

Email Authenticatie

EMMA-nl Workshop 13-10-2009

Maarten Oelering



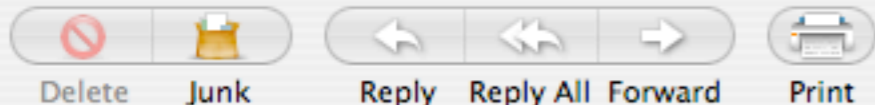
Agenda

- Email authenticatie

- Waarom is het een must?
- SPF, SIDF, DK, DKIM: overeenkomsten en verschillen
- Vragen

- DKIM implementatie

- Waarom juist DKIM?
- Een stappenplan met voorbeelden
- Afsluiting en vragen



From: PayPal@mail.solovirtuoso.com , service@intl.paypal.x.com
 Subject: **Confirm your PayPal Anti-Fraud Protection**
 Date: 4 november 2008 5:57:00 GMT+01:00
 To: Maarten Oelering

Zomaar een email van PayPal...



Protect Yourself from Fraud!

Dear user,

We have noticed an increasing fraudulent activity recently. In order to provide your security and protect you from fraudsters we have introduced a new system of identification that will help us to avoid any kind of fraud or unauthorised access.

To complete your Anti-Fraud Protection, you must click the link below and enter as more information as possible to provide your complete identification and to activate all the features of the new system.

<https://www.paypal.com>

Please do not reply to this email. This mailbox is not monitored and you will not receive a response.

Copyright © 1999-2008 PayPal. All rights reserved.

Consumer advisory- PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore.
 Users are advised to read the terms and conditions carefully.

PayPal Email ID PP051

PayPal – The safer, easier way to pay

- Use your credit card without exposing your card number to merchants.
- Speed through checkout without stopping to enter your card number or address.
- Send money to family and friends for free.

Fight fake emails

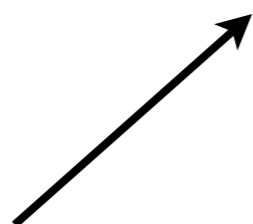
- Make sure you're using the latest internet browser.
- Visit the PayPal Security Center.

`<p>To complete your`

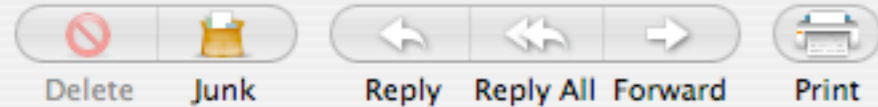
```
    <table cellspacing="0" cellpadding="1" border="0" bgcolor="#ffe65c" align="center" width="300">
```

```
        <tr>
            <td>
                <table cellspacing="0" cellpadding="4" border="0" bgcolor="#fffecd" align="center" width="100%">
```

```
                    <tr>
                        <td align="center" class="sansSerif"><a href="http://secure.paypal.com.session-26352156505235267564.2424-1076902805185708.ssl91.mobi">https://www.paypal.com</a></td>
```



```
                    </tr>
                </table>
            </td>
        </tr>
    </table>
```



From: service@paypal.nl
 Subject: **Activate Your PayPal Account!**
 Date: 1 oktober 2008 11:50:52 GMT+02:00
 To: Suremail <paypal@suremail.eu>

En vertrouw je deze nog...



Confirm Your Email Address!

Beste Suremail,

To complete your **PayPal Business account**, you must **click the link below** and enter your password on the following page to confirm your email address.

[Click here to activate your account](#)

After you confirm your email address, you can send money for FREE, accept unlimited credit card and bank account payments, use special tools for sellers, and receive exclusive customer service hotline help 7 days a week. You will be subject to a low fees for receiving payments.

You can also confirm your email address by logging into your PayPal account at <https://www.paypal.com/nl>. Click on **Confirm Email** in the **To Do List** and then enter this confirmation number: 1415-0047-0059-1657-2314

Dank u dat u heeft gekozen voor PayPal!
 Het PayPal-team

Wij vragen u niet te reageren op dit e-mailbericht. Dit e-mailadres wordt niet gecontroleerd en u ontvangt geen reactie. Voor hulp kunt u [inloggen](#) op uw PayPal-rekening en rechtsboven op een PayPal-pagina op de link Hulp klikken.

