Practical DKIM Deployment (for Mail Service Providers)

Daniel Black

OVEE Systems Consultancy

EMail Volume

EMail Volume

EMail Volume

Email Filtering – first cut

IP Reputation Filtering

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
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

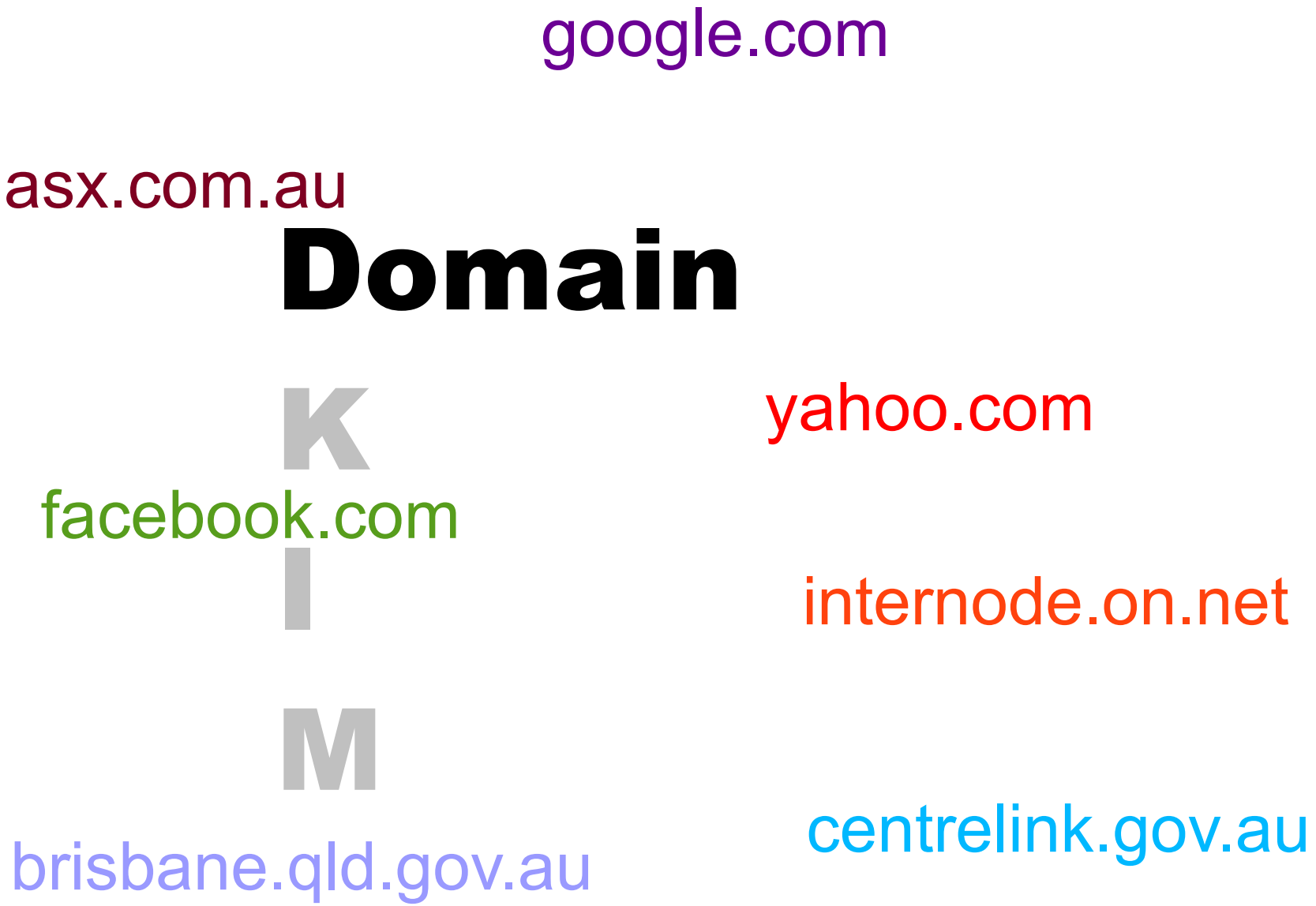
IPv6??

Email Filtering

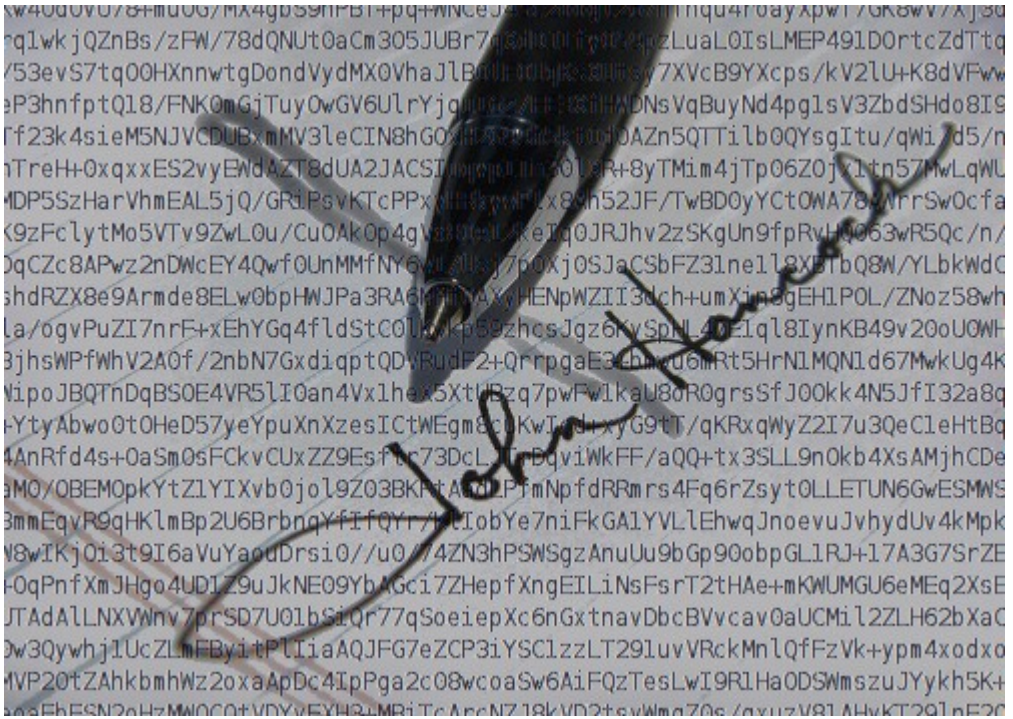
Domain Reputation Filtering

Without forgery

Domain Keys Identified Mail


google.com
asx.com.au
Domain
K
yahoo.com
facebook.com
I
internode.on.net
M
centrelink.gov.au
brisbane.qld.gov.au

