

## Sender ID – Executive Overview

*Microsoft Corporation*

*Published July 12, 2004*

Unsolicited commercial e-mail, commonly called junk e-mail, or “spam”, was once considered a mere nuisance. Today it threatens to overwhelm Internet e-mail. To control junk e-mail – to identify it and filter it – a variety of approaches have been developed. Though different on the surface, these approaches share some common characteristics. They all involve asking certain questions about each e-mail message. In turn, they all use the answers to help classify messages as legitimate or junk.

One of the most important questions asked by junk e-mail filters is simply, “Who sent the message?” Once the filters know with certainty whether a message has come from the source it claims to, they can ask follow-up questions like:

“Do we know this person?”

“Do they have a history of sending legitimate e-mail or junk e-mail?”

“Do we trust them?”

It turns out that answering this one simple question, “Who sent the message,” *with certainty*, is virtually impossible today. That’s because e-mail is typically sent over the Internet without any authentication of the sender or the computers acting on their behalf. In other words, no verification is done to ensure that e-mail which purports to be sent from, say, someone@example.com actually originates from computers under the control of the example.com organization. It is absurdly easy for anyone to send e-mail and pretend to be someone else in doing so. This is a form of forgery often called “spoofing”. There is no automated way to detect spoofing today. Needless to say, spammers routinely exploit this fact.

Consequently, filtering junk e-mail can be an error-prone activity. Junk e-mail that appears to originate from legitimate senders slips through filters. Worse yet, these spoofed emails can be used for fraud and phishing scams, tricking recipients into divulging personal information by sending mail pretending to be from a legitimate source, such as their bank, credit card company or online web merchant. In addition, e-mail from legitimate senders is often blocked because their Internet addresses have been spoofed and their reputations tarnished.

Sender ID is a proposed mechanism for answering an important part of the “Who sent the message?” question, namely, “Which Internet domain sent the message?” Sender ID is the result of a merger of two similar proposals: Sender Policy Framework (SPF) written by Meng Weng Wong and Mark Lentzner, and Caller ID for E-mail written by Microsoft.

Sender ID works in a simple 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 domain 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.

Sender ID has been designed to meet the following requirements.

1. **Ease of adoption.** A key goal of this proposal is rapid and broad adoption. We hope that all Internet domains will quickly publish their outbound e-mail server IP addresses. Therefore, it is a requirement that any technical implementation operate within the capabilities of existing software wherever possible. Clearly, it will not be possible to implement this proposal without changes to some software. However, the proposal has been designed to keep such changes to a minimum in order to speed adoption.
2. **Scalability.** Any implementation must scale up to meet the needs of the largest ISPs and down to the smallest office or home mail server. Specifically, it must support organizations that have hundreds or even thousands of e-mail servers as well as those that have just one. It must also support those who outsource their e-mail servers to another organization.
3. **Fairness.** Any implementation must fairly distribute the costs of compliance. Today, the costs of detecting and remedying spoofing are borne entirely by the receiving organization. Any technical implementation must rectify this imbalance. Organizations that wish to protect their domain names from spoofing should bear part of the cost burden. Organizations that wish to accurately determine whether or not messages they receive have been spoofed should also bear a corresponding cost.
4. **Openness:** The technical implementation must be openly published so that any organization wishing to comply with its provisions may do so.
5. **Extensibility:** The technical implementation must allow for the publication of new or additional information about an organization's e-mail policies and practices should this be required in the future.

Sender ID does not prevent junk e-mail from being *sent*. However, it does make junk e-mail much easier to *detect*. It provides a more reliable answer to the question “Who sent the message?” Sender ID helps e-mail senders to protect their domain names, their reputations and their brands. Sender ID assists e-mail recipients in filtering junk e-mail more accurately and can help prevent the use of spoofing to perpetuate phishing scams. Finally, Sender ID provides a basis for additional filtering decisions based on the reputation and e-mail behavior of the sender. Taken together, we believe these measures will help to dramatically reduce the amount of junk e-mail delivered to users' mailboxes and will assist in better protecting users' overall online experience.

---

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.