

# Practical DKIM Deployment ( for Mail Service Providers )



The screenshot shows an email client window with a list of emails. The columns are: Absender (Sender), Betreff (Subject), Empfangen (Received), and Größe (Size). The list includes various promotional and personal emails, such as those from Rolex, Cartier, Omega, Chanel, and Prada, as well as university news and personal messages.

Absender	Betreff	Empfangen	Größe
Ryan Lee		26.01.08 14:39	17,4 KB
Rosanne Lindsey	:: 86% Cheaper than Original Price: aRolex, Cartier, Omega, Chanel, Tag...	Heute 03:31	1,2 KB
Tasha D. Foley	:: 86% Cheaper than Original Price: aRolex, Cartier, Omega, Chanel, Tag...	24.01.08 05:43	1,2 KB
Maria McClure	:: 86% Cheaper than Original Price: aRolex, Cartier, Omega, Chanel, Tag...	25.01.08 15:20	1,2 KB
Glen Eubanks	:: 86% Cheaper than Original Price: aRolex, Cartier, Omega, Chanel, Tag...	25.01.08 21:16	1,2 KB
erwin erik	08 Collection of Prada Gucci Dior Chanel & More Top Designer Shoes	Heute 04:58	1,3 KB
andr@omegasoftwar...	Re:[1] cigarettes.. Berlin, London Smoking...	Gestern 22:45	2,4 KB
Antony Teague	[University news]	24.01.08 20:22	2,0 KB
Lila Walls	[University news]	Heute 00:05	2,0 KB
rocreant	{r@maso	Heute 11:42	1,3 KB
Leanna Beck	{Viagra_on@2_de}	25.01.08 06:12	3,6 KB
Tonia Rainey	{Viagra_on@2_de}	Heute 07:08	3,7 KB
horacio leland	Order CIA-LIS Now! In FDA Approved Pharmacy	Gestern 13:31	2,1 KB
Nettie Pritchard	100mgFastShippingProducts	25.01.08 18:43	1,0 KB
Tommie Roberson	100mgForValuedCustomerWorldwide	Heute 04:14	1,0 KB
friedric torsten	2008 Designer Shoes Collection from Gucci Ugg Prada Chanel Dsquared	26.01.08 05:54	1,3 KB
5419744	4973594	23.01.08 17:52	1,3 KB
Lillie Thacker	50mgInfoUSlicensed	25.01.08 14:57	1,0 KB
Jacqueline Mcneal	555eu bonus	24.01.08 09:34	1,5 KB
Trinidad	Aaliyah naives Maedel...!	Gestern 03:05	2,1 KB
acelifts	aareilla	23.01.08 21:38	1,4 KB
Melba	Abbey durchgefickt!	25.01.08 18:29	2,0 KB
Amie j. Wu	Add more length and volume to your penile measurements!	25.01.08 10:52	4,6 KB
Francis S. Padgett	Add more length and volume to your penile measurements!	24.01.08 06:22	4,5 KB
Armand Trevino	AdelaShlongBigglsh	23.01.08 16:47	0,9 KB
Alexandra Plummer	AllimmenseCock	26.01.08 20:56	0,9 KB
Rolph Matteo	amaateur blonde gives nice haindjob with a little oralseix mean times	25.01.08 13:44	1,1 KB
Ishmael Eve	amaateur brandi belle smokes a cig n pole white lid	24.01.08 16:00	1,1 KB
Skye Acacia	amaateur haireciore seix on bed grand exact	24.01.08 06:44	1,1 KB
Delice Aisha	amaateur tein pounded by monster CkoK upon ends	24.01.08 09:41	1,1 KB
Rashaun Remington	amateu tein hottie has to take a thick diK takes argue	26.01.08 10:41	1,1 KB
Jenifer Dafinah	amazing busty tein stripping and teasing ruled still	26.01.08 12:25	1,1 KB
Tia	Amazing that we have so much in common.	25.01.08 02:53	1,2 KB
sparkasse	amtlicher Bescheid (nachrichtenzahl: yx9175832)	24.01.08 18:29	4,9 KB
Mara Hines	Re: and lots of	26.01.08 17:46	0,9 KB

Daniel Black

**OVEE Systems Consultancy**

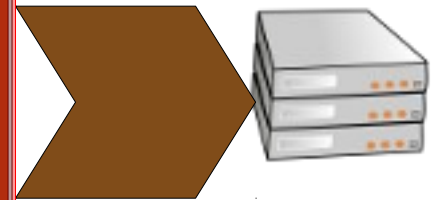
# E-Mail Volume



# E-Mail Volume

Desired mail

Unwanted mail



# E-Mail Volume



# Email Filtering – first cut

IP Reputation Filtering



[zen.spamhaus.org](http://zen.spamhaus.org)

# Email Filtering

## IP Reputation Filtering

---

### **Two /8s allocated to APNIC from IANA (49/8 101/8)]**

**Jeroen van Aart** [jeroen at mompl.net](mailto:jeroen@mompl.net)

*Fri Aug 13 22:52:30 UTC 2010*

- Previous message: [Two /8s allocated to APNIC from IANA \(49/8 and 101/8\)\]](#)
  - Next message: [Reminder: DENOG 2 Call for Participation and Papers](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)
- 

Mikel Jimenez Fernandez wrote:

> *Good news for IPV6 fans!*

>> *Forwarding on behalf of APNIC.*

>> *2010 and will be making allocations from these ranges in the near*

>> *future:*

>>

>> *49/8*

>> *101/8*

[More netblocks to block against spam I say. :-\]](#)