Domain Keys I M



Domain Keys Identified M

centrelink.gov.au

asx.com.au

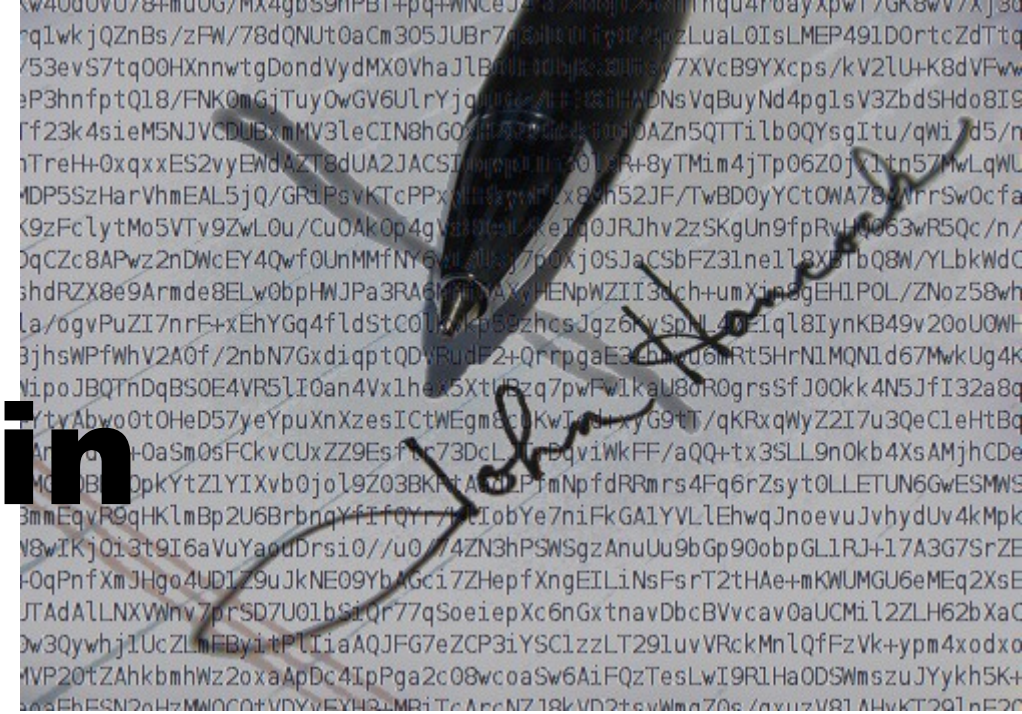
google.com

brisbane.qld.gov.au

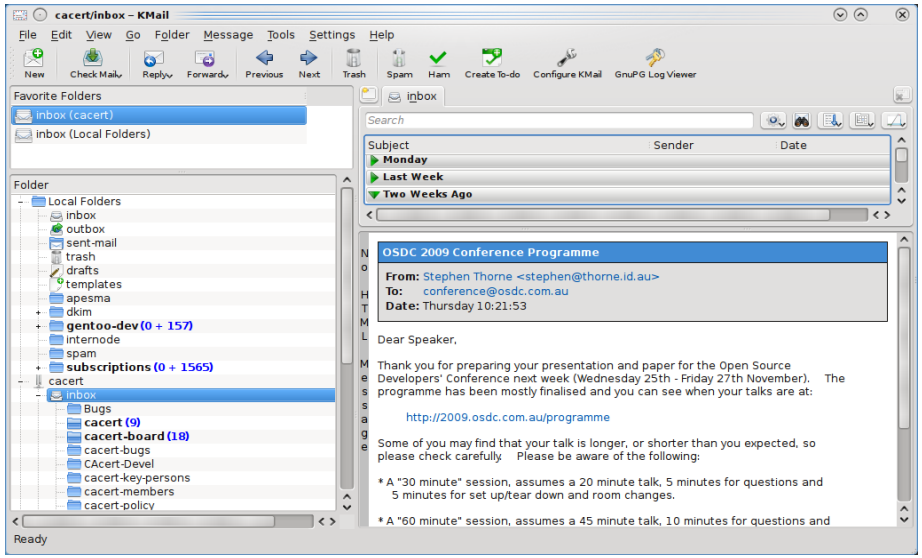
yahoo.com

facebook.com

internode.on.net



Domain Keys Identified Mail

