The What, Why, and How of Email Authentication
by Ellen Siegel: Director of Technology and Standards, Constant Contact

There has been much discussion lately in the media, in blogs, and at trade conferences about the importance of email authentication. This article attempts to separate fact from fiction by covering what email authentication is, why it's important, and what you need to do to authenticate your email. It also looks under the covers to provide some understanding of how email authentication works.
1. Email Authentication in a Nutshell

In a nutshell, email authentication allows an organization that sends an email to take responsibility for it in a way that can be validated by the recipient. In other words, authentication associates a clear sender identity with a message and then enables a recipient to validate that the sender with that identity is in fact authorized to send the message. Note that the responsible (authenticated) sender may not always be the author of the email; sometimes it may be an Email Service Provider or a forwarding entity responsible for the transmission of the message.

This ability to perform identity validation wouldn’t be such an issue if email were secure, but unfortunately email was not designed with security in mind. The technology that supports email was developed back before the evolution of the World Wide Web, back when the network was a fairly closed circle composed of the Department of Defense and a handful of major U.S. universities. At that time, people weren’t worried about malicious behavior; they were just focused on moving messages around in order to communicate.

With so many people dependent on email in their daily lives, it’s not practical to change the core technology. Instead, those in the industry have focused on ways to add new security features, like email authentication, on top of the existing infrastructure. Email authentication is implemented as a set of extensions to the existing email infrastructure so that it doesn’t create any incompatibilities that would break pre-authentication email; this leaves individual deployments free to upgrade to the new capabilities on their own schedule*.

The industry has converged on two basic authentication technologies: Sender ID and Domain Keys Identified Mail (DKIM). Both Sender ID and DKIM take advantage of the existing network infrastructure provided by the Domain Name Service (DNS) to publish authentication data; this works well because interaction with DNS is already an integral part of the email transmission and delivery process.

The basic authentication flow, illustrated in Figure 1(page 2), is the same for both Sender ID and DKIM with some minor differences in Steps 2, 3, and 4:

1. The sender composes a message and hits ‘send,’ which causes the message to be transmitted to the sending mail server.
2. The Sending Mail Server identifies the recipient, processes the message, constructs the message headers, and sends the message to the recipient’s mail server.
3. The Receiving Mail Server processes the incoming message. It then queries the sender’s DNS entry for the relevant authentication information, which it uses to validate the authentication.
4. The Receiving Mail Server uses the authentication information to validate the incoming message.

* For a much more detailed treatment on the need for authentication and the technologies in use to achieve it, see the whitepaper issued by the Messaging Anti-Abuse Working Group in March 2008, “Trust in Email Begins with Authentication” [13]
5. The receiver’s back end processing combines the results of the authentication with any relevant reputation data and content filtering to determine whether the message will be delivered to the recipient’s Inbox, Junk folder, or whether it will be blocked completely.

6. Finally, the recipient will be able to access the message the next time email status is updated, assuming it has not been blocked.

1.1 Sender ID

Sender ID technology was developed primarily by Microsoft. It was designed to be an inexpensive solution for senders; there are no processing changes required on the sender side, so no additional processing is required in Step 2 of Figure 1.

Senders must inventory their use of outbound email and prepare a comprehensive list of all mail servers that send outbound mail on behalf of a designated domain. This list would include all departments of a given organization as well as any 3rd party servers that may send email on behalf of the organization. Remember that different mail servers may be used for corporate and marketing email or for other specific functions. This list is then published as a Sender Policy Framework (SPF) record* in the Domain Name Service (DNS) entry for the organization’s domain.

 Receivers implement the Sender ID Framework (SIDF) that performs the validation analysis for each incoming email (see Step 4 in Figure 1). The receiver determines the Purported Return Address† (PRA) for the email according to a set of rules and then queries the DNS for that domain to check for an SPF record. If the record exists, and if the mail server responsible for sending the email is listed in the record, then the email is successfully authenticated as originating from the PRA domain. If the record is found but the mail server is not listed, then the email fails authentication. If there is no record, then the email is not authenticated.

* For help constructing the SPF record for your domain, Microsoft has created an SPF wizard [10] to walk you through the process. Once it’s published, you can test your SPF record with the Email Sender and Provider Coalition Sender ID Testing Tool [11].

