Inbound Authentication—Applying Reputation Data

Inbound authentication and identity verification provides an added level of spam and phishing detection and is the first step in combating spam. The second step is applying reputation data, including the sender's past behavior, such as user generated spam complaints and compliance data. Reputation is usually generated from user based feedback, community-based reputation systems, and third-party data sources.

By including the Sender ID result in existing anti-spam solutions and applying domain and IP reputation, receiving networks can realize an increased level of spam and phishing detection. Benefits include an improved decision on the trustworthiness of e-mail including reducing the risk of malicious and zero-day exploits that target employee and corporate data.

Worldwide Adoption and Industry Solutions

Today more than seven million domains have published SPF records and more than 500 million users worldwide are protected by SIDF. Providing ease of integration within leading e-mail environments, over a dozen vendors and open source solutions, including Sendmail and Postfix, offer Sender ID support. This industry adoption is significantly increasing the accuracy of spam detection, enhancing the integrity, safety and confidence in e-mail.

alt-n technologies
BARRACUDA NETWORKS
CLOUDMARK
ICONIX
IRONPORT SYSTEMS
message systems
Microsoft Exchange Server 2007
mxlogic
port25 solutions, inc.
SECURE COMPUTING
SENDMAIL
SONICWALL
StrongMail
symantec
TUMBLEWEED COMMUNICATIONS

For more information on SIDF resources, and third-party solutions, visit **www.microsoft.com/senderid** or **www.aotalliance.org.**

For information on Microsoft's commitment to online safety, including industry collaboration, enforcement, education, and technologies, visit **www.microsoft.com/safety.**

© 2007 Microsoft Corporation. All rights reserved.
This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.
Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.
All other trademarks are property of their respective owners.
0107 Part No. 098-104800

Microsoft

Sender ID Framework

Restoring Trust and Confidence in E-mail

Identify Spam, Phishing, and Zero-Day Exploits

SIDF

www.microsoft.com/senderid

The Business Value of Sender ID

E-mail is a vital element in today's business infrastructure, enhancing communications, e-commerce, and online banking. Unfortunately, spammers exploit e-mail, creating security, privacy, and personal identity risks while threatening the brands of businesses worldwide.

To address this critical security issue, Microsoft has collaborated with other industry leaders, Internet service providers (ISPs), and organizations worldwide to develop the Sender ID Framework (SIDF), a leading e-mail authentication solution that helps identify and block forged and deceptive e-mail.

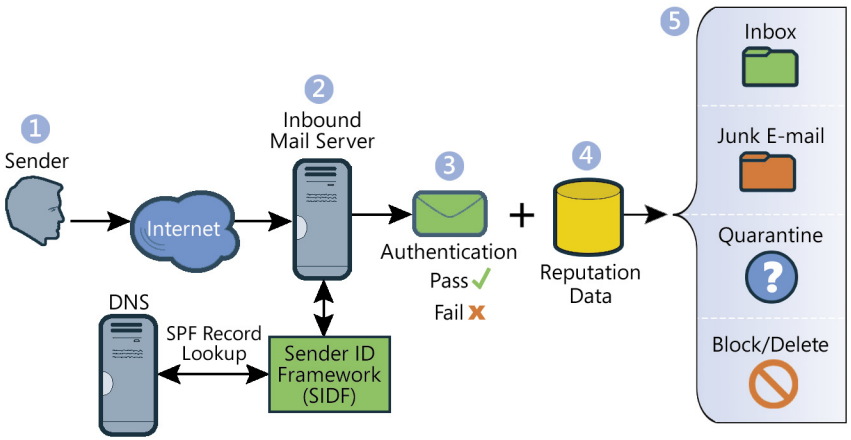
Easy to Implement and Manage—At No Cost

SIDF combines the Sender Policy Framework (SPF) and Microsoft Caller ID for E-Mail in an integrated, no-cost authentication solution that is easy to deploy and maintain and does not require any third party software licenses. Approved by the Internet Engineering Task Force (IETF) as an experimental Request for Comment (RFC), organizations can be assured of compatibility and reliability.

How Sender ID Works

As illustrated below, the Sender ID Framework validates the sender's identity, helping to detect and reduce exploits before they reach the user's Inbox. Transparent to the sender and receiver, SIDF verifies that each message is sent from an authorized source. No additional client software is required, allowing users to send and receive e-mail as usual.

1. The sender sends an e-mail message.
2. The recipient's inbound e-mail server receives the message.
3. The inbound e-mail server checks which domain claims to have sent the message and checks the DNS for the SPF record of that domain. The inbound server then determines if the IP address of the sending e-mail server matches the IP addresses that are published in the SPF record. E-mail messages that fail may be deleted, blocked, or sent to the Junk e-mail folder.
4. As a recommended option, the Sender ID result can be combined with reputation data about the IP/domain holder. This reputation data enhances delivery decisions for all e-mail, including messages sent from both legitimate senders and spammers which may pass the Sender ID check.
5. When combined with the receiving network's anti-spam and anti-phishing technologies, the e-mail may be delivered to the Inbox, the Junk or Quarantine folders, or may be blocked and deleted.



Business Value of Sender ID Authentication

- Improves the deliverability of legitimate e-mail
- Protects your brand's reputation
- Decreases customer exposure to phishing
- Increases your ability to block deceptive e-mail and malicious threats
- Reduces false positives while improving spam catch rates

Outbound Authentication—Creating an SPF Record

The first step is to create an SPF record which lists the IP addresses of all outbound e-mail servers. If your business relies on third-party e-mail support, and merchant services, their IP addresses should be referenced in your SPF record. This can be accomplished in one of two ways: by explicitly listing third-party IP addresses in your SPF record, or by pointing to third party SPF records from within your own record.

You can manually create a record using the published RFC syntax, or you may use one of several tools to automate this process, such as the Microsoft Sender ID SPF Record Wizard. This intuitive tool helps to identify your domain's Mail Exchanger (MX) and A records, adds third-party IP addresses, and provides instructions for receiving networks to apply to the SIDF check result for your domain. For more information, visit www.microsoft.com/senderid/wizard.

Once you have created and saved your SPF record as a text file, your DNS administrator can easily publish the record in the zone file for your domain's DNS—all without any disruption in service, performance or impact to your e-mail architecture or client software.

SIDF