

# Sender ID – Deployment Overview for E-Mail Senders

*Microsoft Corporation*

*Published July 12, 2004*

Unsolicited commercial e-mail, often called junk e-mail or "spam," is frequently sent using forged sender addresses. This type of forgery, known as "spoofing," is used to conceal the true identity of the sender.

Sender ID is a proposed mechanism for helping to detect spoofing. In so doing, Sender ID assists e-mail senders in protecting their domain names, their reputations and their brands, and it helps e-mail recipients to filter junk e-mail more accurately.

This deployment overview describes the steps that e-mail senders need to take to comply with the Sender ID specification. Note that Sender ID is currently a draft proposal and has been submitted for review to the Internet Engineering Task Force (IETF) and other industry organizations. The current proposed Sender ID specification may be found at [www.microsoft.com/senderid](http://www.microsoft.com/senderid). Precise details of the specification are subject to change. Therefore, this deployment guide paints only a general picture of the steps that senders will need to take. Once the specification becomes finalized, the detailed steps will be published.

Sender ID works in a three-step process.

1. E-mail senders, large or small, publish the Internet Protocol (IP) addresses of their outbound e-mail servers in the Domain Name System (DNS) in a format described in the Sender ID specification.
2. Receiving e-mail systems examine each message to determine the *purported responsible domain*, that is, the Internet address that purports to have sent the message.
3. Receiving e-mail systems query DNS for the list of outbound e-mail server IP addresses of the purported responsible domain. They then check whether the IP address from which the message was received is on that list. If no match is found, the message has most likely been spoofed.

To be compliant with Sender ID, e-mail senders need to do two things:

1. **Publish the IP addresses of their outbound e-mail servers in DNS.** This is an administrative step that should require no changes to an organization's e-mail or DNS software.

2. **Ensure their domain can be correctly identified as the purported responsible domain of each message they send.** This means the sender's domain must be shown in certain headers of the e-mail message. Sender ID has been carefully designed to ensure that the overwhelming majority of legitimate e-mailers, remailers and mailing list operators already satisfy this requirement. In a few cases, such as mail forwarding services, additional headers may need to be added to e-mail messages.

## **Publish Outbound E-mail Server IP Addresses in DNS**

Outbound E-mail server IP addresses are published in DNS in an *e-mail policy document* whose format is described in the Sender ID specification. E-mail policy documents are published in "text" or TXT records in DNS. Even if a domain has no outbound e-mail servers, you can still help protect that domain name from spoofing by publishing an e-mail policy document. Follow the steps below to create and publish an e-mail policy document for each domain name your organization owns.

1. [Determine the IP addresses of the outbound e-mail servers for the domain](#)
2. [Create the e-mail policy document](#)
3. [Publish the e-mail policy document in DNS](#)

### ***1. Determine the IP addresses of outbound e-mail servers***

Identify the e-mail servers that transmit outbound e-mail and their IP addresses for all the domains and subdomains in your organization. You will need to publish an e-mail policy document for each of them.

If your organization uses any third parties to send e-mail on its behalf, such as an e-mail service provider or a hoster, you will need to know their domain names. You do not need the IP addresses of their outbound e-mail servers. (You might also advise them to publish e-mail policy documents for their own domains.)

### ***2. Create the e-mail policy document***

Create an e-mail policy document for each domain and subdomain that sends mail from your organization. It is also possible for several domains to share the same e-mail policy document.

Please refer to the Sender ID specification for details on the format of the e-mail policy document.

### ***3. Publish the e-mail policy document***

As described at the beginning of this guide, a domain's e-mail policy document is published in a DNS text record. To ensure the e-mail policy document TXT records do not get mixed up with other TXT records a domain may publish, Sender ID uses a special sub-domain named "\_ep" to hold them. If your organization's domain was example.com, you would publish the necessary TXT records under the domain \_ep.example.com

Once you have created the e-mail policy documents for your organization, you need to publish them in DNS TXT records. You may need the help of a DNS administrator to do this.

For each e-mail policy document, create an `_ep` subdomain of the appropriate domain name. Copy the e-mail policy document into a TXT record in the `_ep` sub-domain using your customary DNS administration tools.

## **Ensure the Correct Purported Responsible Domain**

As stated earlier, receiving e-mail systems examine each message to determine the *purported responsible domain*, that is, the Internet domain that purports to have sent the message. Therefore, e-mail senders must ensure that *their* domain is the one that is identified as the purported responsible domain.