# Email Filtering

IP Reputation Filtering

## IPv6??

# Email Filtering

Domain Reputation Filtering

Without forgery



**Domain**

**Keys**

**Identified**

**Mail**

google.com

asx.com.au

# Domain

K

yahoo.com

facebook.com

I

internode.on.net

M

brisbane.qld.gov.au

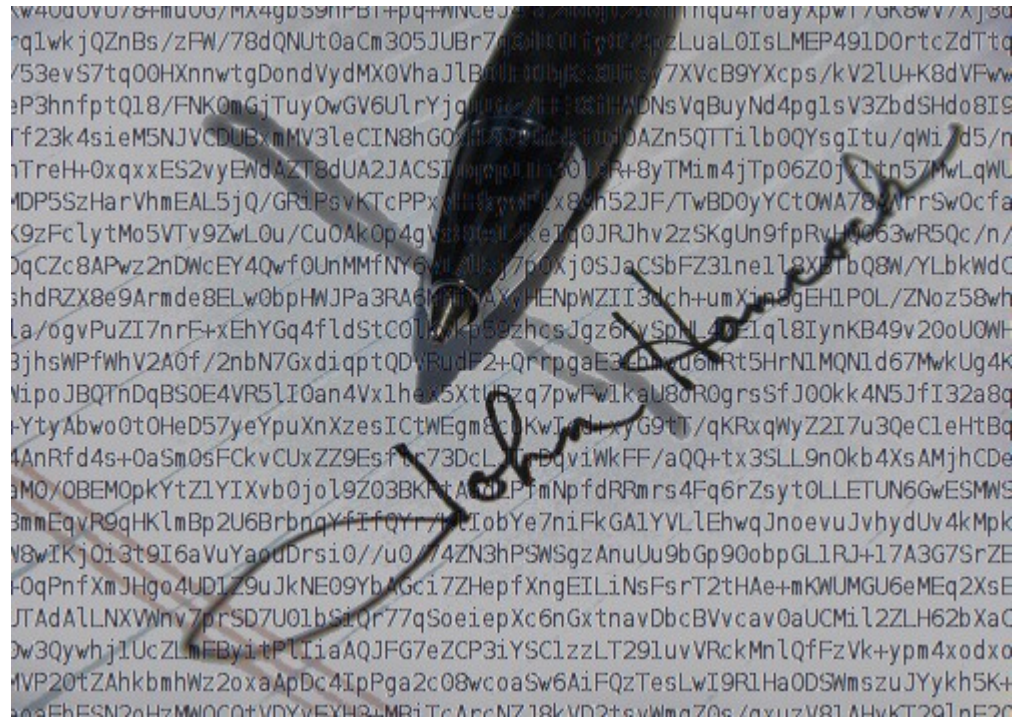
centrelink.gov.au

# Domain

# Keys

I

M





# Domain Keys



# Identified

M



centrelink.gov.au  
asx.com.au

google.com  
brisbane.qld.gov.au  
yahoo.com  
facebook.com  
internode.on.net

# Domain

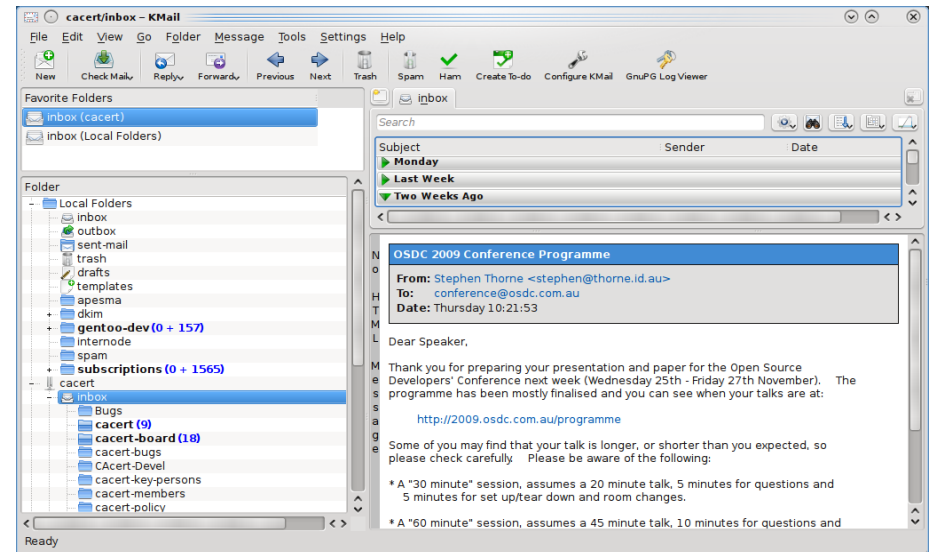
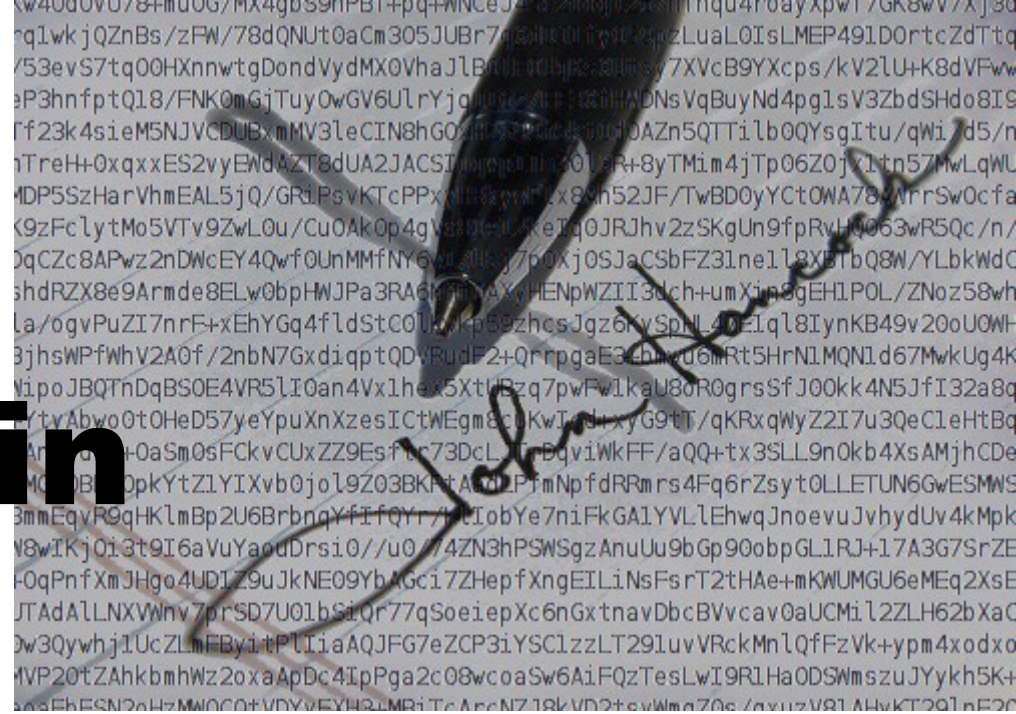
# Keys

# Identified

# Mail



Internode



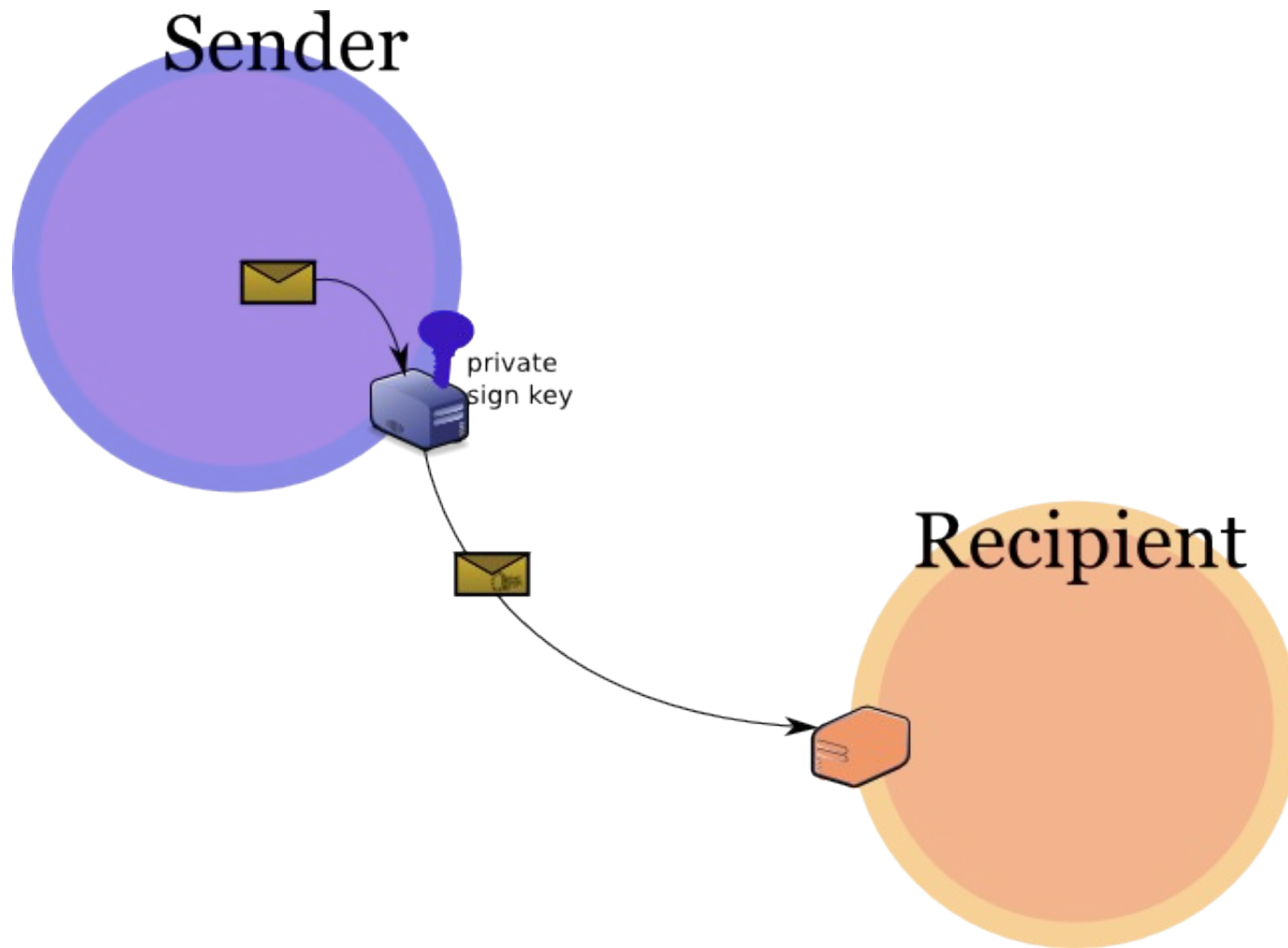
## **Draft 4871bis**

**“Assertion of responsibility** is validated through a cryptographic signature and querying the signer's domain”

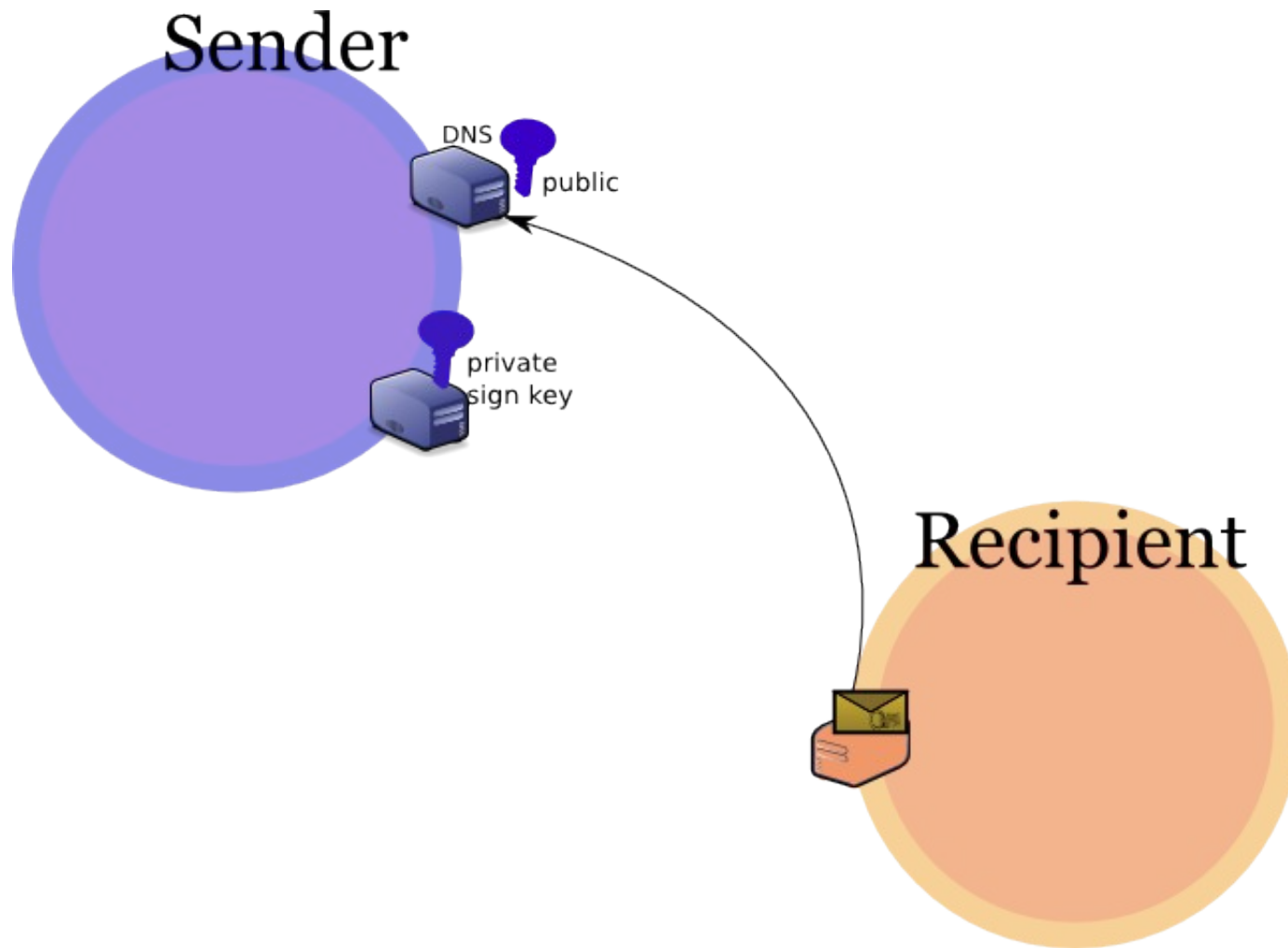
Wording update of:

