

JangoMail Tutorial

DomainKeys (DK) and DomainKeys Identified Mail (DKIM)

Overview:

JangoMail fully supports the DomainKeys and DKIM email authentication standards. If you are sending email using a From Address in the format of `username@jangomail.com`, then all of your outbound email campaigns will already be signed with DomainKeys and DKIM, and you need not do anything further.

What is DomainKeys/DKIM?

DomainKeys and DKIM are two email authentication standards, the former invented by Yahoo!, and the latter a combination of efforts by Yahoo! and Cisco. Both of these standards cryptographically sign an email message using a public/private key mechanism in such a way that a sending server can encrypt a message with a private key and a receiving server can decrypt the message using the public key. This ensures that it has not been tampered with en route to the receiving server and to ensure that it originated from the domain that is claimed in the From Address field.

Email messages that are signed with DomainKeys have a **DomainKeys-Signature** header in the email message such as:

```
DomainKey-Signature: a=rsa-sha1; c=noaws; s=jangomail; d=jangomail.com; q=dns;
h=DKIM-Signature:Subject:Sender:From:Date:To:X-Priority:Content-Transfer-Encoding:MIME-
Version:X-Mailer:X-VConfig:Content-Type;
b=EEUzdikFieudUhYwbTeZKOnL5TwzCqQRG47Qlat3zvE1viBvas0mq9y9REzFoP8riz7U8Nb1tyPi+RIQv8PtDi3
hgnPBFudlRAV3hIffLJrR8MzFG8HGRaDkFgc93Gite7RVZMtqdnswbY9DbO55JtZdXGAjIK4fpqkUiPecMY=;
```

Email messages that are signed with DKIM have a **DKIM-Signature** header in the email message such as:

```
DKIM-Signature: a=rsa-sha1; q=dns; c=simple/simple; d=jangomail.com;s=jangomail;
bh=ZLzckQojTfKSnBkKh0yGb42XEjo=; h=Subject:Sender:From:Date:To:X-Priority:Content-Transfer-
Encoding:MIME-Version:X-Mailer:X-VConfig:Content-Type;
b=YM8+L1Dw59pY0PP6fI54SPkLI+1RfLVLzkh91ZHeSXWsmLH7Bdv6CwgF6hmYyGEKzNbDe14EBJeT/yUf1m5d8Jdu90e
d2CkZSLyTmiZgdCPMQNXRnWOiGQv0Ng141GbWuPXA7iT0Zh72C7RGLB6SsjErzd8sNCOH89Ttir0Nvk=;
```

Since JangoMail supports both DomainKeys and DKIM, email messages signed will have both headers present. The signatures present in the header are based on the email message's From Address and the public key in the From Domain's DNS record. The DomainKeys record for `jangomail.com` looks like:

```
jangomail._domainkey.jangomail.com      text =

"k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqZ/L9o9Tw1xb0tdsgNzzqmG
Fg8srW3kGkszJfUY502io7Sacpw/37FJLbskdYKshk2Q50oNwbml1HwXmSsdPK+PYUXYOu7QAof6WE38
kdXpb5mYE0APXeDPad/cer2C7BggEstbOQj3A0zroqfzCwC2+uIX6M3u/ZQAVbfKU1kwIDAQAB"
```

Note that this is a TXT record in the DNS settings for `jangomail.com`. When adding a DomainKeys/DKIM record for a domain, the public key goes into a TXT record for selector `._domainkey.DomainName.com`. In this example, the selector is "jangomail". **Because this DNS record is in place for JangoMail, if you send your email campaigns with a jangomail.com From Address, your email campaigns will**

automatically be signed with both DomainKeys and DKIM and you need not do anything further to take advantage of these technologies.

Read on to learn how to use DomainKeys/DKIM when sending from a non-jangomail.com domain.

Setting up DomainKeys/DKIM with a non-jangomail.com From Address

To set up DomainKeys/DKIM on your own domain, you need to do the following steps:

1. Login to your JangoMail account.
2. Go to **SETTINGS --> Sending and Receiving --> DomainKeys/DKIM.**
3. Add your domain by entering your domain and a selector for your domain. The selector can be any word such as "jangomail" or even your account username. Keep in mind that the selector you choose will correspond to the DNS record you must add for your domain (TXT record for selector._domainkey.yourdomain.com)
4. A private key has now been created for your domain, *but the key pair will be **disabled** until you add the public key into your DNS server.* You must now add the public key to your DNS server. To view the keys, click the **"View Keys"** link next to your domain. A popup will launch showing you the public key, the private key, and the exact DNS TXT record you must add into your DNS server. Contact your DNS server administrator to have the TXT record added for selector._domainkey.yourdomain.com.
5. Once the DNS record is in place, you must come back to JangoMail to enable the key pair. Go to --> **Sending and Receiving --> DomainKeys/DKIM**, and click the **"Enable"** link next to your domain. JangoMail will then verify that your DNS TXT record is in place and correct, and if so, it will enable the key pair. Your email campaigns will now be signed with DomainKeys and DKIM.