The Sender ID specification describes in detail how the purported responsible domain is determined. In summary, receiving systems examine the RFC 2822 headers of each e-mail message in a particular sequence. The following sections outline a number of different scenarios or use cases for sending e-mail and describe which headers will be used to determine the purported responsible domain in each.

### ***1. Ordinary Interpersonal E-mail***

Ordinary e-mail sent from a user in one domain to a recipient in another is typically injected into the Internet mail system by servers belonging to the sending domain. The “From” header of the message will be used by receiving systems to identify the purported responsible domain.

So long as sending servers use their own domain name in the “From” header of the message, they are already compliant with Sender ID. They should, of course, publish their e-mail policy document in DNS.

### ***2. Mailing Lists***

Mailing list servers receive a message from the original sender and then re-send that message to all the members of the intended mailing list. In so doing, the mailing list server itself becomes the new sender of the message. Sender ID will validate that the message originates from an e-mail server under the control of the mailing list service. In other words, the purported responsible domain of the message is the domain of the mailing list service.

Therefore, a mailing list server must add an appropriate header to each message that contains an email address that it is authorized to use. Most of today's mailing list software already adds an appropriate header, usually “Sender”, which identifies the owner of the mailing list. This software is already compliant with Sender ID.

Sender ID encourages the use of the “Resent-From” header for this purpose. The Sender header is also acceptable.

### **3. Mail Forwarding**

E-mail forwarding services receive mail sent to one address and automatically forward it to a second address. Quite often, forwarding is done by retransmitting messages *verbatim*, preserving exactly both the original SMTP-level envelope information as well as the entire original message body. Unfortunately, this means that the forwarding service is itself never identified as the re-sender of the message. As a result, a message sent via a forwarding service cannot be distinguished from forged mail.

Therefore, Sender ID requires that e-mail forwarding services must add an appropriate header that contains an email address that it is authorized to use. Sender ID recommends the use of the “Resent-From” header for this purpose.

Many of today's forwarders already add a non-standard header to messages such as “Delivered-To”, “X-Envelope-To” or “Envelope-To”. These too are acceptable under Sender ID and forwarding services that add these headers are considered compliant.

### **4. Mobile Users and Third Party Mailers**

It is increasingly common for users to send e-mail from a wide variety of devices including laptop computers and mail-enabled phones or PDAs. Often these devices are connected to the Internet via a third party network carrier or Internet Service Provider (ISP). Although users typically have accounts on these third party networks, they often want mail sent over them to appear to originate from their regular corporate or personal e-mail account. However, since the message is injected into the Internet mail system by the third party network the purported responsible domain of the message is actually the domain of the third party network.

Therefore, Sender ID requires that e-mail services that send mail on behalf of another user in this way must add an appropriate header that contains an email address that it is authorized to use. Typically this address will be the user's address on the third-party network. Such programs should use the “Sender” header for this purpose.

This also applies to other third party mailing services such as Web applications like electronic greeting card and invitation services, "e-mail this article to a friend" services, and the like, that send mail on behalf of their users.

Third party mailers that add a “Sender” header to message today are already compliant with Sender ID.

## 5. *Guest E-mail Services*

Another common scenario involves users who send e-mail over networks where they have only temporary or guest access and no permanent account. For example, hotels commonly offer Internet access to their guests. Guests use their regular corporate or personal e-mail addresses to send mail, but messages are routed through the hotel's e-mail servers.

As in the third party mailer scenario above, Sender ID requires these third party e-mail servers to add an appropriate header that contains an email address they are authorized to use. Sender ID recommends the "Resent-From" header in this case. Since the user does not have an account on the third party network, a generic service address may be used.

## **An Optimization**

In order to determine the purported responsible address of a message, the receiving server must examine the headers in the message body. In other words, the message must first be transmitted to the receiving server before the purported responsible address can be identified.

To enable receiving servers to identify the purported responsible address *before* the message is transmitted, an extension to the SMTP protocol, called "Responsible Submitter", has been proposed. Using this extension, sending e-mail servers would determine the purported responsible address of their own messages and include this address on a new "SUBBITTER" parameter added to the "SMTP MAIL" command.

When the "SUBMITTER" parameter is present, receiving e-mail systems can validate the purported responsible address of the message before the message body is transmitted.

MTA software will need to be upgraded in order to support this proposed extension.

---

Please refer to the proposed Sender ID specification on [www.microsoft.com/senderid](http://www.microsoft.com/senderid) for complete details. For updates on Microsoft's efforts to counter e-mail spam, spoofing and phishing, please visit [www.microsoft.com/spam](http://www.microsoft.com/spam). Pending customer feedback on the draft specification, Microsoft will release Sender ID implementation guides, tools and an online policy generator.