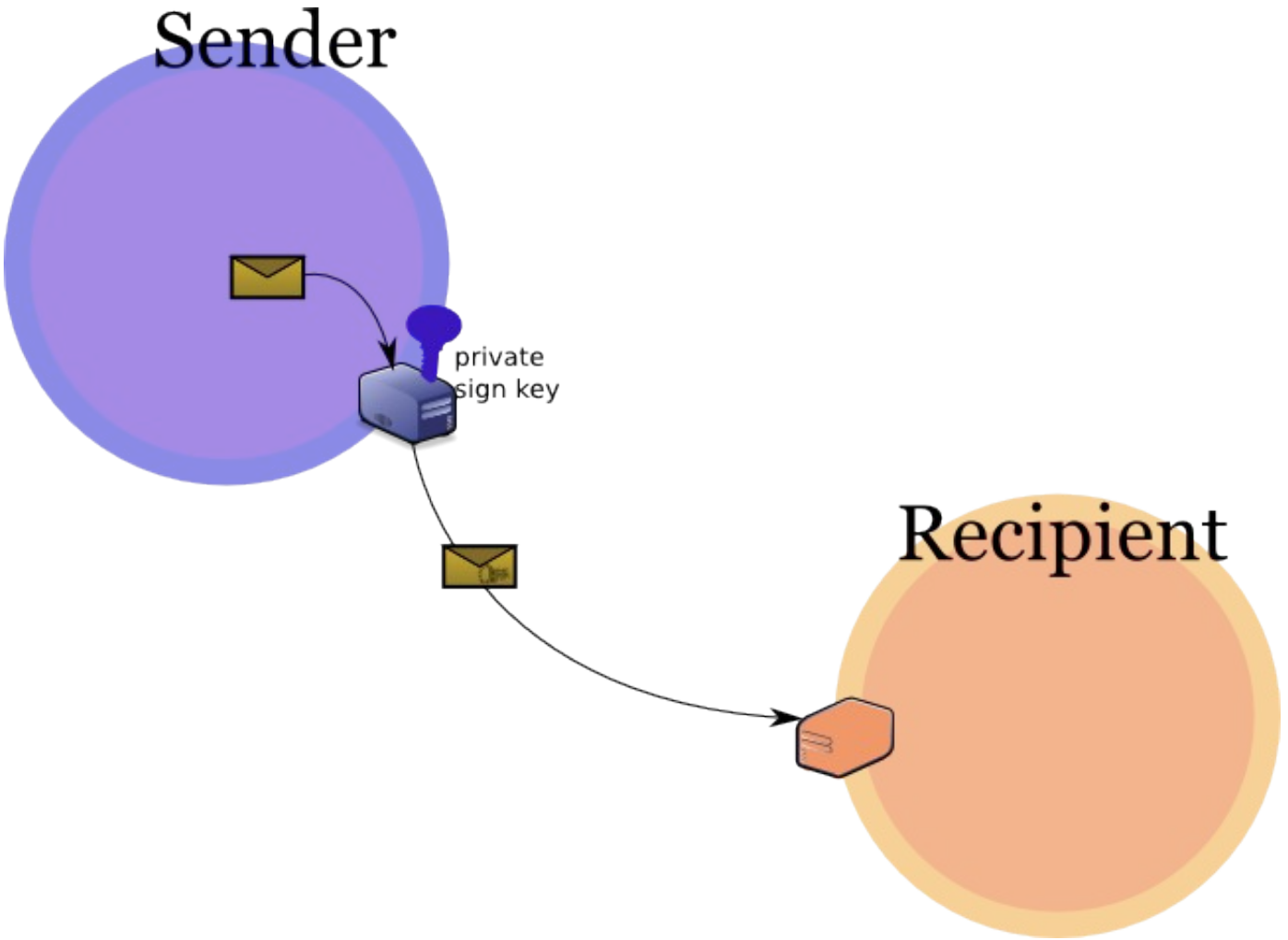


Draft 4871bis

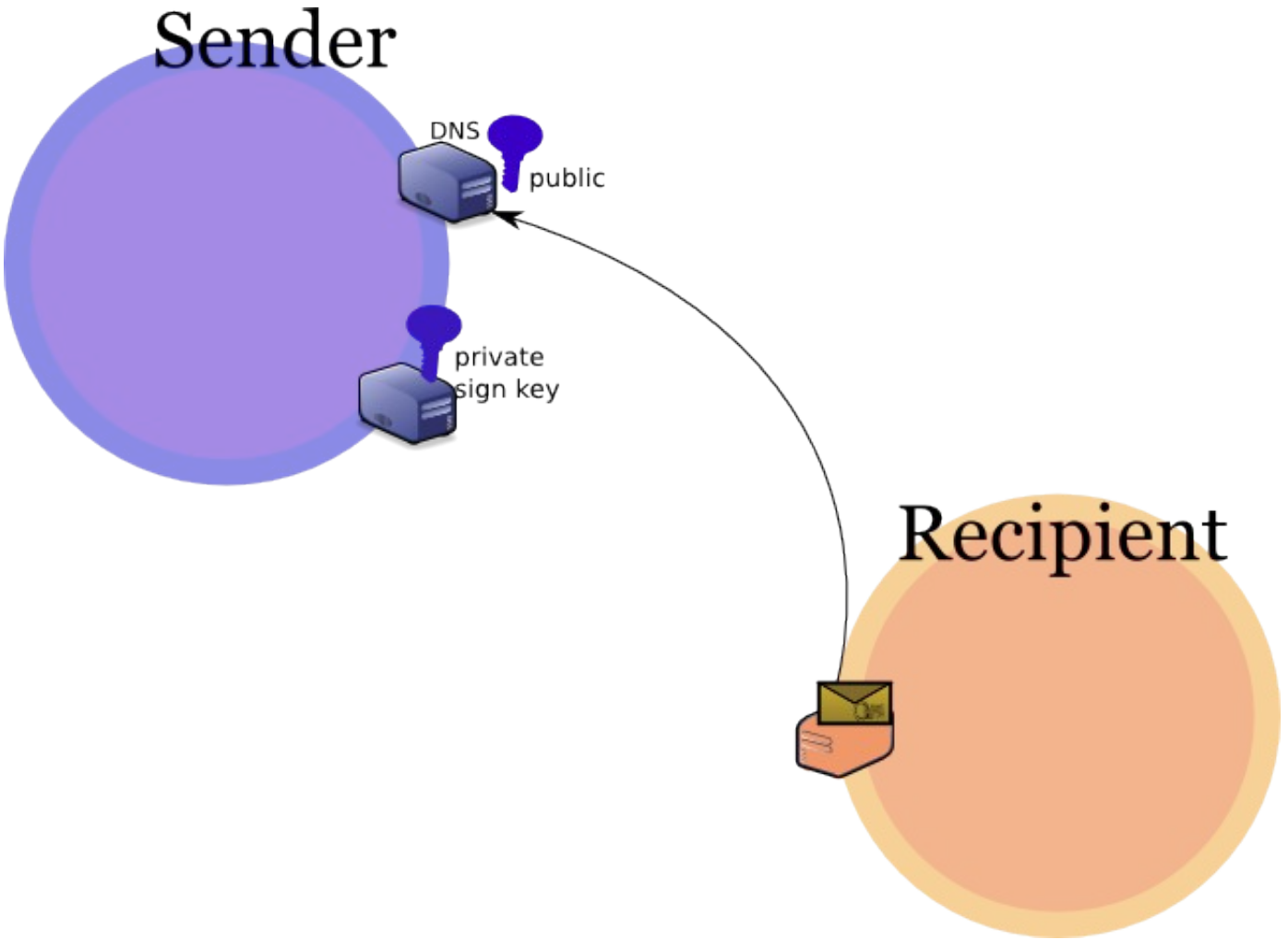
“**Assertion of responsibility** is validated through a cryptographic signature and querying the signer's domain”

Wording update of:
RFC4871 DomainKeys Identified Mail (DKIM) Signatures
February 2007