RFC4871 DomainKeys Identified Mail (DKIM) Signatures  
February 2007

# DKIM Architecture

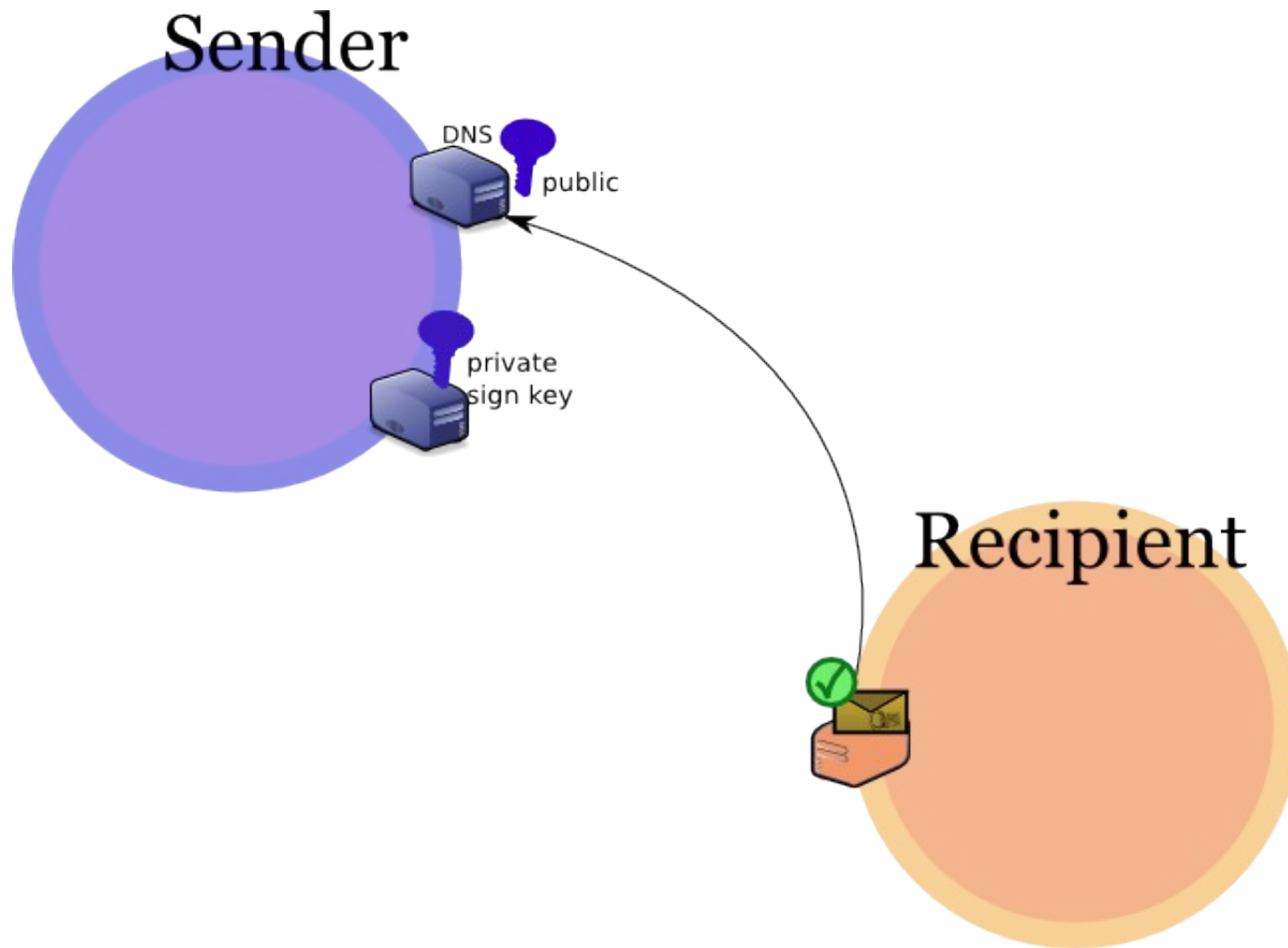


# DKIM Architecture

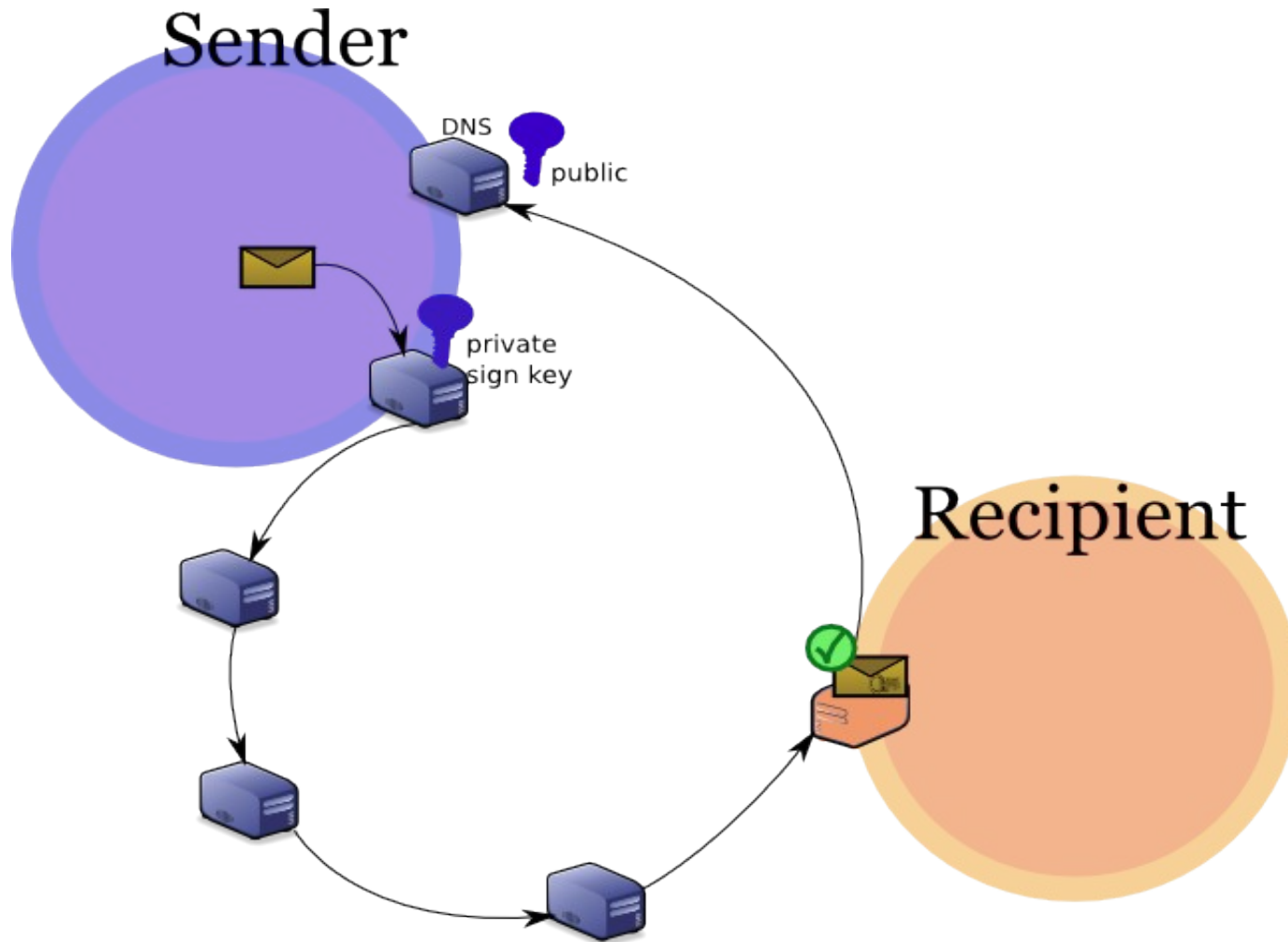




# DKIM Architecture



# DKIM Content and not path



# DKIM Signature

```
Message as Plain Text
id E811C109A0C; Thu, 19 Nov 2009 15:36:21 +0000 (UTC)
Authentication-Results: lists.cacert.org; dkim=pass (1024-bit key)
header.i=@cacert.org; dkim-asp=none
X-Original-To: cacert@lists.cacert.org
Delivered-To: cacert@lists.cacert.org
Received: from email.cacert.org (email.cacert.org [172.16.2.19])
by lists.cacert.org (Postfix) with ESMTPS id 9CF5A1099AC
for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)
Received: from [192.168.1.101] (80-218-4-179.dclient.hispeed.ch [80.218.4.179])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(No client certificate requested)
(Authenticated sender: abuerki)
by email.cacert.org (Postfix) with ESMTPSA id 4C35C94032
for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail;
t=1258644977; bh=iXL4Y4PyZuIVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio
std5jwrD6uzOnAaHFwsjRA6uduOWibvgTi1 ctD+0glvzuEL9x2HT4F90WErDQZijl/R
PFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTcBi3VUIf5uGqTtRIIM+f0Ydbk6j/ioQosqD
893Tutqa5F8MRuv+lZqwFuKdPQf+eHgZc=
Message-ID: <4B0565F1.7050202@cacert.org>
Date: Thu, 19 Nov 2009 16:36:17 +0100
From: =?UTF-8?B?QW5kcmVhcyBCw7xya2k=?= <abuerki@cacert.org>
Organization: CAcert Inc.
User-Agent: Thunderbird 2.0.0.23 (X11/20090817)
MIME-Version: 1.0
To: CAcert Mailingliste EN <cacert@lists.cacert.org>
Subject: CAcert.org Wiki - Restructuring
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="-----ms090108020409060105010004"
Reply-To: cacert@lists.cacert.org
X-Loop: cacert@lists.cacert.org
X-Sequence: 639
Errors-to: cacert-owner@lists.cacert.org
Precedence: list
List-Id: <cacert.lists.cacert.org>
List-Archive: <https://lists.cacert.org/www/arc/cacert>
```

# DKIM Signature – selector + domain = key

**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail;  
t=1258644977; bh=iXL4Y4PyZuIVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;  
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio  
std5jwrD6uz0nAaHFwsjRA6udu0WibvgTi1 ctD+0glvzuEL9x2HT4F90WErDQZljl/R  
PFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTcBi3VUiF5uGqTtRIIM+f0Ydbk6j/ioQosqD  
893Tutqa5F8MRuv+IZqwFuKdPQf+eHgZc=

---

mail.\_domainkey.cacert.org IN TXT "v=DKIM1; g=\*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4G