[Werk uw voorkeuren bij](#) als u e-mailmeldingen in platte tekst in plaats van HTML wilt ontvangen.

PayPal – De veilige en gemakkelijke manier om te betalen

- Gebruik uw creditcard zonder dat handelaren uw kaartnummer te zien krijgen.
- Handel de betaling snel af zonder dat u opnieuw uw kaartnummer of adres hoeft in te voeren.
- Kosteloos geld sturen.

Bescherm uw rekening

Houd uw PayPal-wachtwoord geheim. Verstrek het nooit aan anderen.

Reageer niet op e-mailberichten waarin u om rekeninggegevens wordt gevraagd.



Nut van authenticatie

- **Vertrouwen terugbrengen in email**
 - Ontvanger beschermen tegen ‘spoofing’ en ‘phishing’
 - Verzender beschermen tegen misbruik domein (‘brand protection’)
- **Meer efficiënte spam filtering**
 - Legitieme verzenders beter herkennen (betrouwbaarder, sneller, gedetailleerder)



Authenticatie als bouwblok

Anti-spam beleid

Reputatie / Accreditatie

Authenticatie

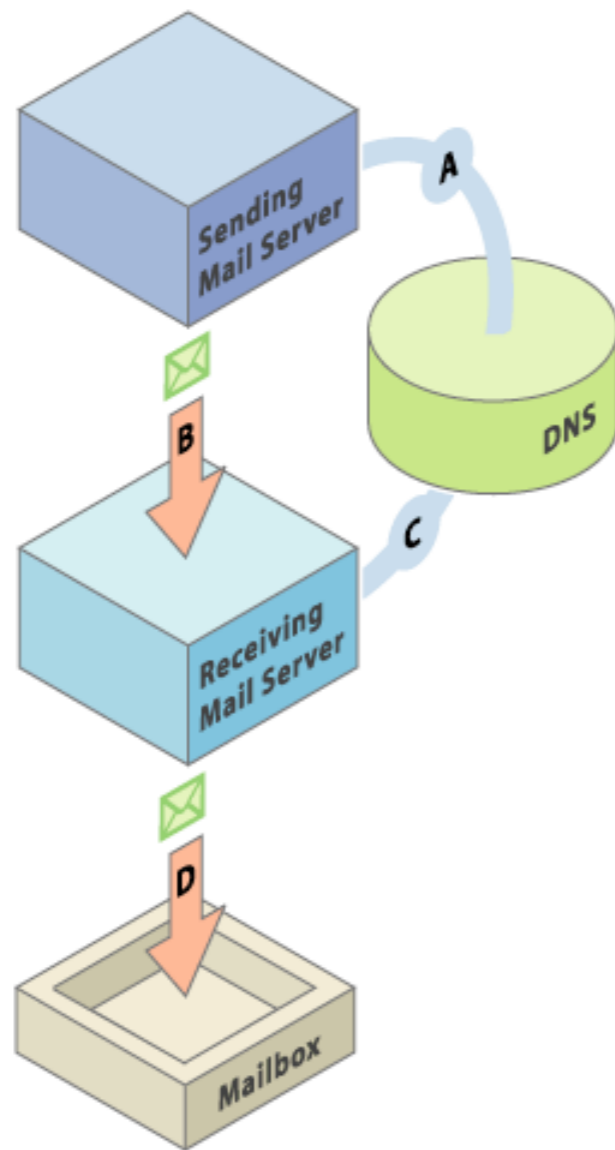
Identiteit



Afzender identiteiten

- IP adres mail server
- Hostnaam mail server (helo)
- Envelope sender (bounce adres)
- Sender header adres (optioneel)
- From header adres

Authenticatie via DNS



- Eigenaar domein plaatst bepaalde informatie in DNS
- Verzender verzend email met dit domein als identiteit
- Ontvanger controleert kenmerken in email met informatie uit DNS
- Ontvanger behandelt email afhankelijk van resultaat