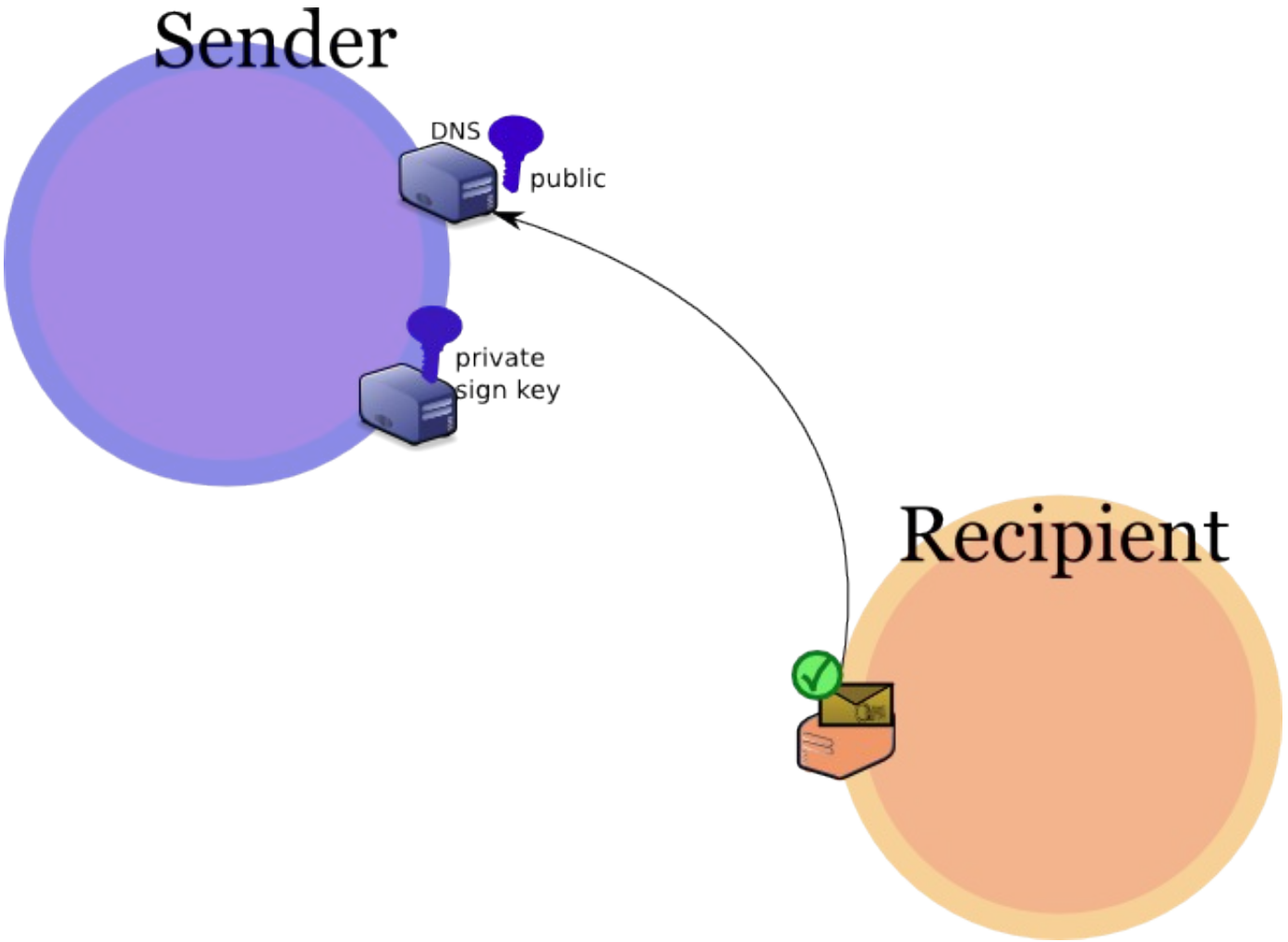
DKIM Architecture



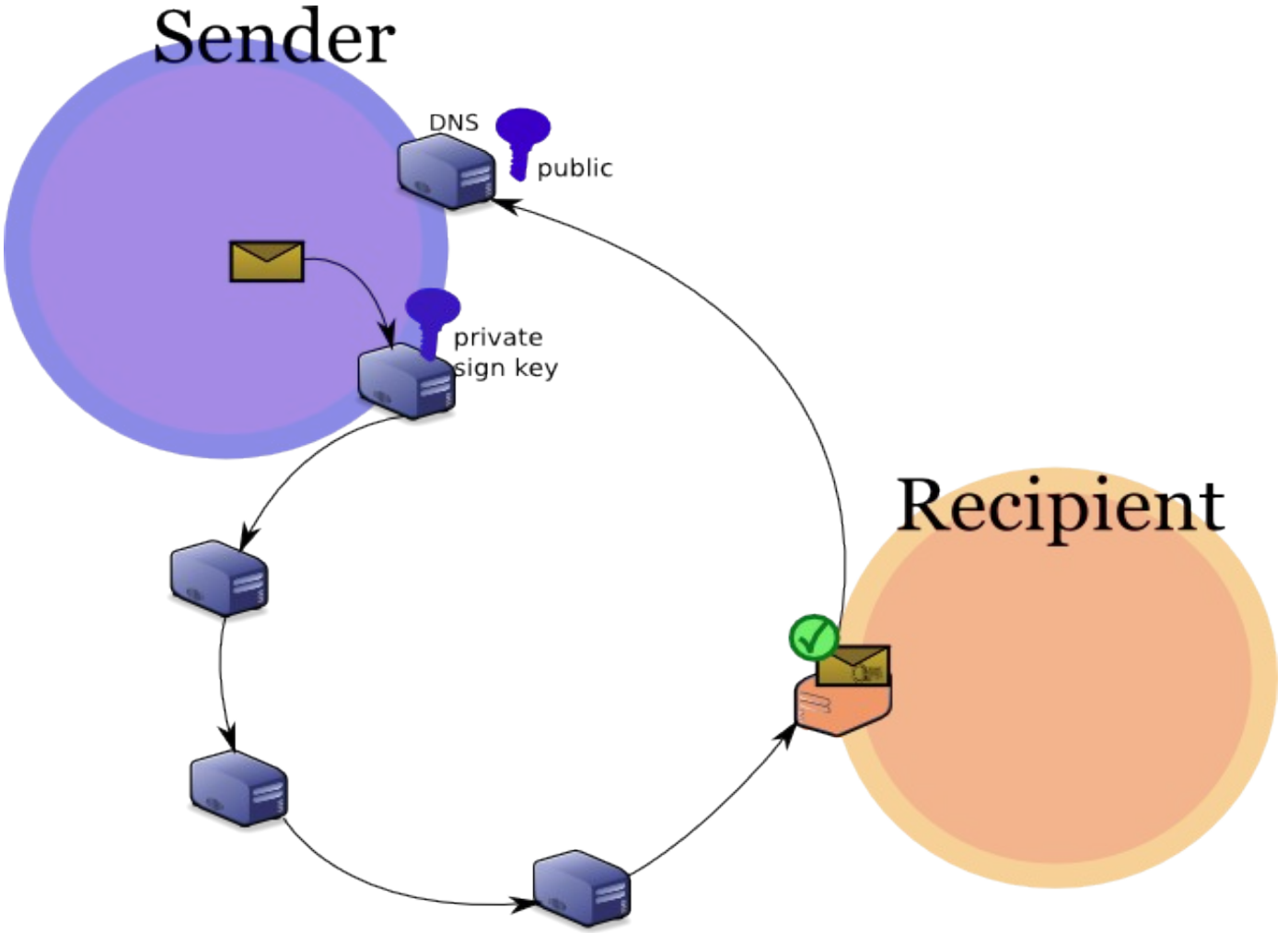
DKIM Architecture



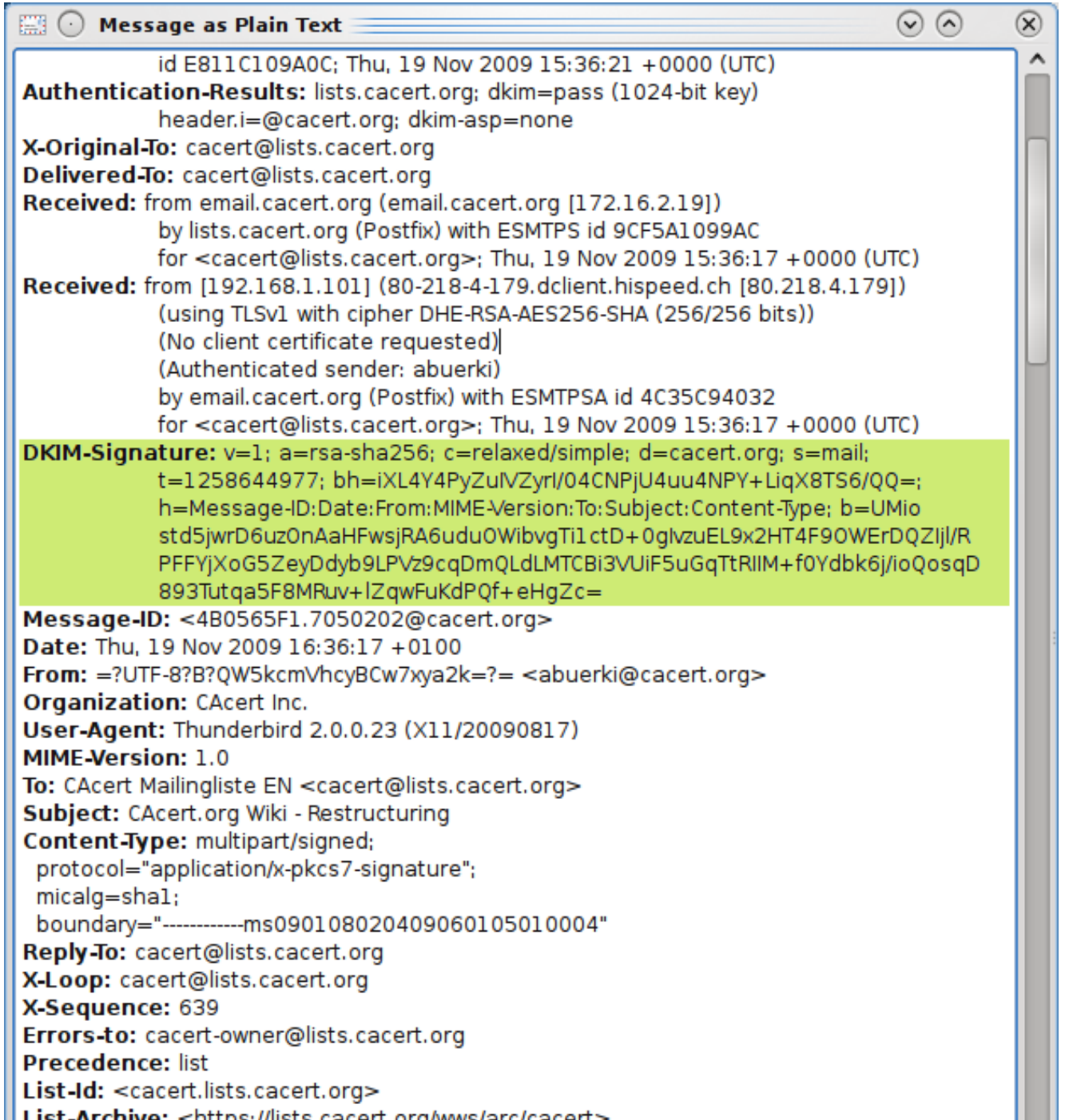
DKIM Architecture



DKIM Content and not path



DKIM Signature



DKIM Signature – selector + domain = key

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail;
t=1258644977; bh=iXL4Y4PyZulVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio
std5jwrD6uz0nAaHFwsjRA6udu0WibvgTi1ctD+0glvzuEL9x2HT4F90WErDQZIjl/R
PFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTCBi3VUiF5uGqTtRIlM+f0Ydbk6j/ioQosqD
893Tutqa5F8MRuv+lZqwFuKdPQf+eHgZc=