---

# DKIM Signature - headers

**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail; t=1258644977; bh=iXL4Y4PyZuIVZyrl/04CNPjU4uu4NPY+LiqX8TS6/qq=; h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMiostd5jwrD6uzOnAaHFwsjRA6uduOWibvgTi1ctD+0glvzuEL9x2HT4F9OWErDQZljl/RPFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTcBi3VUif5uGqTtRIIM+f0Ydbk6j/ioQosqD893Tutqa5F8MRuv+lZqwFuKdPQf+eHgZc=

**Authentication-Results:** lists.cacert.org; dkim=pass (1024-bit key) header.i=@cacert.org; dkim-asp=none

**X-Original-To:** cacert@lists.cacert.org

**Delivered-To:** cacert@lists.cacert.org

**Received:** from email.cacert.org (email.cacert.org [172.16.2.19]) by lists.cacert.org (Postfix) with ESMTPS id 9CF5A1099AC for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)

**Received:** from [192.168.1.101] (80-218-4-179.dclient.hispeed.ch [80.218.4.179]) (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits)) (No client certificate requested) (Authenticated sender: abuerki) by email.cacert.org (Postfix) with ESMTPSA id 4C35C94032 for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)

**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail; t=1258644977; bh=iXL4Y4PyZuIVZyrl/04CNPjU4uu4NPY+LiqX8TS6/qq=; h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMiostd5jwrD6uzOnAaHFwsjRA6uduOWibvgTi1ctD+0glvzuEL9x2HT4F9OWErDQZljl/RPFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTcBi3VUif5uGqTtRIIM+f0Ydbk6j/ioQosqD893Tutqa5F8MRuv+lZqwFuKdPQf+eHgZc=

**Message-ID:** <4B0565F1.7050202@cacert.org>

**Date:** Thu, 19 Nov 2009 16:36:17 +0100

**From:** =?UTF-8?B?QW5kcmVhcyBCw7xya2k=? <abuerki@cacert.org>

**Organization:** CAcert Inc.

**User-Agent:** Thunderbird 2.0.0.23 (X11/20090817)

**MIME-Version:** 1.0

**To:** CAcert Mailingliste EN <cacert@lists.cacert.org>

**Subject:** CAcert.org Wiki - Restructuring

**Content-Type:** multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="-----ms090108020409060105010004"

**Reply-To:** cacert@lists.cacert.org

**X-Loop:** cacert@lists.cacert.org

**X-Sequence:** 639

**Errors-to:** cacert-owner@lists.cacert.org

**Precedence:** list

**List-Id:** <cacert.lists.cacert.org>

**List-Archive:** <https://lists.cacert.org/www/arc/cacert>

**List-Help:** <mailto:sympa@lists.cacert.org?subject=help>

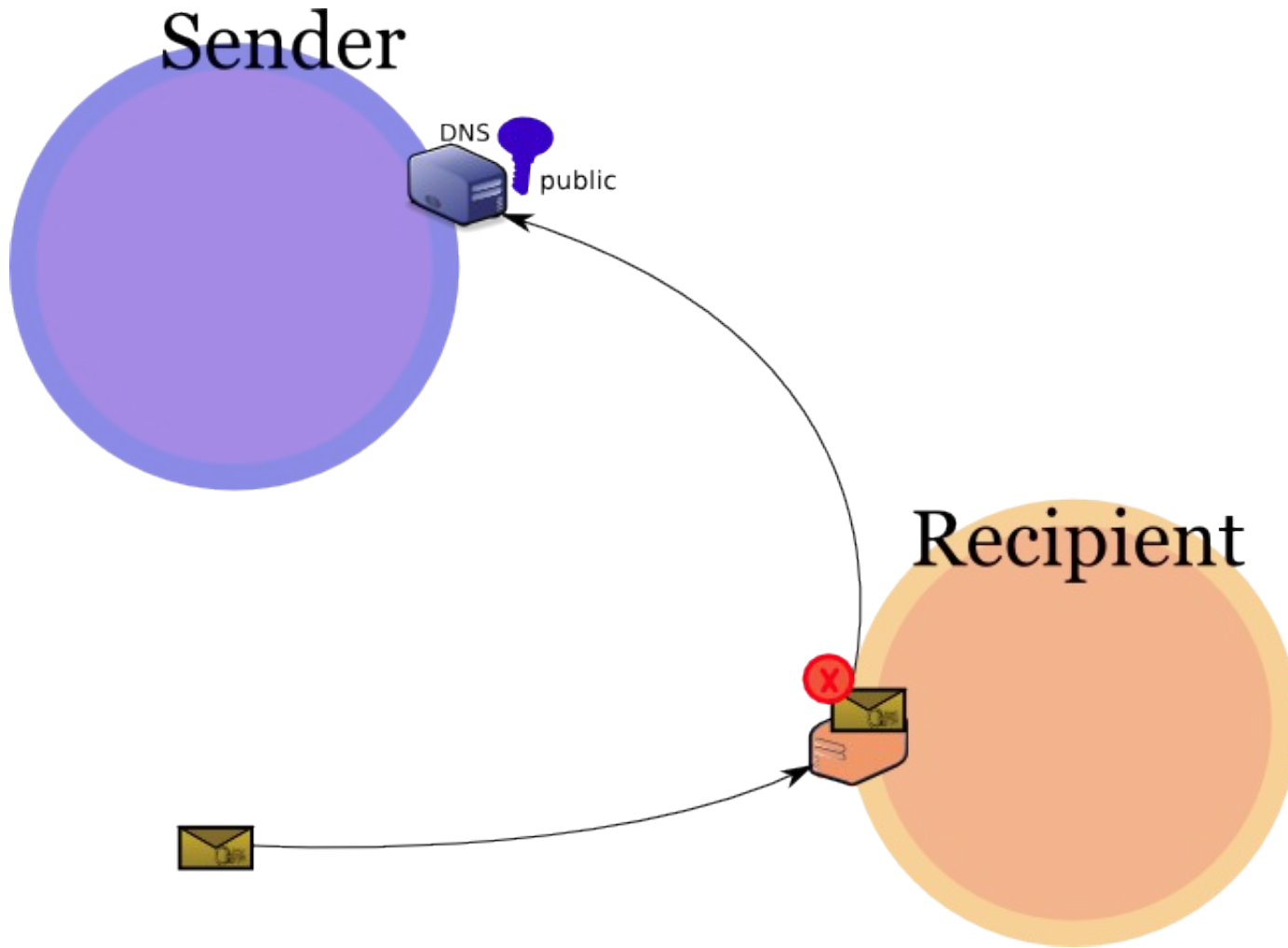
**List-Owner:** <mailto:cacert-request@lists.cacert.org>

**List-Post:** <mailto:cacert@lists.cacert.org>

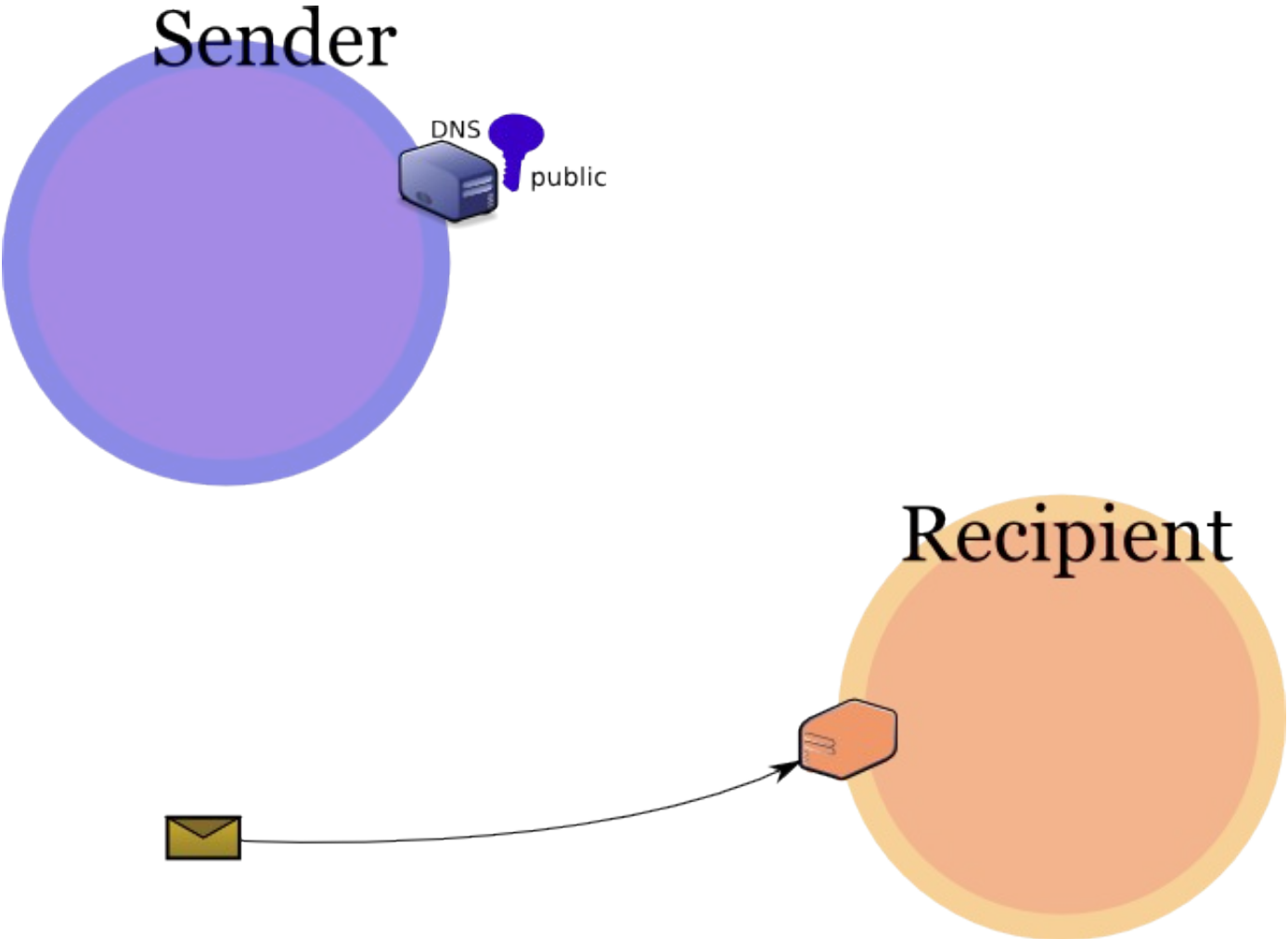
**List-Subscribe:** <mailto:sympa@lists.cacert.org?subject=subscribe%20cacert>

