



Implementing the Sender ID Framework in DNS

July 2005. Report #5020

Ferris Research Analyzer Information Service

For Free Distribution to Attendees at Email Authentication Implementation Summit 2005

Ferris Research, Inc.
408 Columbus Ave., Suite 1
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Recent Reports From Ferris Research

Introduction to Presence Models and Standards
Proofpoint's Content Security and Regulatory Compliance Offering
Using Content Security to Achieve Regulatory Compliance
Microsoft Operations Manager (MOM) 2005 and Exchange Server
2003 Management Pack for MOM
The Total Cost of Ownership of IBM Notes/Domino 6
Zero-Hour Anti-Virus Defense
New Features of IBM Lotus Notes/Domino 6
New Developments in Virus Control
Wikis
The Global Economic Impact of Spam, 2005
Calculating Spam Costs for Your Organization
Adomo Voice Messaging for Exchange: A Messaging-Centric
Approach to Voicemail
Key Trends in Messaging and Collaboration, 2005 – 2010
Email Archiving: In-House, Outsourced, or Hybrid?
Bulletin: Mail Anti-Abuse Working Group First General Meeting
Zero-Hour Anti-Virus Defense
Phishing: What to Tell End Users
Bulletin: Microsoft IT Forum, Copenhagen, Denmark
Microsoft's Lookout Search Tool
Bulletin: Exchange Best Practices Analyzer Tool
Zero-Hour Defense Against Email-Borne Viruses
Implementing the Sender ID Framework in DNS
Syndication for Information Consumption and Publication
Sarbanes-Oxley and the Messaging Manager
An Assessment of Windows Sharepoint Services
Ironport's Virus Outbreak Filters
Voltage's Encrypted Email
Gwaya and GroupWise Security
Email Records Management Survey: Guidelines, Technologies, and
Trends
Spam: Corporate Practices and Priorities in 2004
New Trends in Spam
The Impact of CAN-SPAM on Legitimate Direct Marketers
Upgrading from Exchange 5.5 to 2003: A Financial Case Study
Bonded Sender: A Program for Legitimate Mailers
Exchange Server Reliability
Spim: Spam Over Instant Messaging

Table of Contents

Implementing the Sender ID Framework in DNS.....	4
Executive Summary	4
Email Domain Authentication Summary	4
Why It's Important To Act Now.....	5
Adoption Challenges.....	5
Structure of Sender ID Records	6
Sender ID versus SPF.....	6
A Simple Sender ID Record.....	7
Scope	7
Prefixes.....	7
Example 1: Vanity Domain.....	8
Example 2: Vanity Domain With More Than One Provider	8
Example 3: Small Company.....	8
Example 4: Large Company.....	9
Example 5: ISP.....	10

For Free Distribution to Attendees at Email Authentication Implementation Summit 2005

Implementing the Sender ID Framework in DNS

Executive Summary

The Sender ID Framework is a DNS-based solution to help reduce spam and fraudulent email. Major ISPs, including Microsoft MSN, Hotmail, and America Online, have already begun incorporating SPF or Sender ID validation into spam filtering and the whitelist of registered senders.

If you own a domain and send email from it, it's important for you to configure domain authentication information now. This will allow recipients of your mail to verify the sender, even if you are not yet checking SPF or Sender ID records against your incoming mail.

This report explains what you need to know and do now, and provides a number of clear illustrative examples. Complex implementations, and implementations covering incoming mail, are beyond the scope of the document.

Key points are:

- SPF and Sender ID help prevent forged email and spam by verifying which IP addresses are allowed to send email for a domain.
- Major ISPs and large senders are announcing support.
- It's important to act now, so that your email isn't rejected by organizations deploying SPF and Sender ID, and to protect your domain name from unauthorized usage.
- Organizations that implement Sender ID checking should consult legal counsel to determine if the Microsoft intellectual property rights (IPR) license is appropriate for it.
- We show how to configure Domain Name System (DNS) entries so that receivers checking SPF and Sender ID won't reject your email.