FCrDNS

- Authenticatie van hostnaam mail server
 - IP adres lookup (PTR) => hostnaam
 - hostnaam lookup (A) => IP adres
 - hostnaam == HELO naam
- Toegepast in vele mail software

Sender Policy Framework



- Authenticatie van envelope sender domein en helo naam
- Registratie van mail servers welke namens domein mogen verzenden
- Toegepast door Google en vele anderen



Sender ID

- Authenticatie van “zichtbare afzender” (PRA = Sender cq From header)
- Registratie van mail servers net als SPF
- Optioneel SPF “versie 2” met scope parameter
- Toegepast door Microsoft (Hotmail en Exchange)



DomainKeys

- Authenticatie van email content
- Identiteit is From header domein
- Gebaseerd op cryptografie (PKI)
- Werkt ook bij forwarding
- Toegepast door Yahoo en anderen



DKIM

- Combinatie van DK en Cisco IIM
- Gezien als opvolger DomainKeys
- Willekeurige identiteit (SDID)
- Publicatie signing practices (ADSP)
- Toegepast door Yahoo, AOL, Google



Reguliere post als metafoor

SPF

Dear Email Marketer,
Are you really at
315 Park Ave South
New York, NY 10010?

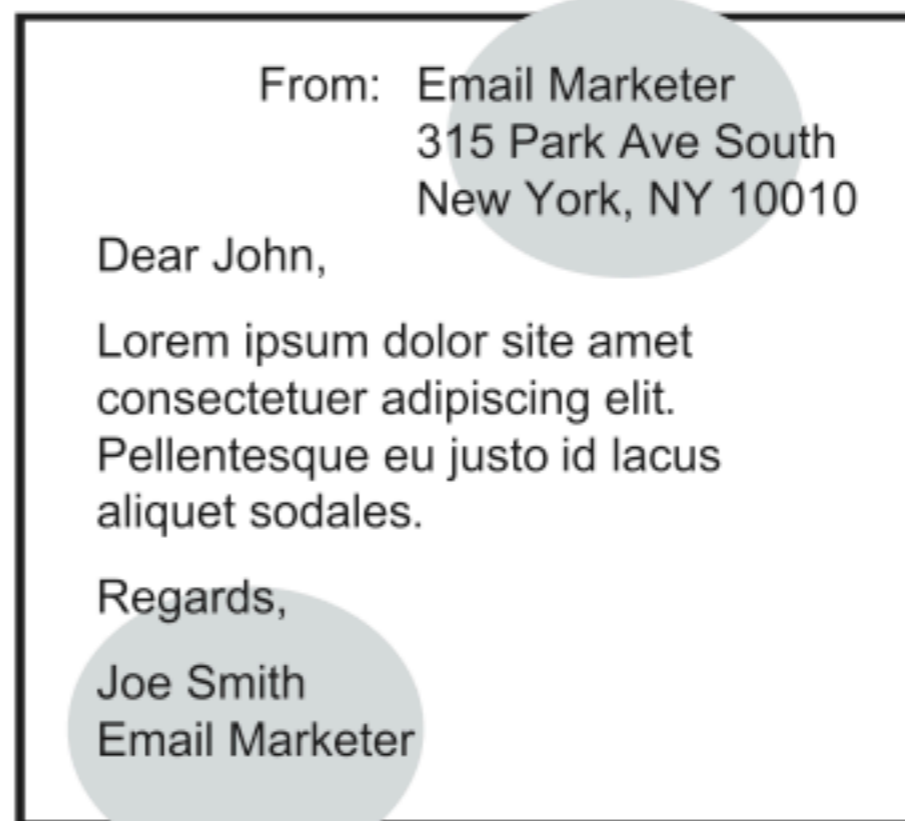


Yahoo DomainKeys

Dear Joe,
Is this really your signature?

Microsoft Sender ID

Dear Email Marketer,
Are you really at
315 Park Ave South
New York, NY 10010?