**List-Unsubscribe:** <mailto:sympa@lists.cacert.org?subject=unsubscribe%20cacert>

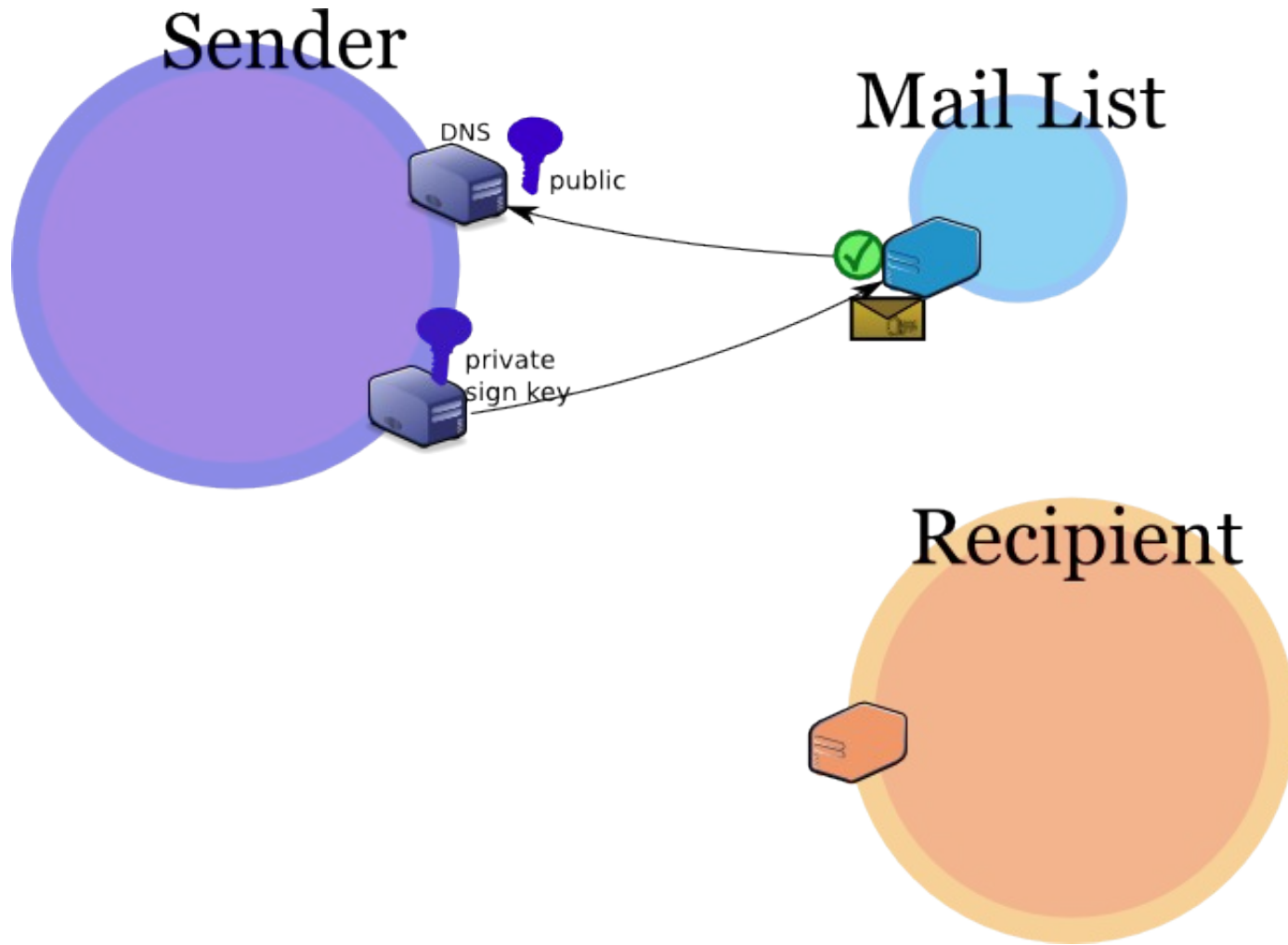
# DKIM Forgeries



# DKIM Unsigned

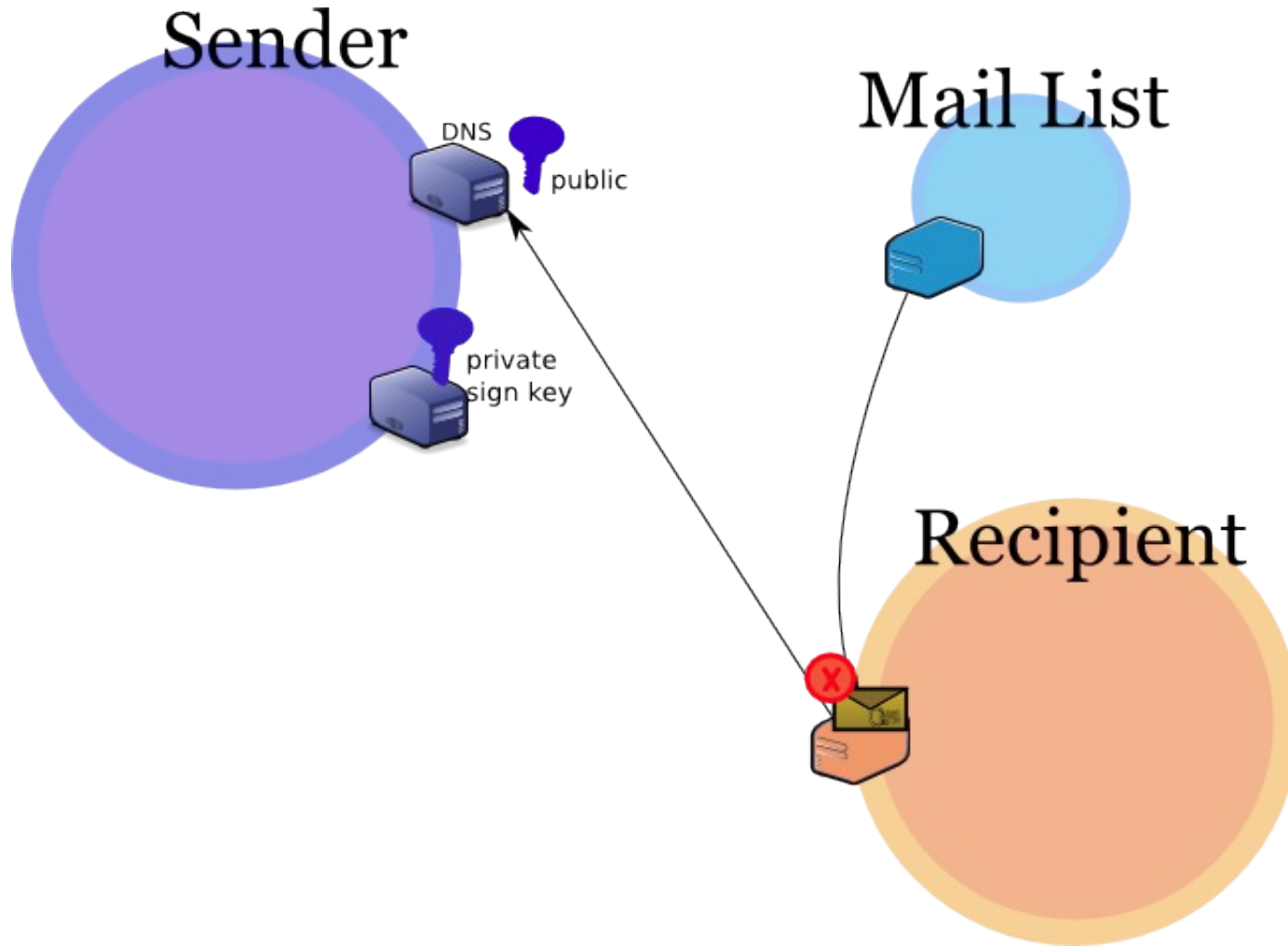


# DKIM Mailing Lists

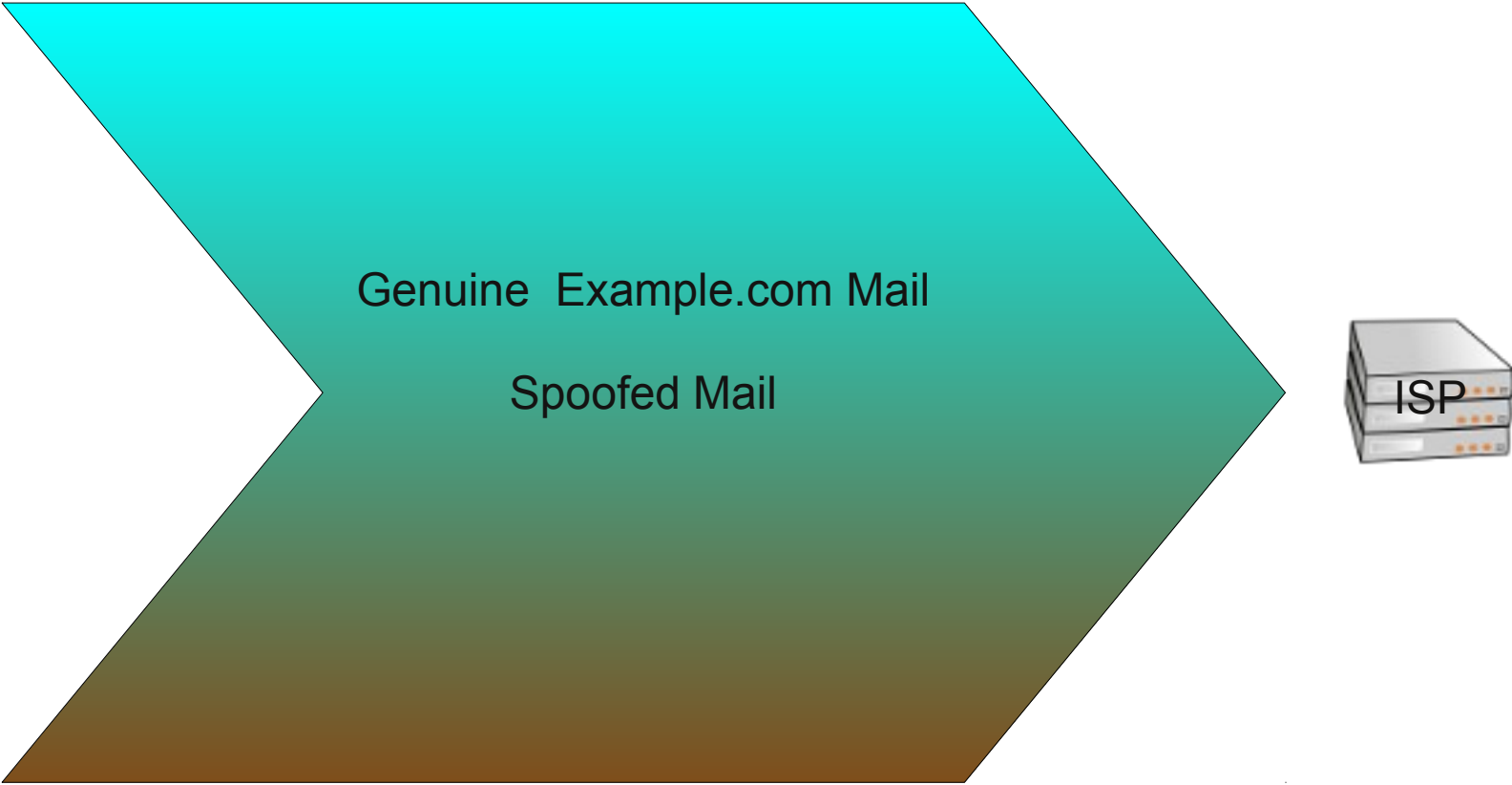




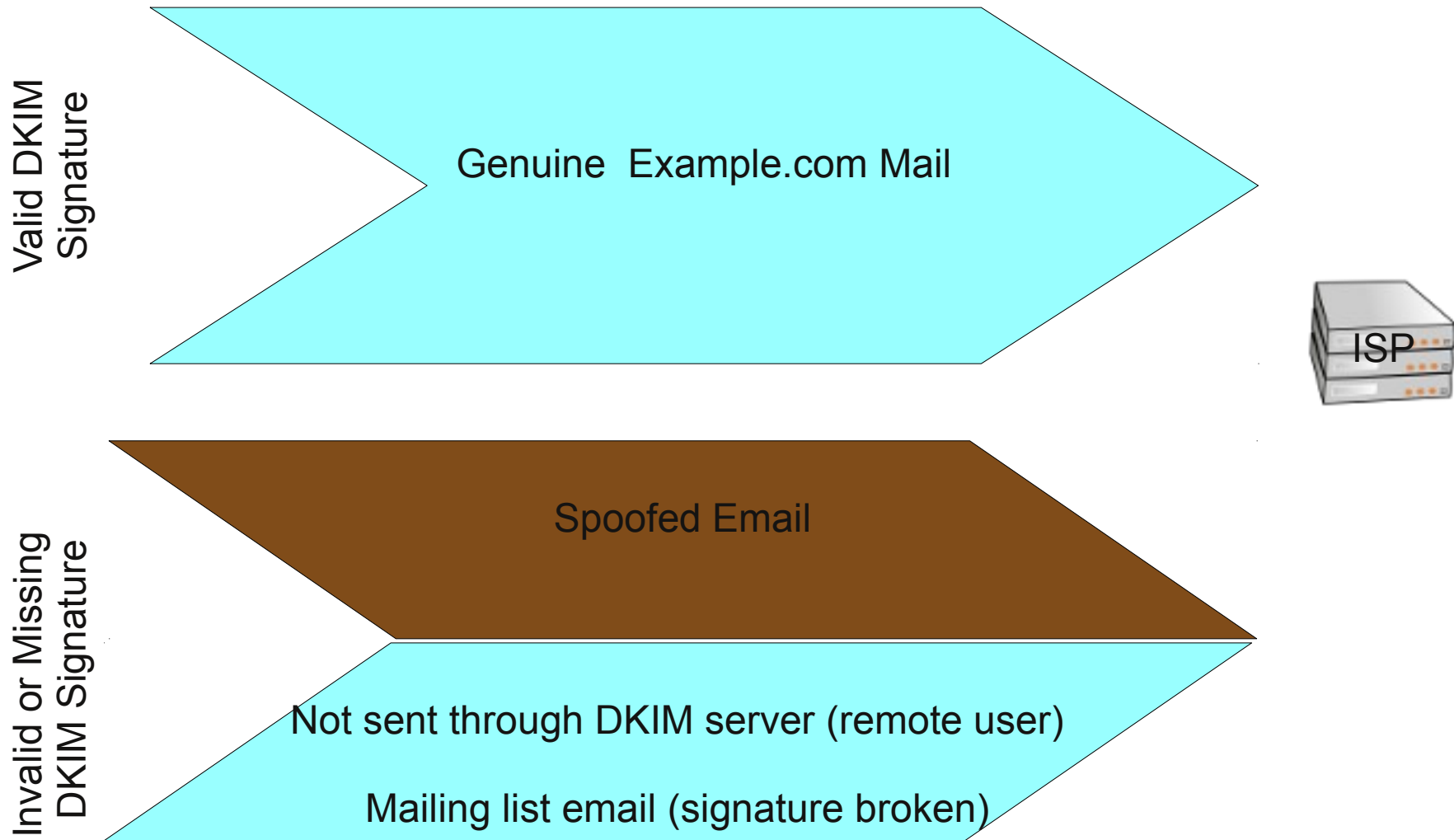