How do I know everything is working?

First, to ensure that your emails are being signed with DomainKeys/DKIM, send yourself a test email message from your account, and then view the full headers of the received message. You should see two added headers, a DomainKey-Signature header and another DKIM-Signature header.

Secondly, to test that the signatures are correct, you can do one of several tests:

1. Send a test email message to an @yahoo.com email address. Then login to your Yahoo! Mail account and view the email message. Yahoo! should display a message indicating that the email has been properly signed:

Previous | [Next](#) | [Back to Messages](#)

[Delete](#) [Reply](#) [Forward](#) [Spam](#) [Move...](#)

This message is not flagged. [[Flag Message](#) - [Mark as Unread](#)]

Subject: Check out our brownies this month

From: "The Brownie Kitchen" <BrownieKitchen@jangomail.com> [Add to Address Book](#) [Add Mobile Alert](#)
Yahoo! DomainKeys has confirmed that this message was sent by jangomail.com. [Learn more](#)

Date: Wed, 11 Apr 2007 08:34:27 +0000

Additionally, you can view the headers by clicking the "Full Headers" link the bottom right corner of your screen.

From The Brownie Kitchen Wed Apr 11 01:34:27 2007

X-Apparently-To:	ajaygoel999@yahoo.com via 209.191.69.58; Wed, 11 Apr 2007 01:34:22 -0700
X-Originating-IP:	[38.192.4.42]
Return-Path:	<browniekitchen@jangomail.com>
Authentication-Results:	mta506.mail.mud.yahoo.com from=jangomail.com; domainkeys=pass (ok)
Received:	from 38.192.4.42 (EHLO bombay.jangomail.com) (38.192.4.42) by mta506.mail.mud.yahoo.com with SMTP; V
DomainKey-Signature:	a=rsa-sha1; c=noaws; s=jangomail; d=jangomail.com; q=dns; h=DKIM-Signature:Subject:Sender:From:Date: b=NbAUHpw+JeGpqjwxmAhsTtrxNSf58LutriSA000dCfpZJKu1vzUmDNEvcW2Qqg9+xQId4G/vEFXAKQf6Aert7wPit
DKIM-Signature:	a=rsa-sha1; q=dns; c=simple/simple; d=jangomail.com; s=jangomail; bh=rCVgY6y0Da2gPPuvunHKBQix7c= h=Subject:Sender:From:Date:To:X-Priority:Content-Transfer-Encoding:MIME-Version:X-Mailer:X-VConfig:Cont: b=UVJ8lGsnmIe47WT802KPK7z7reVubv3eru0K.mM4i6GJO4ypwk9+PoOcNawDcBB7aJJGba7RWeb4dpW/SqAC
Subject:	Check out our brownies this month
Sender:	"The Brownie Kitchen" <BrownieKitchen@jangomail.com>
From:	"The Brownie Kitchen" <BrownieKitchen@jangomail.com> Add to Address Book Add Mobile Alert Yahoo! DomainKeys has confirmed that this message was sent by jangomail.com. Learn more
Date:	Wed, 11 Apr 2007 08:34:27 +0000
To:	ajaygoel999@yahoo.com
X-Priority:	3
Content-Transfer-Encoding:	7bit
MIME-Version:	1.0
X-Mailer:	N/A
X-VConfig:	825591538
Content-Type:	text/plain; charset="ISO-8859-1"
Content-Length:	205

2. Send a test email message to an @gmail.com email address. Then login to your Gmail account and view the email message. Click on "show details" and you should see this information:

Check out our brownies this month [Inbox](#)

★ from **The Brownie Kitchen <BrownieKitchen@jangomail.com>**
to ● **ajaygoel999@gmail.com**
date **Apr 11, 2007 4:34 AM**
subject **Check out our brownies this month**
signed-by **jangomail.com**
mailed-by **jangomail.com**