† Some receivers use the Sender Policy Framework engine rather than the SIDF engine to validate messages. The SPF engine uses the envelope MAIL FROM (sometimes visible as the Return-Path header in a delivered message) rather than the PRA as the domain to be authenticated.
1.2 Domain Keys Identified Mail (DKIM)

Domain Keys Identified Mail differs from Sender ID in that it is a cryptographic mechanism that requires processing on both the sending and receiving side of the message transfer process. DKIM is the evolution of Yahoo’s Domain Keys combined with Cisco’s Identified Internet Mail protocol and has been approved as a draft standard by the Internet Engineering Task Force (IETF), a standards body focused on standards relating primarily to the Internet space.

In order to enable DKIM authentication, a sender must first generate a pair of cryptographic keys: one that is kept private and one that will be published for receivers. They must then inventory all of the mail servers authorized to send mail for the sender’s domain and provide a copy of the private key to each of those authorized mail servers. The details on how the keys are generated and stored will differ according to the mail server implementation, so refer to the product-specific documentation for more detailed instructions.

The public key is then published in the DNS entry for the sender’s domain*, along with some additional information†. To send a DKIM authenticated message as in Step 2 of Figure 1, the outgoing message must be signed with the domain’s private key††. First, a hash of some specified parts of the message is computed, then that hash is encrypted, or signed, with the private key. The signature is inserted into a new message header called DKIM-Signature along with some additional information such as which parts of the message were included in the signature.

A receiver detects the DKIM-Signature header. Then, as seen in Step 3 of Figure 1, it uses information in this header to determine the domain responsible for sending the message. Next, it queries DNS for the record in that domain containing the corresponding public key. If the key is located, it is used to decrypt the signature embedded in the DKIM-Signature header. The receiver then uses the information in the header to generate the same hash that was computed by the sender and compares it to the hash it has just decrypted from the DKIM-Signature header (see Step 4 of Figure 1). If the two match, then the DKIM authentication is successful. If they do not match, or if the key is not found, the DKIM authentication fails.

* Information on constructing your DNS record for the public key can be found at the DKIM Resource Website [2], and to test the validity of your DKIM DNS record and signing process you can use the DKIM Testing Reflector [12].

† For security and flexibility, it is possible to have more than one DKIM public key stored in a single DNS domain entry; the different keys are distinguished by adding different selector prefixes to each. This means, for example, that if a sender does not want to give out their corporate private key to a 3rd party, they may generate a separate key pair for use by the 3rd party mail servers. It also means that should a private key become compromised, it is simple to create and publish a new one without disrupting any existing infrastructure.

†† If you manage your own email servers and want to send DKIM authenticated email, you will need to make sure your mail server software implements DKIM. Several commercial mail servers already have support for DKIM and more will become available as adoption increases.
2. Benefits for Both Senders and Receivers

Everyone has their own slant on the topic of email authentication, but the bottom line is that it is good for everyone who cares about email as a legitimate communication medium. It’s good for senders because it allows them to take clear responsibility for the email they send and helps repudiate a forged email claiming to come from their domains.

It’s good for receivers because it provides validated identities for which behavioral data, or reputation, can be collected; it also makes it easier for receivers to detect email forgeries, which often come in the form of spoofing or phishing scams. It’s also good for recipients because they can have greater confidence that authenticated email in their inboxes is email that truly originates from the sender (i.e., the designated sender is not forged). Recipients will also tend to have fewer legitimate messages that get lost in spam filters and fewer spam messages that slip through.

Email authentication is good for the industry in general. The Email Sender and Provider Coalition (ESPC) requires authentication of its members [7], who represent a significant portion of the major Email Service Providers. The Messaging Anti-Abuse Working Group (MAAWG) has also published a Sender Best Communication Practices document [8] that strongly recommends that senders “should adopt email authentication for all types of messaging,” as well as a whitepaper entitled “Trust in Email Begins with Authentication” [13].

In Senate testimony about the July 2007 Federal Trade Commission Spam Summit, FTC Chairman Deborah Platt Majoras states that “Industry is taking a leading role in developing technological tools, such as domain-level email authentication, to ‘uncloak’ these anonymous spammers, and the Commission is encouraged by reported increases in the adoption rates for email authentication.” The FTC agrees that technological solutions are more effective than legislation in tackling the enormous volumes and dynamically changing tactics of spam and relies on the industry to drive adoption of these key solutions so as to avoid legislation that is likely to be outdated before it is enacted.