# DKIM Mailing Lists



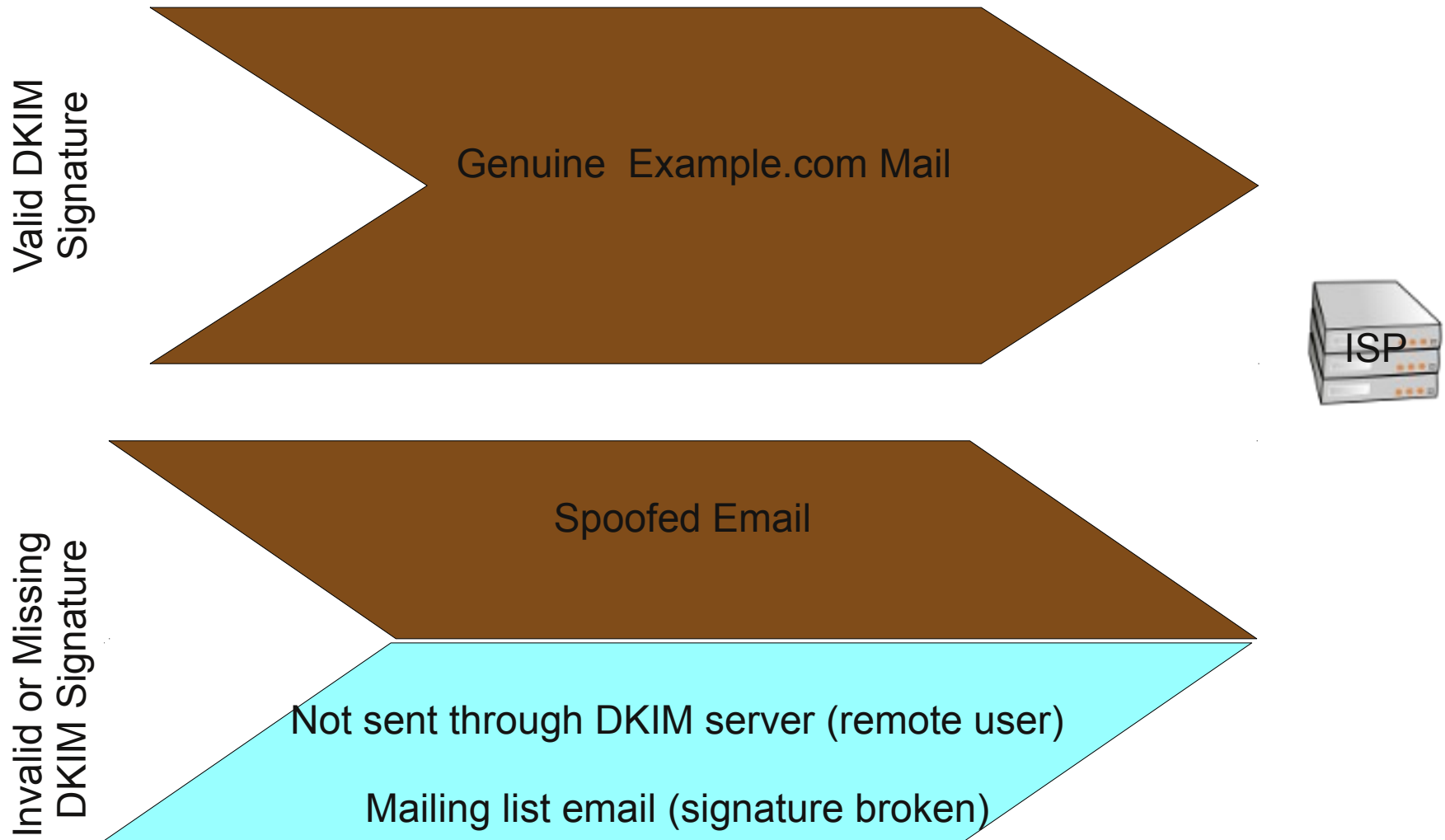
# Example.com email stream - pre-dkim



# Example.com email stream – dkim signed



# Example.com email stream – dkim signed



# ISP.com email streams – dkim signing outbound



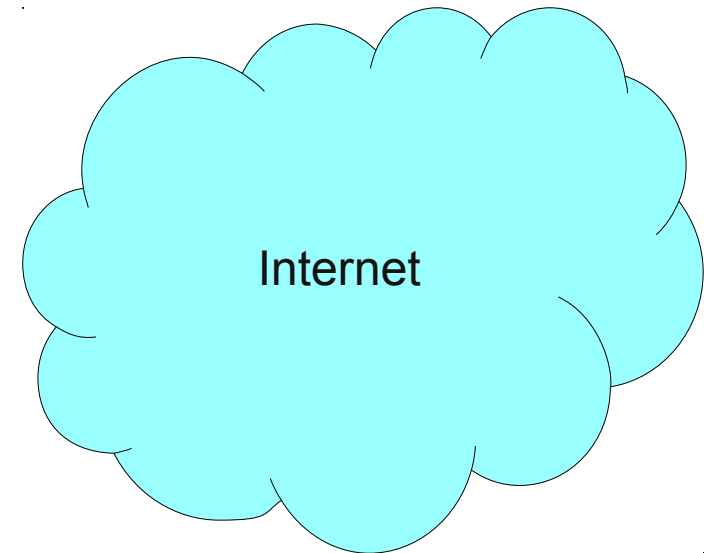
Corporate email  
(d=isp.com)

