

administrators to learn about DomainKeys, a new (for now useless) standard aimed to separate spam from real e-mail messages.

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [October](#) >

It is time for mail administrators to learn about DomainKeys, a new (for now useless) standard aimed to separate spam from real e-mail messages.

LinuxReviews.org

Google has now implemented Yahoos new proposed anti-spam standard DomainKeys, allowing mail transfer agent software to check if a message who claims to be from gmail comes from them or a spoofed source. There is a experimental open source implementation available, sendmail and qmail support is being developed.

1. [What are DomainKeys](#)
 - ◆ [1.1. How it works](#)
 - ◆ [1.2. Who uses it?](#)
 2. [Why is it \(almost\) useless?](#)
 - ◆ [2.1. DomainKeys does have a practical use as of today](#)
 - ◆ [2.2. Can you use it legally?](#)
-

1. What are DomainKeys

The DomainKey-Signature systems works by applying a field `DomainKey-Signature:` to the message headers. A valid signature may look like this:

```
Received: by mproxy.gmail.com with SMTP id 74so160719rnl
DomainKey-Signature: a=rsa-sha1; c=noFWS;
    s=beta; d=gmail.com;
    h=received:message-id:date:from:reply-to:to:subject:mime-version: \
    content-type:content-transfer-encoding;
    b=WPnI/E1Lo6a/DjT2CarFp ..... TgmeYVheCZa/k4KKejI
Received: by 10.38.152.19 with SMTP id z19mr1347226rnd;
```

(header of a mail sent from gmail)

1.1. How it works

The sender side makes a key pair with a public and private key what will be used for signing. You should read up on the far better verification and encryption standard [GnuPG](#) if you are not familiar with this concept. The private key is added to the MTA program and the public key is published in DNS (Domain Name System) records. The MTA will use the private key to generate signatures for outgoing messages.

administrators to learn about DomainKeys, a new (for now useless) standard aimed to separate spam from real e-mail messages.

The receiving side will check the DomainKey-Signature against the public key stored in DNS. The signature will be broken if the message is not intact or generated by someone using a different key-pair. The recipient MTA will verify that the message is received intact and originates from the sender domain given in the message headers.

1.2. Who uses it?

Yahoo and Gmail are the only major mail providers who have implemented the standard so far. None of them use it to filter, they only support it.

Gmail is still in beta and you must be invited to join the network. LinuxReviews.org has a few invites left, but this may have changed by the time you read this because we are willing to give away on a first ask first get basis. :-)

2. Why is it (almost) useless?

The concept does have potential to be useful, but like all the new proposed anti-spam standards, this can only be practical if it ever becomes a commonly accepted standard and is implemented into the common mail transfer agents used on the market today. [Sendmail](#) already has experimental support, and Yahoo are developing their own Qmail implementation. No Open-Source fully supports the standard as of today. So for now now, rejecting non-signed mail would mean classifying 99,9% of your incoming mail as spam.

A strange effect of all new anti-spam standards is that people who have a legitimate, working mail system that has been running and working for years are likely not to upgrade or change their servers according to the anti-spam standards, while the spam-senders implement such standards very quickly because they are the only ones who have a genuine interest in following such specifications.

This also applies to Microsoft's proposed [anti-spam standard called Sender-ID](#). This standard, however, has a license that makes it impossible to implement it into an open source-based product, meaning the most common MTAs will never support it. LinuxReviews [announced Sender-ID dead](#) a while ago.

If a normal, legitimate user is able to implement any anti-spam measure, then obviously the spam-senders are able to do this too. As domain names are cheap at only \$10, it's a small issue to register a new domain, add the right records and keys, send spam until it is blacklisted and then just move along to the next random domain name.

In short, anyone only accepting mail verified by any of today's anti-spam standards would be rejecting almost all valid mail while accepting spam freely.

2.1. DomainKeys does have a practical use as of today

The DomainKeys can in some way be useful already: It allows domain name owners to make sure nobody uses their domains as a sender address for spam. It also allows the recipient to verify that the mail is delivered intact and untampered.

administrators to learn about DomainKeys, a new (for now useless) standard aimed to separate spam from real e-mail messages.

As said, rejecting all mail without the right records would be terribly foolish, but rejecting false mail from those domains who have implemented the standard is quite possible. A MTA can safely reject unsigned mail from Google because mail valid from their services include keys. So disallowing false mail in those cases where a key exists but does not match is possible. It would not even limit a mere percent of spam, but it would make customers slightly more comfortable. As the last few years of politics and security debate in the USA shows, reality means nothing compared to media propaganda.

2.2. Can you use it legally?

The [Yahoo! DomainKeys Patent License Agreement v1.0](#) does sound quite OK, but do note that are only allow to implement this in "specific portions of a hardware or software implementation expressly required to be compliant with the Specifications for the sole purpose of a sender verification solution in connection with e-mail."

Totally irrelevant, the Norwegian financial magazine Dagens Næringsliv had a headline called [Internet will collapse in 2006 because of spam and viruses](#) today. They base this on loose quotes from [Hannu H. Kari](#). Check out the article for a good laugh if you understand Norwegian.

Learn more:

- [DomainKeys: Proving and Protecting Email Sender Identity](#) (yahoo.com)
- [Gmail Begins Signing Email with DomainKeys](#) (slashdot.org)
- [INTERNET DRAFT Domain-based Email Authentication Using Public-Keys Advertised in the DNS \(DomainKeys\)](#)

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [October](#) >

It is time for mail administrators to learn about DomainKeys, a new (for now useless) standard aimed to separate spam from real e-mail messages.