Email Domain Authentication Summary

Email domain authentication techniques such as SPF and Sender ID were developed to prevent email address forgery commonly used in phishing, spam, and viruses. Domain owners must identify their sending mail servers in a new DNS format. Receivers verify the *Purported Responsible Address* (PRA), the SMTP MAIL FROM, the SMTP HELO domain, or all three against the information stored in DNS to reject unauthorized messages.

Sender ID is an evolution of the *Sender Permitted From* (now known as Sender Policy Framework, or SPF) proposal developed by Meng Weng Wong, Mark Lentczner, and others. Earlier this year, it was combined with the Caller ID proposal developed by Microsoft. Sender ID has broad industry support from ISPs, anti-spam vendors, mail server vendors, and legitimate direct marketers. On June 30, 2005, the Internet Engineering Steering Group approved both Sender ID and SPF as experimental standards.

In late June of 2005, Microsoft began marking messages that do not pass Sender ID checks with a warning stating that the sender of the message could not be verified. Microsoft has announced that before the end of 2005, messages that have no authentication will be more likely to be quarantined in the spam folder. In addition, AOL has begun using SPF to maintain its whitelist of reputable IP addresses.

Sender ID and SPF will help to stop fraudulent email, spam, and viruses. As adoption grows over the next 12 months, it will become increasingly difficult for non-authenticated email to be successfully delivered to the inbox.

Why It's Important To Act Now

Even though the standard is not finalized, major Mail Transport Agent (MTA) vendors are announcing plans to incorporate Sender ID checks into their next releases.

Senders should therefore begin publishing Sender ID and SPF records now so they are prepared and compatible with mail receivers that start verifying incoming mail. In the short term, not publishing information about your domain will increase the likelihood that your email will be flagged as spam. In the long term, it could result in some of your emails being rejected outright.

Anyone sending email outside their own corporate domain should publish Sender ID and SPF records in their DNS, and should educate their users to ensure that they are only using authorized IP addresses and MTAs to submit their email.

Adoption Challenges

There are still a few significant challenges to the adoption of Sender ID. Microsoft claims to have a patent application on portions of Sender ID. The firm is offering a royalty-free license to anyone who wants to use it, but the specific terms of the license may pose challenges for open-source developers, who usually need to sublicense or comply with open source licenses such as the GNU Public License (GPL) or the Apache License.

One solution for open-source developers may be to use the Sender ID framework without a license. Most commercial software developers will benefit from the terms of the license, although each company should consult legal counsel to determine its choice.

It is important to note that these license restrictions do not apply to domain owners publishing records in DNS. Only developers of mail receiving software that validates Sender ID records need be concerned with licensing.

Because both Sender ID and SPF have been accepted as experimental standards by the IESG, both are being checked by large ISPs, and the records are so similar, you should publish both SPF and Sender ID records until the future of email authentication becomes more clear.

Structure of Sender ID Records

Sender ID is a way of directly or indirectly encoding all of the IP addresses allowed to legitimately send or relay email for a domain into the DNS records for the domain. PRA is an algorithm for identifying the “purported responsible address” in the message. In simple cases this is the From address that users see when they read their email. It can also be the address of a forwarding server.

Sender ID information is published by a domain owner using special DNS records. In the future, this will use a new DNS record type called *SPF2*. However, this is not currently supported by most DNS servers, so in the meantime TXT records will also be accepted.

Sender ID versus SPF

Because Sender ID is an evolution of SPF, the records published by both are quite similar. In fact, the Sender ID specification says that if no Sender ID record is found, any SPF record found should be used to perform the Sender ID check. This means that you could just publish SPF records and expect to pass Sender ID checks, but you should generally publish both, to avoid problems with ISPs that use incorrect or out of date implementations. In most cases these records will be nearly identical.

The major difference between Sender ID and SPF is that SPF is only intended to validate the domain of the MAIL FROM address (also known as the Return-Path) and/or the HELO domain, which is usually not visible to the recipient, while Sender ID may also check the PRA, which is visible. For many senders, this will be the same, however some configurations (such as outsourced delivery) may use a different domain. In these cases, the SPF records and Sender ID records may specify different sets of IP addresses.

To distinguish a SPF record from a Sender ID record, you can look at the version identifier (described below). A Sender ID record will use “spf2.0”, while a SPF record uses “v=spf1”.

