



Email Authentication Technologies

Forging of another person's or company's email address or identity to get users to trust and open a deceptive spam message is one of the biggest challenges facing both the Internet community and anti-spam technologists today. These fraudulent tactics are growing problems, both for consumers who are victims, and for brands misrepresented.

Without sender authentication, verification, and accountability, email providers and ISP's can never know for certain if a message is legitimate or forged and will have to continually make educated guesses on behalf of their users on what to deliver, what to block, and what to quarantine.

Every email includes several separate pieces of data that attempt to establish the "identity" of the sender. Each one of these can potentially be forged. This document discusses the current forge prevention approaches, and e-Dialog recommendations, for two of those identifiers: the visible HEADER FROM address or the PRA (the Purported Responsible Address) and the ENVELOPE FROM address.

- **Spoofting:** Email spoofing happens when a message has a HEADER FROM that isn't really from that identity. Some virus programs do this when they send messages that contain recipients that are in your address book. Some messages will look like they are from you; others will look like they are from your friends. Spam also forges the HEADER FROM. It is never really from who it says it is.
- **Phishing:** Phishing is email that looks like a real message coming from a legitimate identity. It is a cleverly crafted message designed to extract personal information as well as account information. Phishing involves outright fraud.
- **Joe Jobbing:** 'Joe jobbing' forges the ENVELOPE FROM. This FROM is where bounces go to. Spammers and viruses set this to an innocent party's email address. The end result is that bounces end up going to this email address. The targets of 'joe jobbing' end up getting bounces for email they never sent in the first place.

E-Dialog recommends that each client use their own brand identity for each of these addresses. It usually looks like <brand>@email.customer.com. With email, it is rather easy for someone else to assume this identity and send email claiming to be from your brand.

Authentication Standards Overview

- **SPF Classic:** SPF Classic attempts to protect the ENVELOPE FROM. For our production email e-Dialog sets the ENVELOPE FROM to a domain which e-Dialog controls. This address is not normally visible to a user. It is the address that receives bounces. For SPF Classic to be effective it requires action from both senders and receivers. Senders (like e-Dialog) publish authorization records in DNS. Receivers check these records upon reception. SPF Classic can stop forged ENVELOPE FROM messages at delivery time. This means a forged message can be prevented from being sent before it leaves a sending system.

SPF Classic has a drawback. It breaks down when systems forward messages. For example, MIT has alumni accounts. These accounts can forward messages to another email address automatically. Depending on how the forwarding is done, if the receiving system does an SPF Classic check, the forwarded message may be rejected.

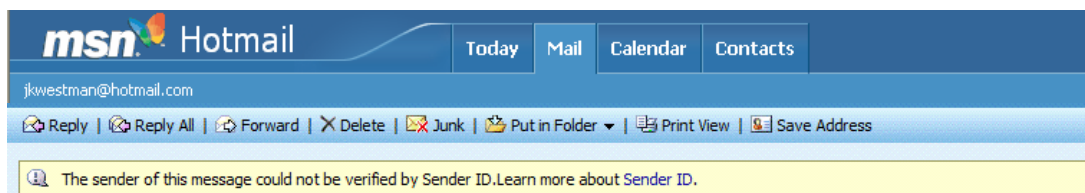


SPF Classic is supported by many ISPs, such as AOL, Yahoo and Google. These ISPs don't actually reject forged messages - they currently use it simply to help determine and report the "spamminess" of each message.

- **Sender ID:** Sender ID was proposed by Microsoft and Meng Wong. It is a combination of SPF Classic and the technology known as Caller-ID. Its primary focus is to protect the FROM HEADER however it can also protect the ENVELOPE FROM. The latter check is called MFROM. Sender ID can either use the same records as SPF Classic in DNS or a newly created record just for Sender ID. In this way Sender ID was made backwards compatible with SPF Classic in the hopes that it will be quickly adopted.