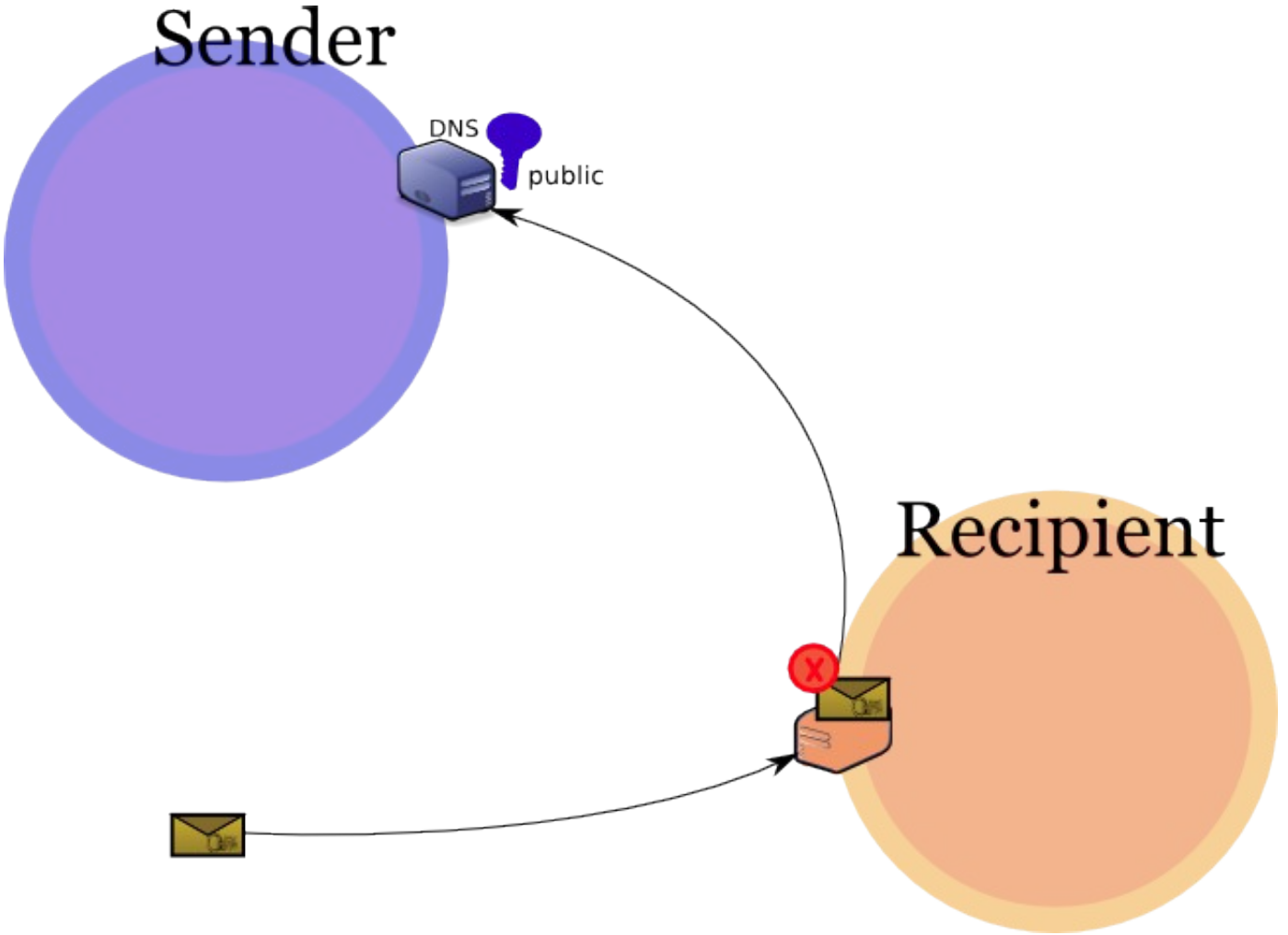
```
mail._domainkey.cacert.org  IN TXT "v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4G
```

DKIM Signature - headers

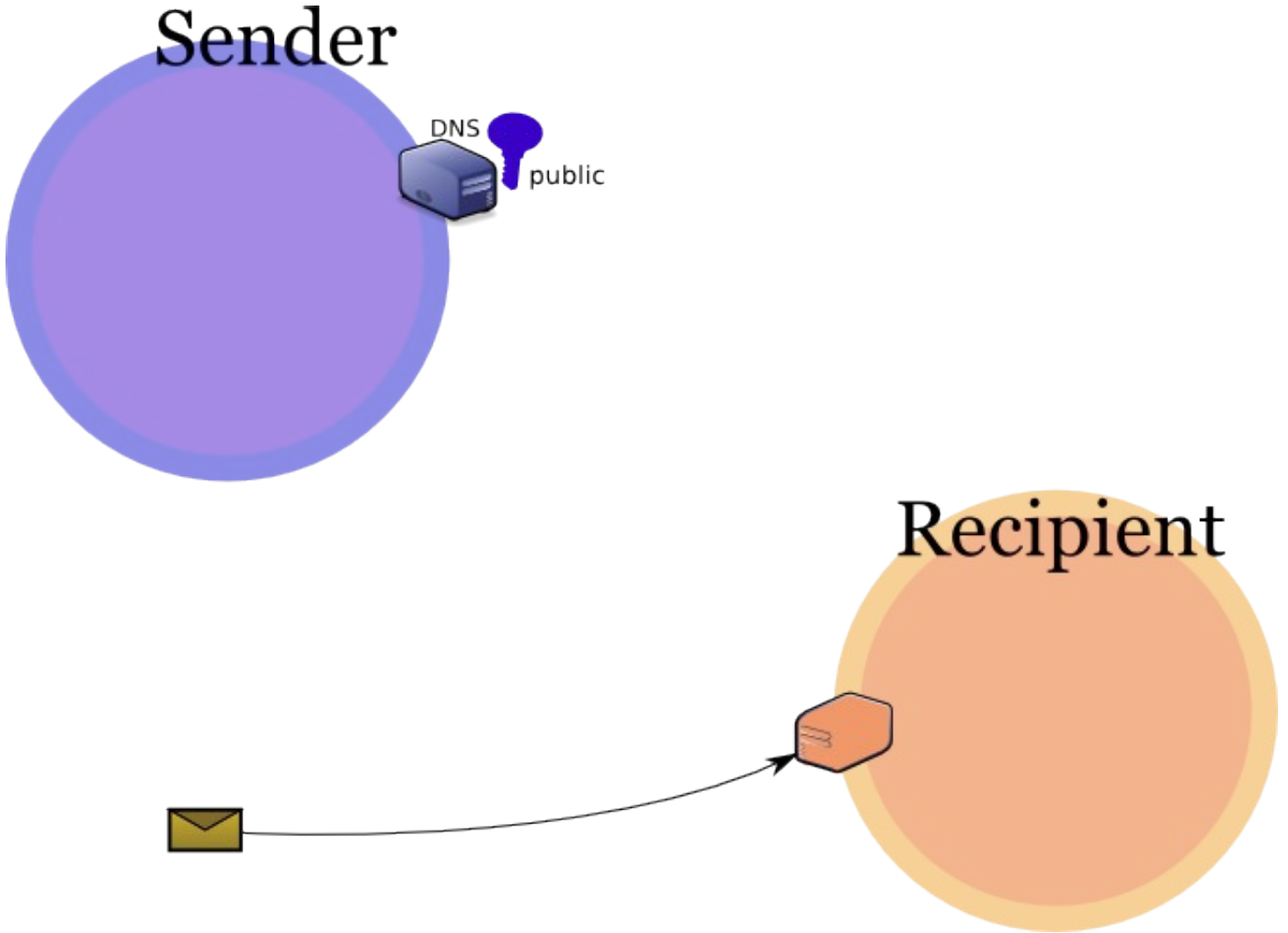
nature: v=1; a=rsa-sha256; c=relaxed/simple; d=cacert.org; s=mail;
t=1258644977; bh=iXL4Y4PyZulVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio
std5jwrD6uz0nAaHFwsjRA6udu0WibvgTi1ctD+0glvzuEL9x2HT4F90WErDQZIjl/R
PFFYjXoG5ZeyDdyb9LPVz9cqDmQLdLMTCBi3VUiF5uGqTtRIIM+f0Ydbk6j/ioQosq
893Tutqa5F8MRuv+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=iXL4Y4PyZulVZyrl/04CNPjU4uu4NPY+LiqX8TS6/QQ=;
h=Message-ID:Date:From:MIME-Version:To:Subject:Content-Type; b=UMio
std5jwrD6uz0nAaHFwsjRA6udu0WibvgTi1ctD+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/wws/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>