Beleid providers



4. Authenticate your outbound e-mail: Publish Sender Policy Framework (SPF) records

Windows Live Hotmail currently uses Sender ID to provide additional input to the SmartScreen™ junk e-mail filter process which helps determine if the e-mail or sender is legitimate. The Sender ID Framework is an authentication technology and the key piece of the framework is checking SPF records. Unauthenticated e-mail sent to Windows Live Hotmail users is not necessarily deleted or junked,



To ensure that Gmail can identify you:

- Use a consistent IP address to send bulk mail.
- Keep valid reverse DNS records for the IP address(es) from which you send mail, pointing to your domain.
- Use the same address in the 'From:' header on every bulk mail you send.

We also recommend publishing an [SPF record](#), and signing with [DKIM](#) or [DomainKeys](#).



Use email authentication such as DKIM. This will help us show users that the email is legitimately from you and, if you sign all your email, it will help us identify forgeries, too. In addition, using dedicated selectors/domains for different mail streams (e.g., transactional messages vs. marketing emails) is also a recommended practice.



Waar staat u het liefst?



DKIM Implementatie

EMMA-nl Workshop 13-10-2009

Maarten Oelering



DKIM is hot

Powerful new antiphishing weapon DKIM emerges

DKIM standard attracts Cisco, Google, PayPal and more

By [Carolyn Duffy Marsan](#), Network World, 02/11/2008

[« HTML Email on Apple's iPhone | Main | MailChimp is Hiring »](#)

Postini Likes DKIM Authentication

We've posted in the past how frustrating it can be to get legit er

June 15, 2009

DomainKeys Identified Mail (DKIM) Grows Significantly

DomainKeys Identified Mail (DKIM), an IETF standards-track signature-based mechanism for authenticating email messages, has seen significant growth in



[DKIM: Not Shiny, But Very Important](#)

By J.D. Falk
Director of Product Strategy, Receiver Services

When a new [iPhone or Palm device](#) is released or [Google announces a new OS](#), everybody hears about it. These are, for a short time, the shiniest thing in the tech world. One reason for this phenomenon -- perhaps the primary reason -- is that they directly affect end users. They're things that early adopters drool over and stand in



Waarom DKIM?

- Veilig door gebruik van cryptografie
- Werkt ook bij forwarding van emails
- Identiteit onafhankelijk van inhoud
- Publieke internet standaard
- Sterke groei in gebruik en acceptatie



Wat is DKIM niet

- Zegt niets over ‘waarheid’ van headers of content
- Zegt niets over de identiteit van de auteur
- Zegt niets over consequenties ontbrekende of ongeldige authenticatie

DKIM implementatie stappenplan



- Kies geschikte identiteit
- Maak sleutelpaar aan
- Publiceer gegevens in DNS
- Configureer mail server
- Test juiste werking