A Simple Sender ID Record

Figure 1 illustrates a simple Sender ID record, and its interpretation. A Sender ID record in DNS comprises a number of different components, some of which can appear more than once.

FIGURE 1 A SIMPLE SENDER ID RECORD

```
spf2.0/pra,mfrom +mx +a:mail.example.com +ip4:22.22.22.22 -all
```

Interpretation:

spf2.0/pra,mfrom	This is SPF version 2.0, and should be applied to both PRA and MAIL FROM. If this was “spf2.0/pra” the receiver should check only the PRA. A SPF “classic” record will have “v=spf1” as the version string, and is semantically equivalent to “spf2.0/mfrom.” Most organizations will likely publish both records with similar contents for compatibility with both AOL and Hotmail.
+mx	Any mail servers that appear in the MX records for the domain are allowed to send mail for the domain
+a:mail.example.com	Any IP addresses that are in A records for mail.example.com are allowed to send mail
+ip4:22.22.22.22	The IP address 22.22.22.22 is allowed to send mail. CIDR notation is also allowed for specifying ranges of IP addresses
-all	No other addresses are allowed to send mail for this domain

Sender ID records indicate IP addresses that are allowed to send email for a domain.

Scope

The string immediately after the version is the “scope” of the record. This can currently be either “pra,” signifying the PRA; “mfrom,” specifying the SMTP MAIL FROM parameter; or “pra,mfrom,” specifying that both should be checked. The mfrom scope is useful for preventing your domain from being used in the return path of spam or virus messages, and is helpful in preventing “backscatter” but does not protect any identity visible to the end user. The PRA scope protects the address visible to the end user, making it useful for preventing phishing and forgery.

Prefixes

There are four possible prefixes to put before each rule:

- “+”: This means “Pass.” If a Pass rule matches, the receiving server should mail from this server as authenticated. It still may be subject to further spam filtering.
- “-”: This means “Fail.” If a Fail rule matches, it means that the server is not supposed to send mail for this domain.

- “~”: This means “SoftFail.” If a SoftFail rule matches, the mail should not be rejected outright, but it should be subject to additional scrutiny.
- “?”: This means “Neutral.” Neutral rules mean that this mail should not be rejected, but it is not explicitly allowed to be sent from the source. This is usually used where people will be sending mail from many unknown locations or servers.

A missing prefix means the same as “+.”

One thing to note in these examples is the use of *-all*. Technically, if your records are correct and you do not send mail from anywhere else, this is the appropriate rule. However, in practice, for initial deployment it is recommended that *~all* or *?all* be used to avoid problems.

Another thing to note in these examples is that for most uses the published SPF and Sender ID records will be identical. However, in the case of an organization using an email service provider, the bounce address (checked by SPF) may be different than the PRA (checked by Sender ID), so the records could be slightly different. This is illustrated in Example 4.

Example 1: Vanity Domain

This is a simple case. The domain is used by a handful of people who always send email through their ISP’s mail server. When traveling they use Webmail, which also goes through the ISP. All of the ISP’s outgoing mail server addresses are defined by the ISP’s Sender ID information.

Simply delegate the Sender ID information to the ISP’s domain:

```
spf2.0/pr,from redirect=example-isp.net
v=spf1 redirect=example-isp.net
```

Example 2: Vanity Domain With More Than One Provider

This is very similar to the previous example, but since the domain has more than one ISP or mail provider, the record cannot be completely delegated to a single provider. In this case, the “include” mechanism can be used to include the records of both domains:

```
spf2.0/pr,from include:example-isp.net include:example-isp2.net
v=spf1 include:example-isp.net include:example-isp2.net
```

Example 3: Small Company

This is a little more complex, but still fairly simple. It’s similar to the vanity domain case, except that everyone uses the company email server. There are one or two other sources of email, such as a Web site notification (e.g., where someone does something at the company’s Web site that generates email), and an email list server.

The appropriate records are:

```
spf2.0/pr,a,mfrom +mx +a:www.example.com +a:lists.example.com -all
v=spf1 +mx +a:www.example.com +a:lists.example.com -all
```

where

- mail.example.com is the company's mail server, and the MX record for the domain.
- www.example.com is the Web site that notifications come from.
- lists.example.com is the email list server.