Billing email  
(d=billing.isp.com)

Marketing email  
(marketing.isp.com)

Customer email  
(d=customer.isp.com)

Customer high-rate email  
(d=high-rate.customer.isp.com)



**FUN FACT:** There are more Yahoo! Mail users around the world than two times the population of Mexico.

## Press Release

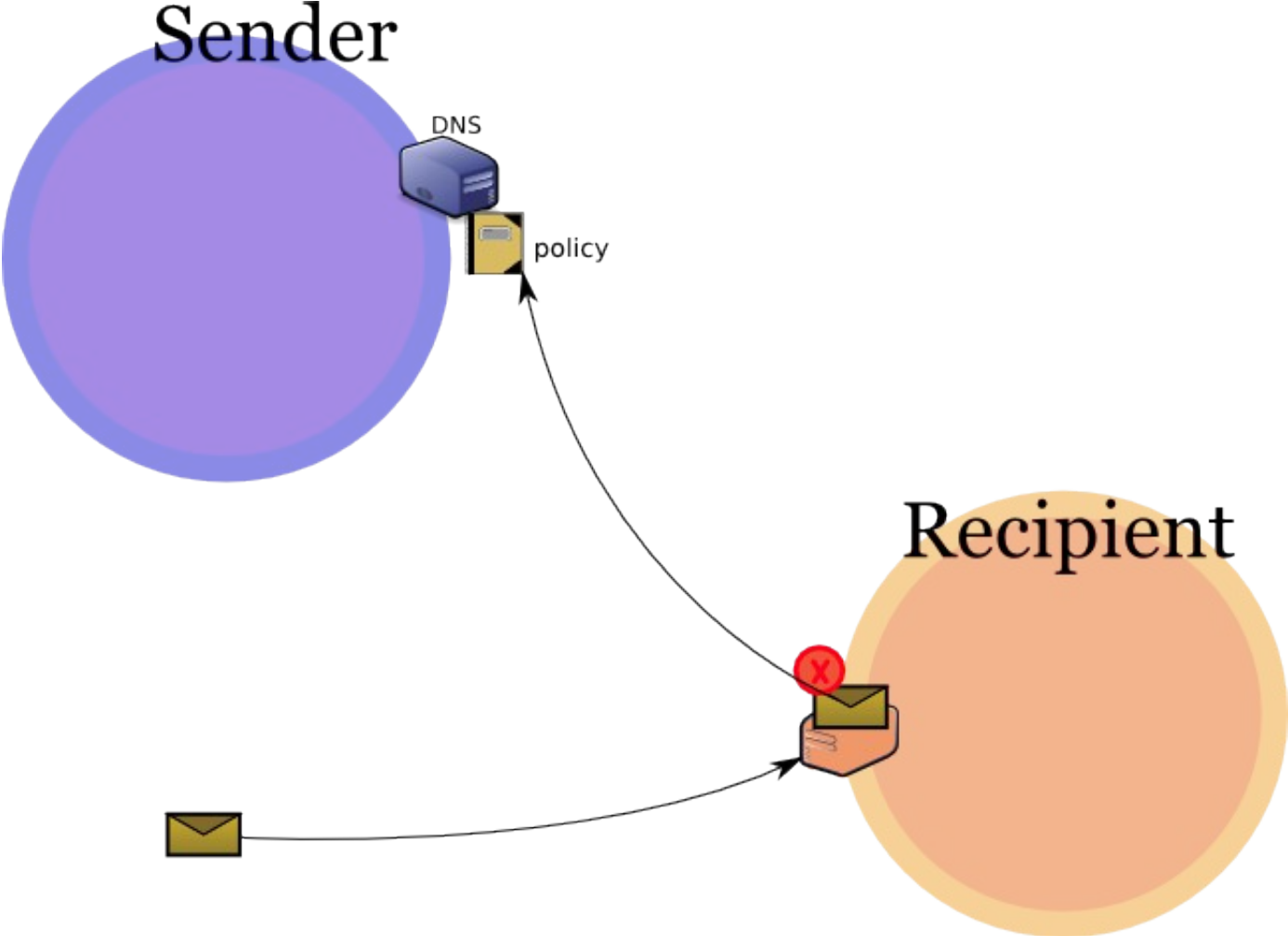
# Yahoo!, eBay and PayPal Join Forces to Protect Consumers Against E-mail Fraud and Phishing Scams

## Yahoo! Mail First to Protect Consumers by Blocking Fraudulent eBay and PayPal E-mail

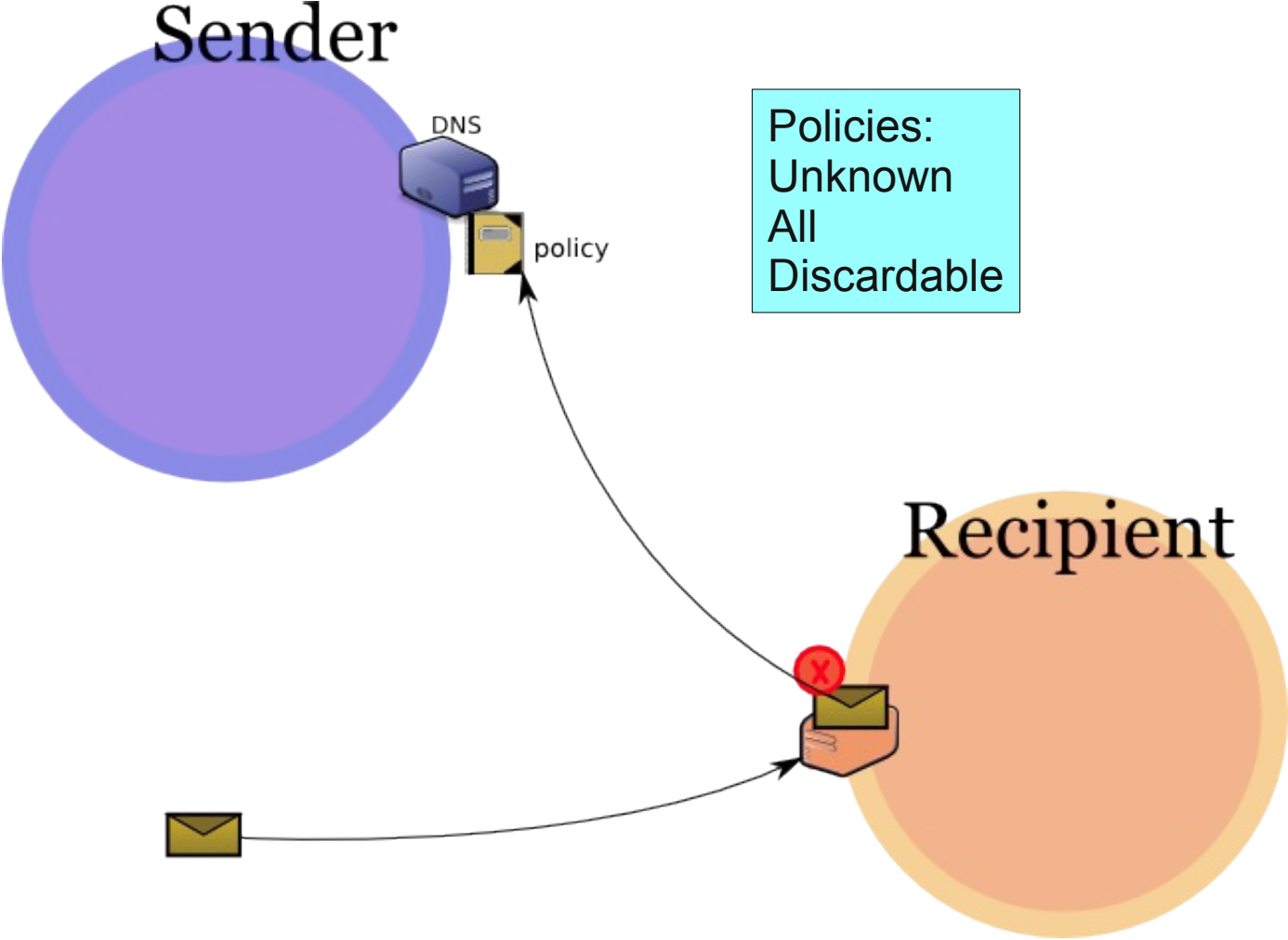
SAN JOSE, Calif. & SUNNYVALE, Calif., Oct 04, 2007 (BUSINESS WIRE) -- Yahoo!, eBay and PayPal today announced a collaborative effort to better protect consumers against fraudulent e-mails and the dangerous scams known as phishing attacks. Starting today, eBay and PayPal customers worldwide using Yahoo! Mail will have a safer e-mail experience - they will begin receiving fewer fake e-mails claiming to be sent by eBay and PayPal. Yahoo! Mail is the first Web mail service to block these types of malicious messages for eBay and PayPal through the use of DomainKeys e-mail authentication technology.

The technology upgrade will be rolled out globally over the next several weeks to all users of Yahoo! Mail.