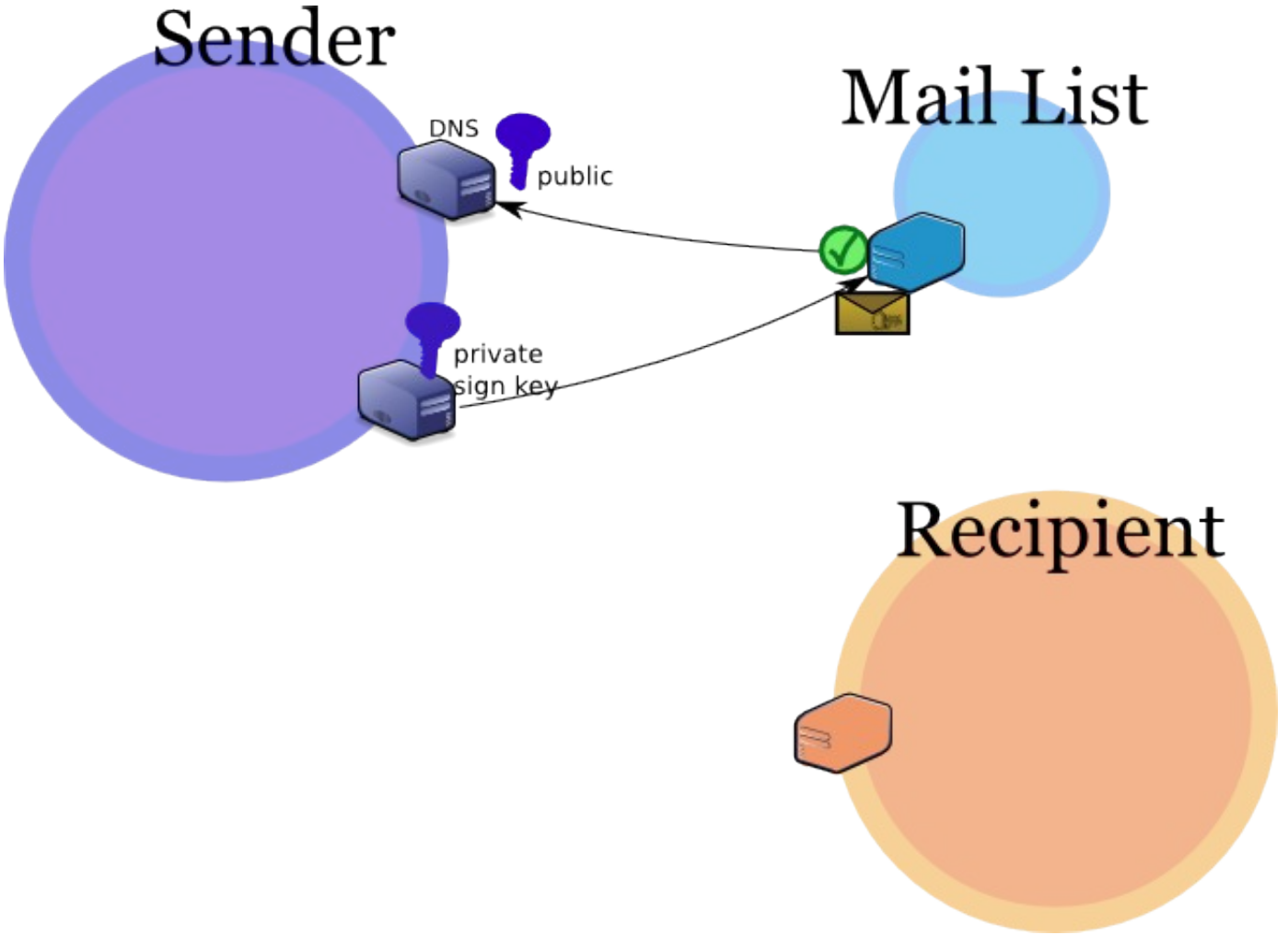
DKIM Forgeries



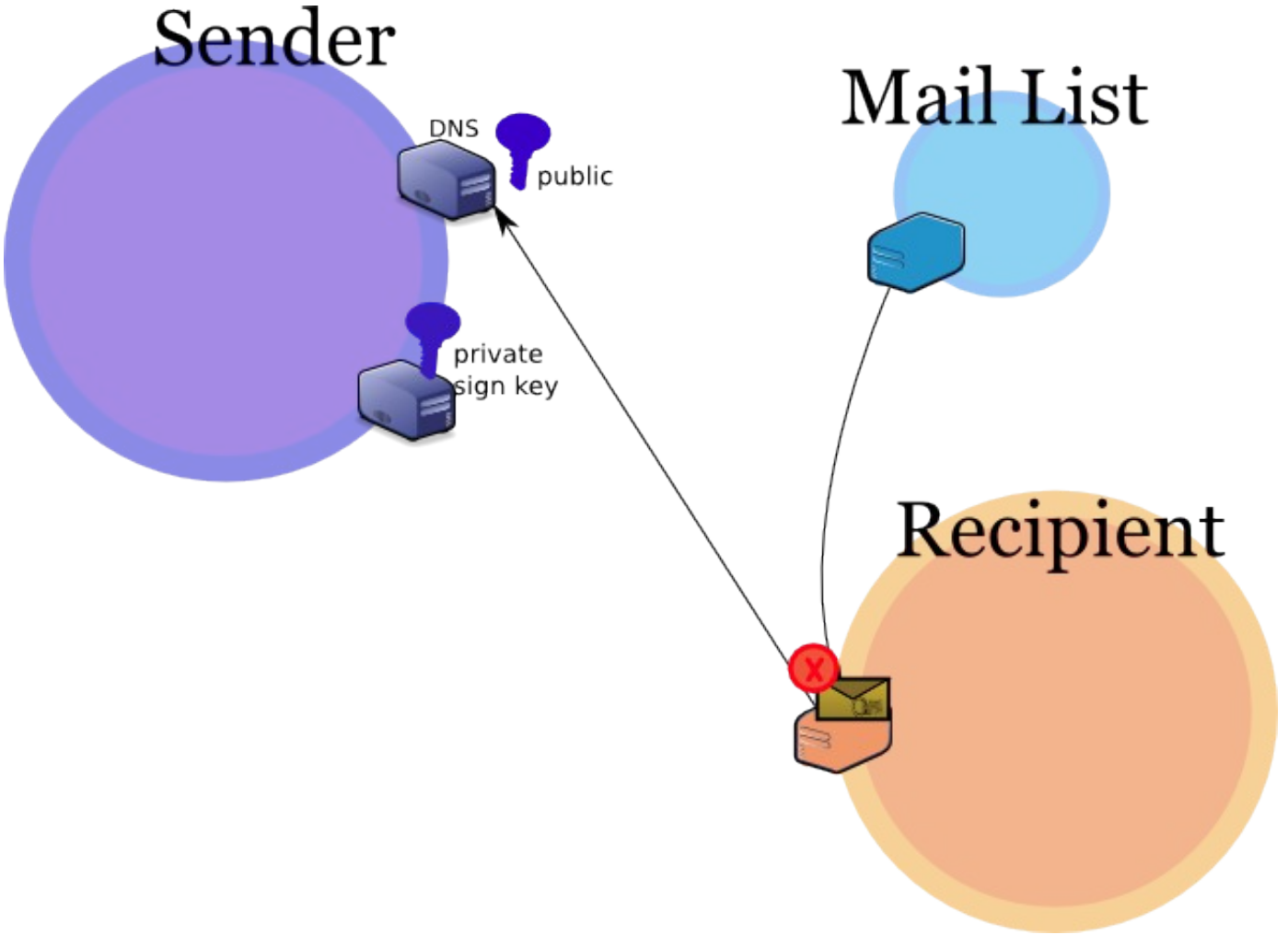
DKIM Unsigned



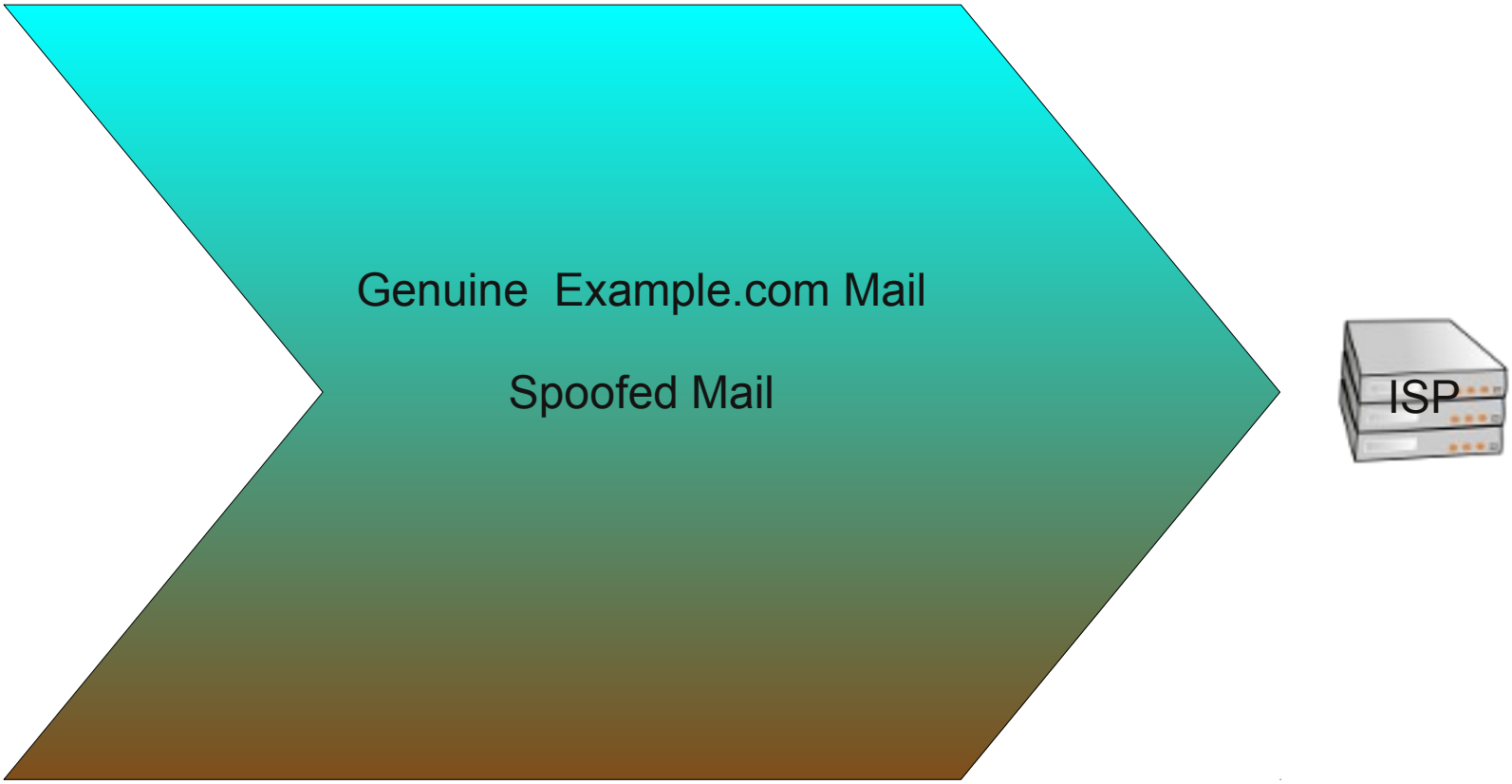