2.1 Benefits for Senders

The most immediate benefit of email authentication today, from a sender’s perspective, is the increased recipient confidence. Recipients receiving a successfully authenticated email can have confidence that the message truly originated from the designated sender. This helps senders protect their brands and maintain their customers’ confidence in their email and in their company as a whole.

Many senders also want to know how authenticated email can help their delivery rates. This is a much more difficult question to answer. Because authenticated email helps receivers filter out forged email and because few spammers stay at a given location long enough to make it worthwhile to publish authentication data, some receivers are already providing some positive weight in their filtering mechanisms for successfully authenticated email. The effect is still fairly minor today, but it will likely increase as authentication becomes more prevalent.
It’s important to note, though, that authentication alone is not a silver bullet. Just because you are authorized to send mail for a particular domain does not automatically mean that you are sending permission-based email or that you’re not generating complaints from your recipients. The real benefit of authentication is that it provides a verifiable identity to which receivers can attach reputation data; it’s the reputation data, or the actual behavior of that verified identity over time, which will have the greatest impact on delivery metrics.

2.2 Benefits for Receivers

Receivers realize two key benefits from authenticated email: the existence of a verifiable identity for which reputation data can be collected and the ability to more easily detect forgeries.

The vast majority of spam today is malicious and criminally-focused email generated by botnets, or dynamic groups of compromised machines. Running email through content filters is a fairly resource-intensive operation, so mechanisms that help tag an email as malicious before it even gets to the content filters can improve the overall efficiency of email delivery. Detecting spoofed or forged emails via failed authentication can therefore be very helpful to inbound email filtering efficiency* if it can enable a receiver to throw out any email that fails authentication. However, because authentication is just beginning to achieve broad adoption, both senders and receivers are being somewhat conservative about taking decisive action based on authentication failure. Today, receivers are more likely to assign a positive weight for a successful authentication and to possibly allow the email to bypass selected parts of the content filtering; as industry confidence in authentication builds and its adoption increases, we will likely see more negative consequences attached to failed authentication.

For email that is successfully authenticated, receivers now have a verifiable identity for which they can build a reputation by collecting things like complaint data from their customers and incidence of bad addresses. They can also augment their private reputation data by consulting with 3rd party reputation engines that monitor other aspects of sender behavior. The reputation data builds up a model of a sender’s behavior that, over time, becomes a fairly reliable predictor of future behavior.

3. Setting up Authentication

Setting up authentication is reasonably straightforward for network administrators, but somewhat less straightforward for individuals managing their own domains†. The basic requirement is that special records with authentication data need to be published in the Domain Name Service (DNS) entry for the domain that represents your email identity.

---

* Microsoft publishes some data on the efficacy of Sender ID authentication in filtering out forged email in the Sender ID Framework White Paper [9].

† Since most people are not DNS experts, the most straightforward approach is to find a solution that does not require hands-on DNS management. If you’re not interested in all of the details in this section, you may want to read Section 3.1 and skip Section 3.2.
The approach you need to take in order to get this information published will differ according to your specific situation, but most people fall into one of three basic categories:

- Using an Email Service Provider (ESP) to send email
- Owning and managing your own DNS domain
- Using an Internet Service Provider (ISP) account for email

For Sender ID, the record that needs to be published is called the Sender Policy Framework (SPF) record. The SPF record lists all of the mail servers that are authorized to send email on behalf of your domain. These servers can be listed explicitly and they can also be included from an existing SPF record in another domain by including a reference to that external SPF record.

For DKIM, the information that needs to be published in your DNS entry is the public key that receivers will use to validate your DKIM signed messages.

3.1 Using an Email Service Provider (ESP) to Send Email

If you use an ESP to send your email, you should talk to them about what it takes to get your authentication information published. Almost all reputable ESPs already support at least one and often both of the two main authentication technologies and should be able to either publish your authentication records for you or give you guidance on how to publish them yourself if you maintain your own domain name*.