Example 4: Large Company

This is a still more complex case. There are several internal mail servers for different divisions, Web site notifications, two email service providers, plus a customer resource management (CRM) solution through salesforce.com.

Three divisions have their own incoming and outgoing mail servers, with unique DNS names for their addresses:

- Someone@div1.example.com sends and receives through div1.example.com.
- Someone@div2.example.com sends and receives through div2.example.com.
- Someone@div3.example.com sends and receives through div3.example.com.

Note that mail.example.com is the main company mail server, and also the MX record for the domain; and www.example.com is the Web site that notifications come from.

The IP range used by email service provider 1 goes from 1.1.1.8 to 1.1.1.15. This service provider handles all bounces from the messages sent by this domain. This means that the service provider needs to publish appropriate SPF records and there is no need to add the service provider's servers to this organization's SPF records.

The IP range used by email service provider 2 goes from 2.2.2.16 to 2.2.2.31.

The IP address used by the CRM solution is 3.3.3.3.

In this case, there will be multiple Sender ID records:

```
div1.example.com IN TXT "spf2.0/pr,a,mfrom +mx -all"
div1.example.com IN TXT "v=spf1 +mx -all"
div2.example.com IN TXT "spf2.0/pr,a,mfrom +mx -all"
div2.example.com IN TXT "v=spf1 +mx -all"
div3.example.com IN TXT "spf2.0/pr,a,mfrom +mx -all"
div3.example.com IN TXT "v=spf1 +mx -all"
example.com IN TXT "spf2.0/pr,a,mfrom +mx +a:www.example.com
+ip4:1.1.1.8/29 +ip4:2.2.2.16/28 +ip4:3.3.3.3 -all"
example.com IN TXT "v=spf1 +mx +a:www.example.com +ip4:2.2.2.16/28
+ip4:3.3.3.3 -all"
```

Example 5: ISP

Here, there are lots of mail servers, but only simple record formats are involved. The easiest course is to simply list the IP addresses individually or by range.

If the IP addresses are noncontiguous, list them separately, as in:

```
spf2.0/pramfrom +ip4:1.1.1.8+ip4:1.1.1.9 +ip4:1.1.2.8 +ip4:1.1.2.9 -all
v=spf1 +ip4:1.1.1.8+ip4:1.1.1.9 +ip4:1.1.2.8 +ip4:1.1.2.9 -all
```

If the IP addresses are all in a range, such as 1.1.1.8 to 1.1.1.15, then use a range, as in:

```
spf2.0/pramfrom +ip4:1.1.1.8/29 -all
v=spf1 +ip4:1.1.1.8/29 -all
```

If the outgoing mail servers are the same as the incoming ones, then you can simply use:

```
spf2.0/pramfrom +mx -all
v=spf1 +mx -all
```

Authors: Joshua Baer, Ian Ragsdale

Editors: David Ferris, Nick Shelness, Richi Jennings

For Free Distribution to Attendees at Email Authentication Implementation Summit 2005

For Free Distribution to Attendees at Email Authentication Implementation Summit 2005

Want Help Implementing Sender ID?

Let Ferris Research help you implement Sender ID in your organization. We provide several reports to help formulate your plans. Then we provide up to eight hours of phone- and email-based consulting over a 60-day period. This short project costs \$6,500; see www.ferris.com/static/services/IT_short_consulting.php.

To order, call +1 (415) 986-1414, or email sales@ferris.com.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide, with analysts located in North America, Europe, and Asia/Pacific.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

Free Messaging Newsletter

Ferris Research publishes a free daily newsletter. It provides comprehensive coverage of the the messaging and collaboration field, and is a great way to keep current. Topics include spam, email, email retention/archiving, mobile messaging devices, consumer messaging services, web conferencing, email encryption, email migrations & upgrades, regulations compliance, instant messaging, ISP messaging, and team workspaces.

The service is available daily, and as a full weekly digest. To register, go to http://www.ferris.com/forms/newsletter_signup.php. In addition to the daily or weekly news, you will also receive one or two emails every month, announcing new Ferris reports or conferences. To opt out and suppress further email from Ferris Research, you click on the opt-out button at the end of each news mailing.