Sender ID for the most part, fixes the forwarding problem with SPF Classic. However the presentation of the message may look different than those messages that were not forwarded. The forwarding fix can actually make Phishing easier. Further details about this issue can be requested.

Sender ID checking is now being done by Hotmail/MSN. It will soon be incorporated into Outlook. Ultimately, e-mails in which the sender cannot be verified will be sent to customers' junk e-mail boxes. During the initial implementation of this Microsoft plans to place a yellow alert line to the recipient for any e-mail that does not pass the Sender ID check. For now, the recipient will still see the messages in their in-box from unauthenticated senders. Actual junk box filtering or blocking is not scheduled to take effect until fall 2005. This date however, is not yet confirmed.



Sender ID allows the receiver to choose DNS information from **either** of two sources; the PRA (the visible HEADER FROM), or the ENVELOPE (bounce) FROM address. Microsoft's program however, **only checks the visible PRA FROM** e-mail address not the real reply/bounce address from e-Dialog. Adjustments to your DNS must be made to be compliant with Microsoft. Instructions for this are detailed below.

The point of Sender ID is to check official DNS records (the records of who owns a URL) to make sure that the e-mail sender, based on the @ e-mail address in the visible FROM line, is who they say they are. Whatever you choose to display as the visible FROM, it has to be one your brand actually owns and has to be updated properly.

- **Domain Keys/IIM (DKIM):** Yahoo Domain Keys protects both the FROM HEADER, and the contents of the message itself. It does this by using digital signatures and keys being placed in DNS. Most messages that fail this check can be safely rejected. Computationally Yahoo Domain Keys is the most expensive. Further, Domain Keys is not immune from Phishing, because the forger can digitally sign a message. Currently, very few receivers (Gmail and Yahoo) do Domain Keys checking. The Domain Keys scheme has recently been combined with another similar scheme called Identified Internet Mail (IIM) developed by Cisco.



What Is Required From Our Clients

The following section details what actions need to be taken for a client's email messages to support each authentication scheme.

- **SPF Classic:** To support SPF Classic, no action is required from our clients. e-Dialog currently publishes SPF records for all clients. If you wish e-Dialog not to publish SPF Classic records in order to allow your messages to be forwarded by some forwarding systems, please let us know.
- **Sender ID:** e-Dialog has been publishing ENVELOPE FROM records for Sender ID because they are both SPF and Sender ID compliant. Since Microsoft has decided that it is only checking PRA FROM information changes will be need to be made to your DNS records.

To support Sender ID, entries must be added to your DNS. There is a [wizard](#) to help you though this process. If other ESP's besides e-Dialog are sending mail on your behalf, it may be difficult to specify exactly what should be in your DNS record. There is a section on that web site that mentions this.

- **Domain Keys/IIM (DKIM):** Supporting Domain Keys [requires the generation of public and private key pairs](#). If needed, e-Dialog can generate a key pair for you. Once the public key is in DNS (for the domain that is used in the FROM HEADER), all outgoing email can be signed by the private key.

Note that the Domain Keys scheme has recently been combined with another similar scheme called Identified Internet Mail (IIM) developed by Cisco, and a spec for the new combined scheme is being developed. e-Dialog will fully support DKIM once the specification has been finalized.

Conclusion

e-Dialog has been reviewing this and other authentication and reputation proposals and is making preparations to implement the appropriate technologies to deliver our client's mail. Since a clear winner(s) is not yet evident and each proposal has advantages and disadvantages, we will continue to test the impact of implementation of each proposal.

While these proposals are thought to be the first step to solving the spam problem, they offer more immediate relief to issues like spoofing and phishing. Authentications systems won't stop spam in and of themselves, but they will make it possible for reputation systems and blacklists and white lists, to be more effective.

The current state of affairs is that there is no single standard for senders and receivers to use universally as a means for identifying authentic e-mail. Until this problem is solved we will be faced with the difficult challenge of deciding which e-mail is authentic and, if and where it should be delivered.