3.2 Owning and Managing Your Own DNS Domain

If you (as an individual or a company) own and manage your own DNS domain, you can create and publish your own authentication records. Note that having your own domain name does not always imply that you can manage your DNS entry; whether or not you have that access depends on your domain hosting provider’s policies. With this level of self-management, it helps to have an experienced IT department or consultant in order to avoid problems with incorrect or out-of-date DNS authentication entries.

Assuming that you do have access to your DNS entry, you next have to decide which authentication information you want to publish. Sender ID (or SPF) is the simplest way to implement authentication on the sender side since it requires that you publish an accurate SPF record†. DKIM is somewhat more complex; in addition to publishing the authentication information, your mail servers (or the mail servers of your ESP) need to be prepared to do the cryptographic signing required by the sender side of the DKIM authentication protocol.

*If you manage your own domain and you maintain corporate email servers separate from those of your ESP, make sure that your corporate mail servers are also included in your published SPF record; you don’t want your corporate email to fail authentication even if your marketing email is passing with flying colors!

†Please refer to Section 1.1 for details on how to construct an SPF record for your organization.
For details on configuring your mail servers and on creating and publishing the necessary DNS information to support DKIM, please refer to Section 1.2.

3.3 Using an Internet Service Provider Account for Email

If you do not own your own domain and do not use an ESP, then you probably use an email address from your Internet Service Provider (ISP) as your email identity. In that case, your email address will look something like jsmith@yahoo.com or jdoe@hotmail.com. You probably do not have any access to the DNS for your email domain and it is unlikely that your ISP will be interested in making any special arrangements for publishing your authentication information.

The good news is that many of the major ISPs are creating authentication records for their outgoing mail, so your mail may already be authenticated even though you don’t know it.

The bad news is that because you are sharing the authentication identity with all the other customers of your ISP, the authentication is probably not going to help you very much. It will help reduce the likelihood that someone could forge email from you, but won’t do much to help you build a positive reputation because there are likely many “legitimate” customers of your ISP who are using their accounts to send out abusive email.

It’s possible that this will change in the future as authenticated reputation plays an increasingly important role in ISP email filtering mechanisms, but for the present, if you want to be able to build up a positive sender reputation that really belongs to you, you should consider getting your own authentication domain – either on your own or by using an ESP or ISP that can manage the details for you.

4. Reputation: The Next Step

No discussion of authentication in the email industry would be complete without setting it in the larger context of reputation. The huge volumes of spam that plague the internet make the ability to distinguish legitimate email from spam a critical function for receivers; and, clearly, simply knowing who sent an email (authentication) is not very helpful unless you know something about the sender’s identity that allows you to make an assessment of how likely it is to be legitimate (sender’s reputation).

With the increasing adoption of authentication, receivers now have a reliable, verifiable identity to which they can attach reputation data. Most receivers keep their own proprietary reputation data, fed in large part by complaints from their customers, but many also use various 3rd party reputation engines. The combination of authentication with reliable reputation engines will yield a very powerful filtering tool and should help stem the flood of spam while enabling the vast majority of legitimate emails to be safely delivered to their intended recipients.
5. References

1. Microsoft Sender ID Resource Website:
   http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

2. Domain Keys Identified Mail (DKIM) Resource Website:
   http://dkim.org

3. Domain Keys Resource Website:

4. Cisco Identified Internet Mail Resource Website:
   http://www.identifiedmail.com/

5. Email Sender and Provider Coalition (ESPC) Website:
   http://www.espcoalition.org

6. Messaging Anti-Abuse Working Group (MAAWG) Website:
   http://www.maawg.org

7. ESPC Authentication Position Statement:
   http://www.espcoalition.org/eaps.php

8. MAAWG Sender Best Communication Practices Document:
   http://www.maawg.org/about/publishedDocuments/MAAWG_Senders_BCP_Ver2.pdf

9. Microsoft Sender ID Whitepaper:

10. Microsoft Sender ID Framework SPF Record Wizard:
    http://microsoft.com/mscorp/safety/content/technologies/senderid/wizard/

11. Email Sender and Provider Coalition Sender ID Testing Tool:
    http://www.espcoalition.org/senderid

12. Domain Keys Identified Mail Testing Reflector:
    http://testing.dkim.org/reflector.html

13. MAAWG Email Authentication Whitepaper *Trust in Email Begins with Authentication*:
    http://www.maawg.org/about/publishedDocuments/MAAWG_Email_Authentication_Paper.pdf