DKIM Mailing Lists



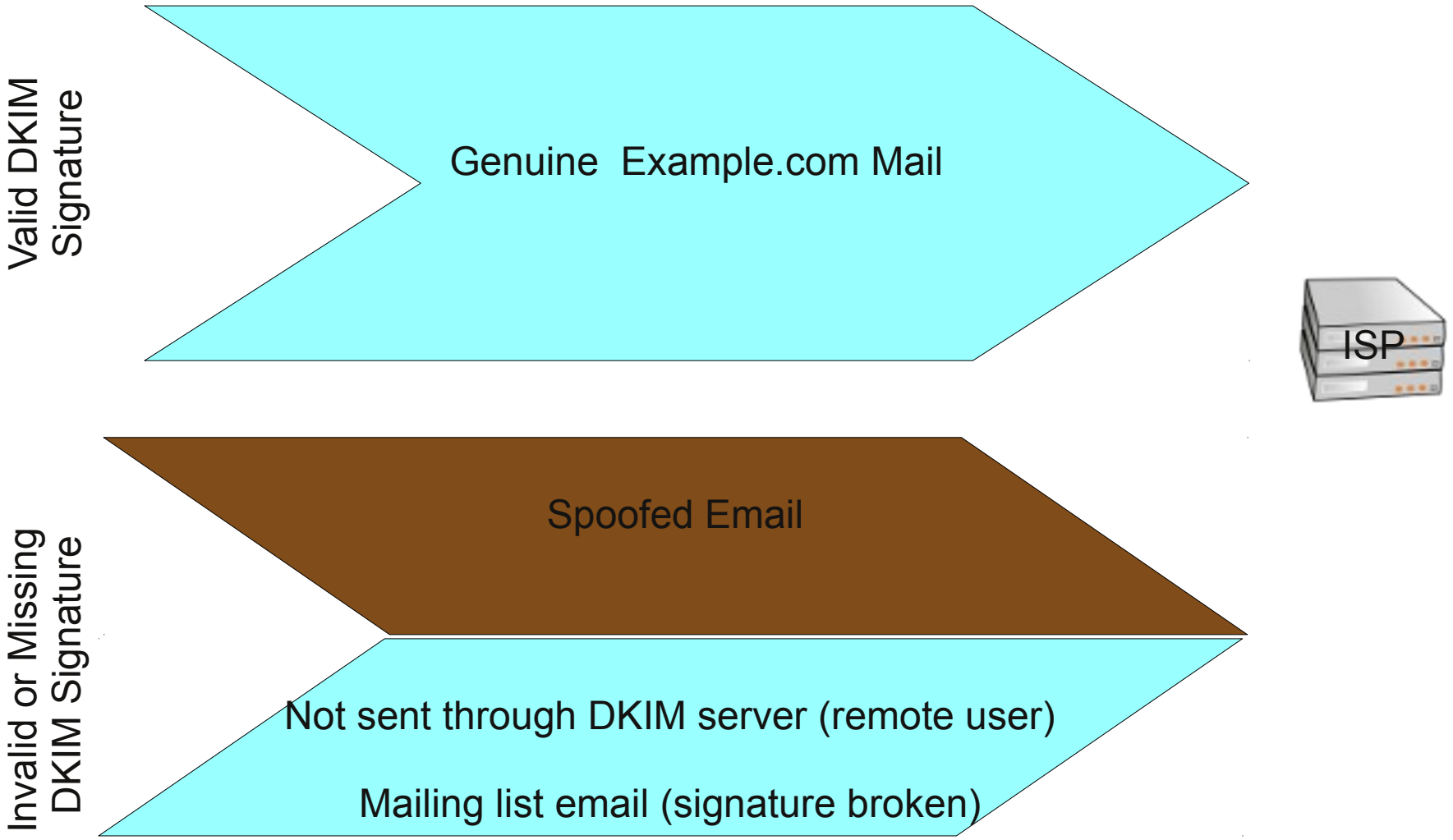
DKIM Mailing Lists



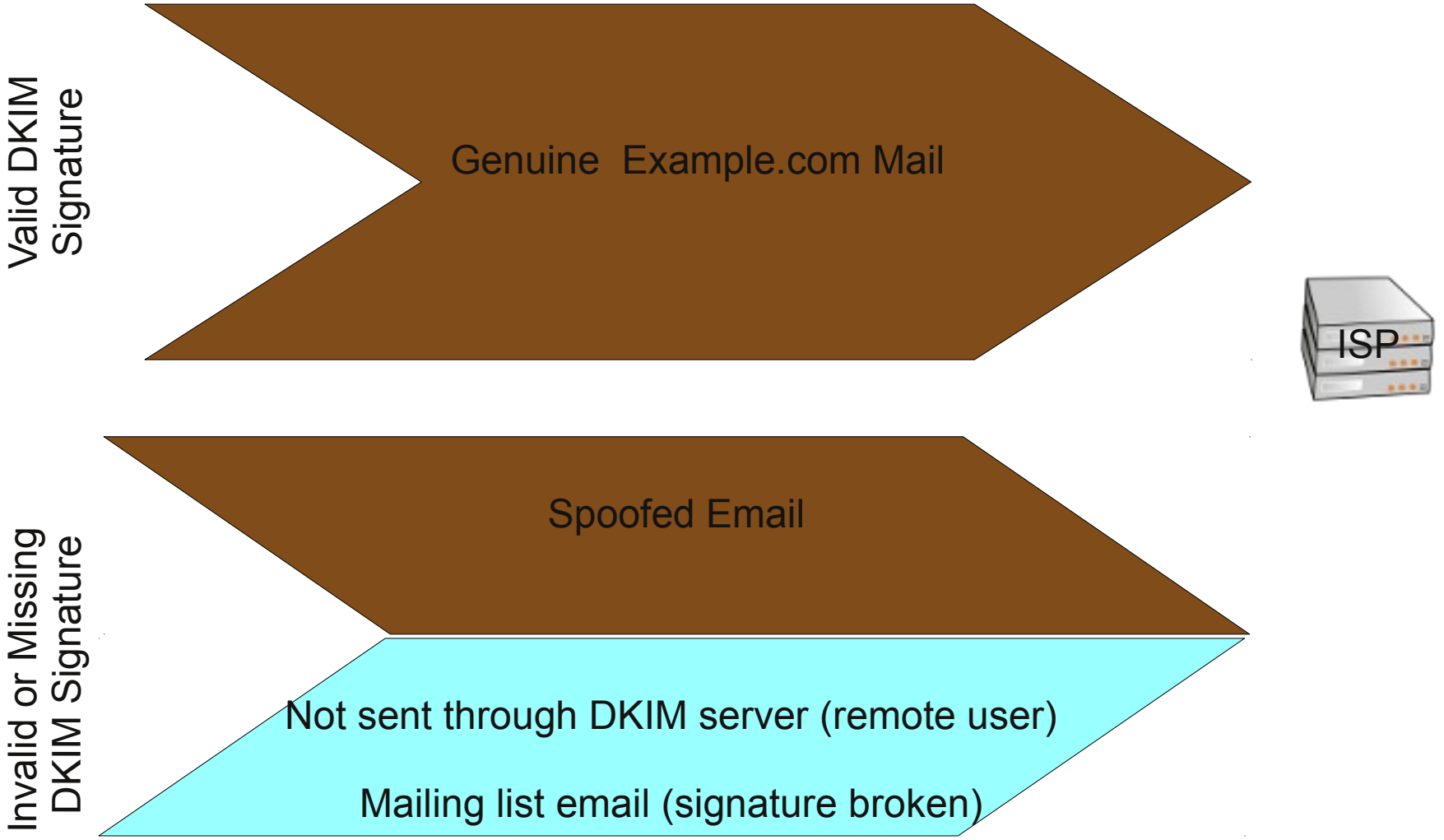