# Author Domain Signing Practices (ADSP - RFC5617)



# Author Domain Signing Practices (ADSP - RFC5617)



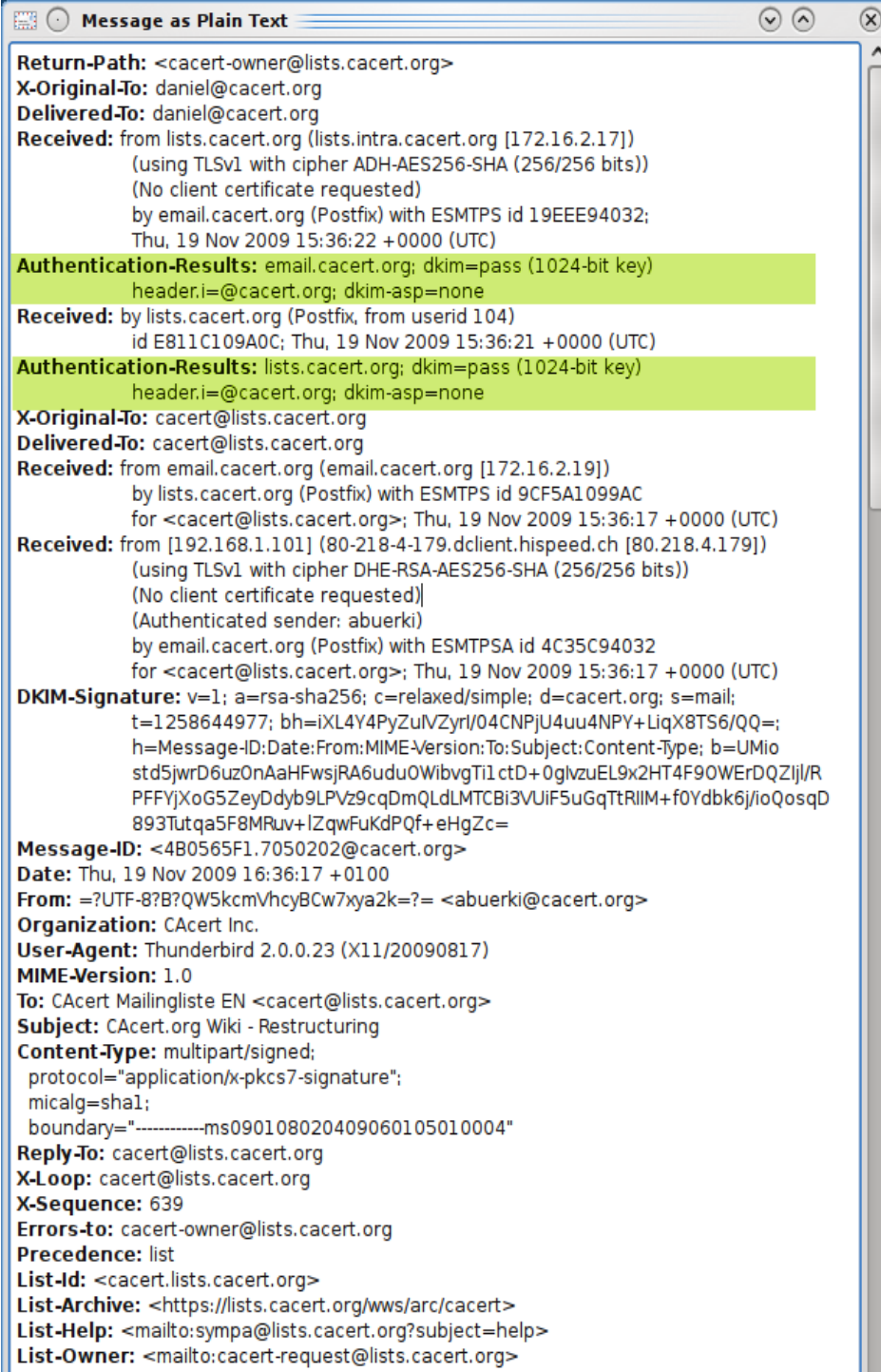


## DKIM (near) Future – Reporting Failures

- Improved DKIM / ADSP failures – reported to author/signing domain  
<http://tools.ietf.org/html/draft-ietf-marf-dkim-reporting-00>
- Feedback loop by standard rather than bilateral arrangements
- Reporting address in DKIM DNS key and/or ADSP DNS policy
- Makes author domain aware of what signature failures are occurring

# DKIM Future – Authenticated Results

- Authenticated-Results:  
RFC5451
- Email clients
- Webmail display and filters
- Allows building of trust chains



Message as Plain Text

**Return-Path:** <cacert-owner@lists.cacert.org>  
**X-Original-To:** daniel@cacert.org  
**Delivered-To:** daniel@cacert.org  
**Received:** from lists.cacert.org (lists.intra.cacert.org [172.16.2.17])  
(using TLSv1 with cipher ADH-AES256-SHA (256/256 bits))  
(No client certificate requested)  
by email.cacert.org (Postfix) with ESMTPS id 19EEE94032;  
Thu, 19 Nov 2009 15:36:22 +0000 (UTC)

**Authentication-Results:** email.cacert.org; dkim=pass (1024-bit key)  
header.i=@cacert.org; dkim-asp=none

**Received:** by lists.cacert.org (Postfix, from userid 104)  
id E811C109A0C; Thu, 19 Nov 2009 15:36:21 +0000 (UTC)

**Authentication-Results:** lists.cacert.org; dkim=pass (1024-bit key)  
header.i=@cacert.org; dkim-asp=none

**X-Original-To:** cacert@lists.cacert.org  
**Delivered-To:** cacert@lists.cacert.org  
**Received:** from email.cacert.org (email.cacert.org [172.16.2.19])  
by lists.cacert.org (Postfix) with ESMTPS id 9CF5A1099AC  
for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)

**Received:** from [192.168.1.101] (80-218-4-179.dclient.hispeed.ch [80.218.4.179])  
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))  
(No client certificate requested)  
(Authenticated sender: abuerki)  
by email.cacert.org (Postfix) with ESMTPSA id 4C35C94032  
for <cacert@lists.cacert.org>; Thu, 19 Nov 2009 15:36:17 +0000 (UTC)

**DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail;  
t=1258644977; bh=iXL4Y4PyZuIVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;  
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio  
std5jwrD6uz0nAaHFwsjRA6udu0WibvgT1ctD+0glvzuEL9x2HT4F90WErDQZijl/R  
PFfYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTcBi3VUif5uGqTtRIIM+f0Ydbk6j/foQosqD  
893Tutqa5F8MRuv+lZqwFuKdPQf+eHgZc=

**Message-ID:** <4B0565F1.7050202@cacert.org>  
**Date:** Thu, 19 Nov 2009 16:36:17 +0100  
**From:** =?UTF-8?B?QW5kcmlVhcyBCw7xya2k=?= <abuerki@cacert.org>  
**Organization:** CAcert Inc.  
**User-Agent:** Thunderbird 2.0.0.23 (X11/20090817)  
**MIME-Version:** 1.0  
**To:** CAcert Mailingliste EN <cacert@lists.cacert.org>  
**Subject:** CAcert.org Wiki - Restructuring  
**Content-Type:** multipart/signed;  
protocol="application/x-pkcs7-signature";  
micalg=sha1;  
boundary="-----ms090108020409060105010004"

**Reply-To:** cacert@lists.cacert.org  
**X-Loop:** cacert@lists.cacert.org  
**X-Sequence:** 639  
**Errors-to:** cacert-owner@lists.cacert.org  
**Precedence:** list  
**List-Id:** <cacert.lists.cacert.org>  
**List-Archive:** <https://lists.cacert.org/www/arc/cacert>  
**List-Help:** <mailto:sympa@lists.cacert.org?subject=help>  
**List-Owner:** <mailto:cacert-request@lists.cacert.org>

# DKIM Future - Reputation

- DKIM Reputation
- <http://www.dkim-reputation.org/>
  
- Lookup of domain reputation based on DKIM
- (NEW) Non-IETF Working group - domain rep  
<http://www.ietf.org/mail-archive/web/domainrep/>

# DKIM Future – Mailing List Managers

Danger Work in progress:

<http://tools.ietf.org/html/draft-ietf-dkim-mailinglists-02>

Mailing List Operator:

- Guidance for DKIM/ADSP handling
- Guidance for DKIM signing

Recipient:

- Guidance for verification
- Guidance for Feedback loops with DKIM

# DKIM Future - You

## Deploy DKIM Signing

- Stream based

## Deploy DKIM verification Filtering

- Use DKIM verification to guide filtering
- Local arrangements to protect important business relationships

## Feedback Loops

- DKIM reporting draft

## Mailing Lists

- Draft RFC move to DKIM-Friendly lists

## Authenticated Results

- Webmail enhancements

# DKIM Future - You

IETF

- Participation welcome – (mailing list + meetings)
- Statistics on DKIM signatures
- Operational Experience desired

Interested? See: [Http://tools.ietf.org/wg/dkim](http://tools.ietf.org/wg/dkim)

## **Questions? And Thanks**

Thanks:

### **OVEE and OpenDKIM**

- IETF DKIM working group – for working out standards
- Product Developers – chance to reduce email spoofing
- Murray S. Kucherawy – for OpenDKIM
  
- Gimp / Inkscape /OpenOffice developers good tools
- Creative Commons Licencing for ease of reuse
- APNIC – for the opportunity to talk
- YOU for your interest

Questions?

## DKIM References

- DKIM Standards <http://tools.ietf.org/wg/dkim>
- Feedback and reporting: <http://tools.ietf.org/wg/marf/>
- Authenticated Results RFC 5451
  
- Training Videos <http://www.maawg.org/activities/training>
  
- Me [daniel.black@ovee.com.au](mailto:daniel.black@ovee.com.au)



## Presentation Credits and Licensing

Niels Heidenreich - SpamInbox - Flickr - <http://www.flickr.com/photos/schoschie/2225345267/>



Vino Family – Stool – Flickr - <http://www.flickr.com/photos/vinofamily/4094653647/>



Vino Family – Stool – Flickr - <http://www.flickr.com/photos/vinofamily/4095412074/>



Brenda Star – Old Key – Flickr - <http://www.flickr.com/photos/brenda-starr/3466560105/>



Walknboston – Car Keys – Flickr - <http://www.flickr.com/photos/walkn/3041590472/>



James Hammer – Signature – Flickr - <http://www.flickr.com/photos/hammer51012/3012413440/>



John Loo – Licence – Flickr - <http://www.flickr.com/photos/johnloo/3518552653/>



Uzwards – Snail Mail - Flickr - <http://www.flickr.com/photos/uzwards/2481348414/>



Various – Diagram Clipart - Open ClipArt - <http://www.openclipart.org/>



Daniel Black – All other diagrams and screenshots