Additionally, if you click the Down arrow next to "hide details", and then choose to "Show original", you will see the full email headers, including the DomainKey-Status header.

```
Delivered-To: ajaygoel999@gmail.com
Received: by 10.100.6.12 with SMTP id 12cs30263anf;
  Wed, 11 Apr 2007 01:34:24 -0700 (PDT)
Received: by 10.70.52.2 with SMTP id z2mr703472wxz.1176280464071;
  Wed, 11 Apr 2007 01:34:24 -0700 (PDT)
Return-Path: <BrownieKitchen@jangomail.com>
Received: from bombay.jangomail.com (bombay.jangomail.com [38.192.4.42])
  by mx.google.com with ESMTSP id h7si479795wxd.2007.04.11.01.34.21;
  Wed, 11 Apr 2007 01:34:24 -0700 (PDT)
Received-SPF: pass (google.com: domain of BrownieKitchen@jangomail.com designates
38.192.4.42 as permitted sender)
DomainKey-Status: good
Message-Id: <461c9d8e.67dfabae.4af9.ffff9552SMTPIN_ADDED@mx.google.com>
DomainKey-Signature: a=rsa-sha1; c=noaws; s=jangomail; d=jangomail.com; q=dns;
  h=DKIM-Signature:Subject:Sender:From:Date:To:X-Priority:Content-Transfer-
Encoding:MIME-Version:X-Mailer:X-VConfig:Content-Type;
  b=W2lJIVf3fB/iKheqPAOFDP8qfRmLIizQHxX6obnSBIBxWs4bsApKBm9/d6pSfjv3zXpOXZ6eD/9v2vS
fKAZQrzka0/oVgPjUWJtMop8IpTyVHWD6yDUSMqszqw2Z/7MuPxPm6ScVjaHKxm39GRm+j1+beibb3NFVMnjWKiEdn
Pw=;
DKIM-Signature: a=rsa-sha1; q=dns; c=simple/simple; d=jangomail.com;s=jangomail;
bh=rCVgY6y0Da2gPPuvunHKBQQix7c=; h=Subject:Sender:From:Date:To:X-Priority:Content-
Transfer-Encoding:MIME-Version:X-Mailer:X-VConfig:Content-Type;
b=erluSwcWV/SPnZsbtySmQ09vvOhDlhbJegIiPsh9TdtR731i+s0/CLuRqbLuHetgOntKamYsu6SVrozVZK7ieC1S
7Ab3D1keXxJrC0CrogKkzJgfpNq3Ndy+Tsp8CmUck2BiR9Rv3Dx/hLqNKYB+DjbocHmsaL0xo/EK/vBocKQ=;
Subject: Check out our brownies this month
Sender: "The Brownie Kitchen" <BrownieKitchen@jangomail.com>
From: "The Brownie Kitchen" <BrownieKitchen@jangomail.com>
Date: Wed, 11 Apr 2007 08:34:27 +0000
To: ajaygoel999@gmail.com
X-Priority: 3
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
X-Mailer: N/A
X-VConfig: 825591541
Content-Type: text/plain; charset="ISO-8859-1"
```

3. Send a test email message to the Sendmail reflector service. Do this by sending an email message to sa-test@sendmail.net. Sendmail will respond immediately with an email message sent back to the From Address of your test message. The message will look like below and will show you the results of multiple email authentication tests:

We hope this service has been helpful to you.

Authentication System: DomainKeys Identified Mail
Result: DKIM signature confirmed GOOD
Description: Signature verified, message arrived intact
Reporting host: sendmail.net
More information: <http://mipassoc.org/dkim/>
Sendmail militer: <https://sourceforge.net/projects/dkim-milter/>

Authentication System: Domain Keys
Result: DK signature confirmed GOOD
Description: Signature verified, message arrived intact
Reporting host: sendmail.net
More information: <http://antispam.yahoo.com/domainkeys>
Sendmail militer: <https://sourceforge.net/projects/domainkeys-milter/>

Authentication System: Sender ID
Result: SID data confirmed GOOD
Description: Sending host is authorized for sending domain
Reporting host: sendmail.net
More information: <http://www.microsoft.com/senderid>
Sendmail militer: <https://sourceforge.net/projects/sid-milter/>

Authentication System: Sender Permitted From (SPF)
Result: SPF data confirmed GOOD
Description: Sending host is authorized for sending domain
Reporting host: sendmail.net
More information: <http://spf.pobox.com/>

Additional Resources:

- Official DomainKeys website: <http://antispam.yahoo.com/domainkeys>
- Wikipedia explanation of DomainKeys: <http://en.wikipedia.org/wiki/DomainKeys>
- Official DKIM website: <http://www.dkim.org/>
- Wikipedia explanatio of DKIM: http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail
- Differences between DomainKeys and DKIM: bottom of <http://www.dkim.org/info/dkim-faq.html>
- Test your DomainKeys DNS record: <http://domainkeys.sourceforge.net/selectorcheck.html>