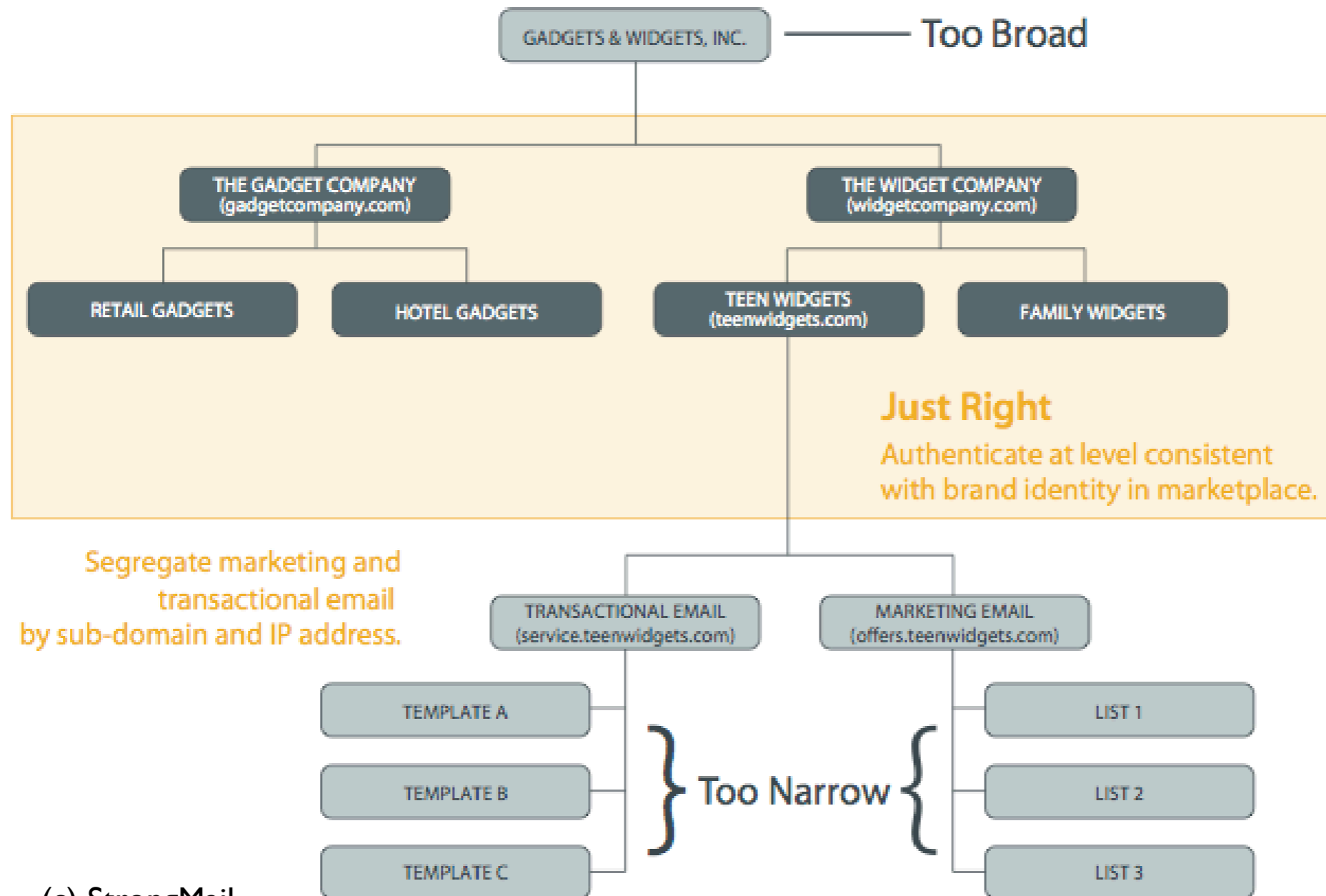


DKIM identiteit

- “...claiming responsibility for the introduction of a message into the mail stream...”
- Onafhankelijk van From, Sender
- Verschillende rollen mogelijk, bijv.
 - domein van auteur
 - domein van ESP
 - domein van reputatie provider (bv EMMA)
- Basis voor opvragen DNS record



Eigen domein als identiteit



(c) StrongMail



DKIM sleutelpaar

- Gebruikt om hash te versleutelen
- RSA 1024 bits of meer
- “selectors” voor sleutelbeheer
 - gebruikt in DNS lookup
 - periodieke vervanging sleutels
 - delegeren sleutel uitgifte



Sleutelpaar aanmaken

Generate private key

```
openssl genrsa -out sel001.deliverability.nl.rsa  
1024
```

Generate public key

```
openssl rsa -in sel001.deliverability.nl.rsa  
-out sel001.deliverability.nl.pub -pubout
```



Sleutelpaar aanmaken

suremail

Address Check Reputation Check **DKIM Wizard**

Enter a domain to create a key pair and DNS record.

Sending domain:

Selector: (e.g. 's001' or '2009')

Click [here](#) to download your private key.

Add a new TXT record to the DNS with the values below.

