPF; in fact the record is also called an SPF 2.0 record. This lists all of our IP addresses that are allowed to send mail for exacttarget.com

spf2.0/pr a ip4:207.67.38.0/24 ~all

Though the standards may change with IETF input, here is what a record one of our clients might look like when exacttarget.com and bounce.exacttarget.com are appropriately included as “outsourced domains” when the record is published.

spf2.0/pr a:64.15.205.132 include:exacttarget.com include:bounce.exacttarget.com ~all

In the example above, the IP address is a place holder for what your IP addresses may be for your company. The “include:exacttarget.com” statement says that you authorize ExactTarget to send email on behalf of your domain.

NOTE: You must customize the Sender ID record for your own domain. Do not cut and paste the example above in your DNS zone file. Use the tools on www.anti-spamtools.org to develop your own record.

Questions?

Have questions on implementing Sender ID at your organization? Contact us at privacy@exacttarget.com