An Introduction To DKIM

DKIM stands for Domain Keys Identified Mail, it helps associate a domain with an email message to help prove the authenticity of the message. DKIM is a successor of DomainKeys developed by Yahoo!, it was deprecated in 2007 but some providers still use it. DKIM was created by an informal group and was submitted to IETF for further development and standarization. DKIM uses public key encryption for signing.

How It Works

The sender (sometimes the signer, not always, for example GMail/Sendmail signs it's users' message, not the users) adds a mail header field *DKIM-Signature:*, the receiver (not necessarily the recipient, it may be the ESP/MTA, like GMail, Yahoo! etc.) recovers the signer's public key from their DNS records - which is computed using details provided in the *DKIM-Signature:* header field - which is used to verify the contents of the message & it's integrity.

A *DKIM-Signature:* header field contains many name-value pairs, know as tags. Names are short maximun one or two letters. The **b** tag contains the digtal signature of the mail contents (body & headers), **bh** stands for the body hash i.e. a fingerprint of the body - which can be used to detect tampering, **s** is for selector which needs to used when fetching the public key from DNS record, **d** is for signing domain. These are the most important tags, there are other tags which provides the DKIM version, cryptographic algorithm, etc being used.

Here's what a typical *DKIM-Signature:* header field looks like:

Code:

```
DKIM-Signature:    v=1; a=rsa-sha256; c=relaxed/relaxed; d=pradeep.net.in;
s=google; h=mime-version:date:message-id:subject:from:to:content-type;
bh=nw/QWDoxuQkO68EUCcAaGvG3rO+avgp48t/a9fE6+HE=;
b=FemyVfhLK3JzsCVGJNIMeGU7M5CJnuTL101xRmLLa5X4zthW4balBzTvDHY1mpcMps
P7V2X+OE9MMMLyMrtsrJx0njInNdrutAEwDbUYIOLKr4SjGPYp9z3lYrA8S4ZRYuYTCL
eoocBienz/OHTE9tWK9Gvgjl5qq5cJw8aytu8=
```

And, here's the correnspondingDNS record for the above header which has the public key:

Code:

```
[pradeep@ubuntu-desktop ~]$ dig google._domainkey.pradeep.net.in TXT

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-16.P1.el5 <<>>
google._domainkey.pradeep.net.in TXT
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64127
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google._domainkey.pradeep.net.in. IN   TXT
```

```
;; ANSWER SECTION:
google._domainkey.pradeep.net.in. 14395 IN TXT  "v=DKIM1\; k=rsa\; t=y\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCWD379T9KmuZecREnBLuRhFEFS6/QknNmevrp
x+PQLUy9I5BlrollH3sXMOGpnAXhdL0gz5MBGwhqQMlsyI//hJ9ijtQIOwwHVL8/A8WTUoVGFOeOf
l8Ss72ijij5aK4f+toSX/gA4pMdUE0cqYNPtn2uzl/dlj29HC9bEZ214yQIDAQAB"

;; Query time: 0 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Tue May 29 00:47:56 2012
;; MSG SIZE  rcvd: 302
```

The receiver/receiving MTA uses the public key to match the signature provided, thereby knowing whether the message is genuine or not, also whether if it was tampered with or not.

Implementing It In MTAs

There are filters available for all the popular MTAs like Sendmail, Postfix, PowerMTA are available online:

Sendmail - http://blog.mixu.net/2009/11/03/sett...sing-sendmail/
Postfix - http://eric.lubow.org/2009/mail/sett...m-and-postfix/
Exim - http://www.systemajik.com/blog/imple...kim-with-exim/

Personal Use

If you have your domain configured for Google Apps, you can easily enable DKIM in all outgoing mails, here's how to go about it http://support.google.com/a/bin/answ...&answer=174124

If you are aware of any other hosting/email provider having DKIM support like Google Apps please do post in the comments, it might help someone setting up DKIM for personal/SOHO use.

Signing Email via Custom Scripts

You may also sign you email with DKIM and forward it to your MTA (in case it does not support DKIM integration, or you may not have the privilege to do so), for that purpose all popular scripting & programming languages have free libraries which will help you accomplish the task. We'll cover this topic another day.

Source: http://www.go4expert.com/articles/introduction-dkim-t28471/