Name: s001._domainkey.deliverability.nl

Value:



DNS DKIM record

BIND formaat

```
sel001._domainkey.deliverability.nl. IN TXT (  
  "v=DKIM1;t=s;p=MIGfMA0GCSqGS Ib3DQEBAQUAA4GNADCBiQKB"  
  "gQC5mcIZMNtPgvNutAg6GUqe1Dgwnp0j1toZ8UCzZRfhFZ7jdz"  
  "1HyZ0rBWemqwD5N/eXfZancA4FNUTra/Po283T5jA3Z2PWjgLh"  
  "zjKCT4srQR9ZQezOK7LS6sdfqy0yz5BZ0eXb+uwokBQ90Lqrxj"  
  "Z/bdCfhbm7NXc+IeUF07qugwIDAQAB")
```

DNS beheer tool

sel001._domainkey 1 Dag TXT v=DKIM1;t=s;p=MIGfMA0GCS ×



DKIM signature

- “a=”: hash algoritme
- “c=”: canonicalizatie (voorbewerking content voor toepassen hash)
- “d=”: domein verantwoordelijke identiteit
- “i=”: identiteit van gebruiker of onderdeel van “d=” domein
- “s=”: selector voor sleutelbeheer



Ondersteuning DKIM

- Plugins voor Sendmail, Postfix
 - dkim-milter
 - dkimproxy
- Professionele MTA software
 - StrongMail (Email Delivery Server)
 - Port25 (PowerMTA)
 - Message Systems (Momentum for Sending)



PowerMTA configuratie

port25
solutions, inc.

PowerMTA™ 3.5r14

Home

Status

Queues

Domains

Virtual MTAs

Jobs

Logs

```
domain-key sel001, deliverability.nl,  
    /etc/pmta/sel001.deliverability.nl.rsa
```

```
<domain *>  
    dkim-algorithm    rsa-sha256  
    dkim-body-canon   simple  
    dkim-identity     @deliverability.nl  
    dkim-sign         yes  
</domain>
```



Testen DKIM

What's New | **Inbox** 101 messages | **dit is een test**

Delete | Reply | Forward | Spam | Move | Print | More Actions

dit is een test
From: Maarten Oeling <maarten@deliverability.nl> Add | Monday, 12 October, 2009 14:40:05
To: maarten.oeling@yahoo.co.uk

Hallo,
Dit is een test bericht.
Maarten

Full Message Headers

```
X-Originating-IP: [83.160.157.77]
Authentication-Results: mta150.mail.ukl.yahoo.com from=deliverability.nl;
domainkeys=pass (ok); from=deliverability.nl; dkim=pass (ok)
Received: from 83.160.157.77 (EHLO oeling.demon.nl) (83.160.157.77)
by mta150.mail.ukl.yahoo.com with SMTP; Mon, 12 Oct 2009 12:40:07 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed; s=sel001; d=deliverability.nl;
h=Mime-Version:Content-Transfer-Encoding:Message-Id:Content-
Type:To:From:Subject:Date;
bh=O8QrJi54TjGHrOpVLE+8yPxnZtrmWUcNDUB8kNFngdl=;
b=aPSyh7+eeo0iQdxPWAH6YHSaGiQ0BBINdb+2Advn2DmX0f1Tp6OJ6sL/1qc
G+s2kYCI6EmDQFA0R

PcJkXSu4OOZA29+L5KZeoU4LSUIvt9Fkk7hrH1/CSF9xQ7YpddPV0c4nlwIF55C
LfyZIP9ao19Ut
0CI89IKCXEcuhYmQs+w=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=sel001;
d=deliverability.nl;
b=uXIOa48GpCNZzmW9EdYVNgBlqL4AdNG/ytzMweL01LzeX8z4+n/37063fyaL
DsBqXco3MbXHIN5F

pOtRynxWZ0vC+dmr44Wys5MZludFmqdfncoDVDhjPYPjNzopcZVwGJTWLRQb
0LXCF510K100
```

OK



Meer weten?

- domainkeys.sourceforge.net
- dkim.org
- www.ietf.org/rfc/rfc4871.txt
- dkimcore.org
- maarten@suremail.eu