Example.com email stream - pre-dkim



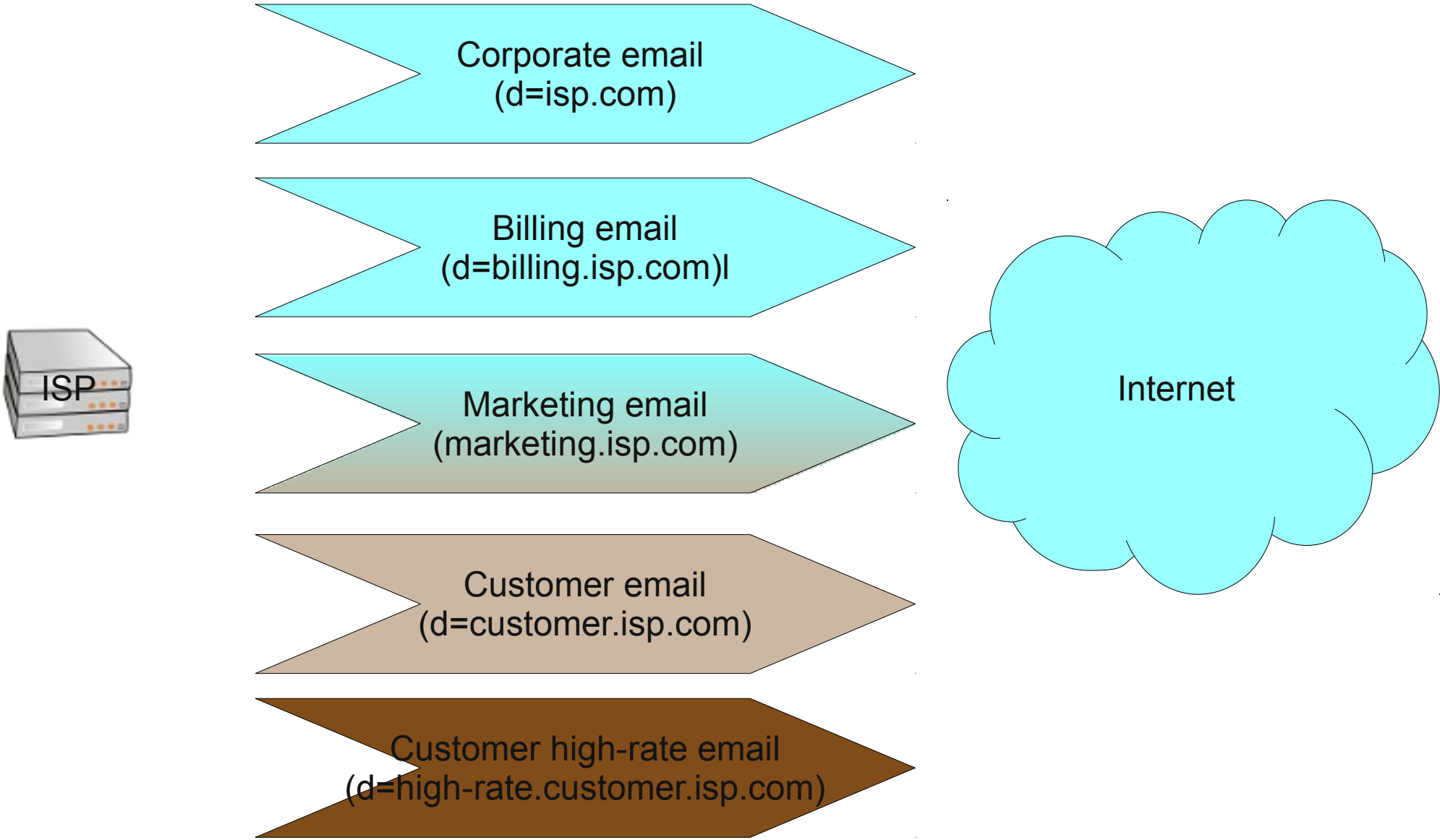
Example.com email stream – dkim signed



Example.com email stream – dkim signed

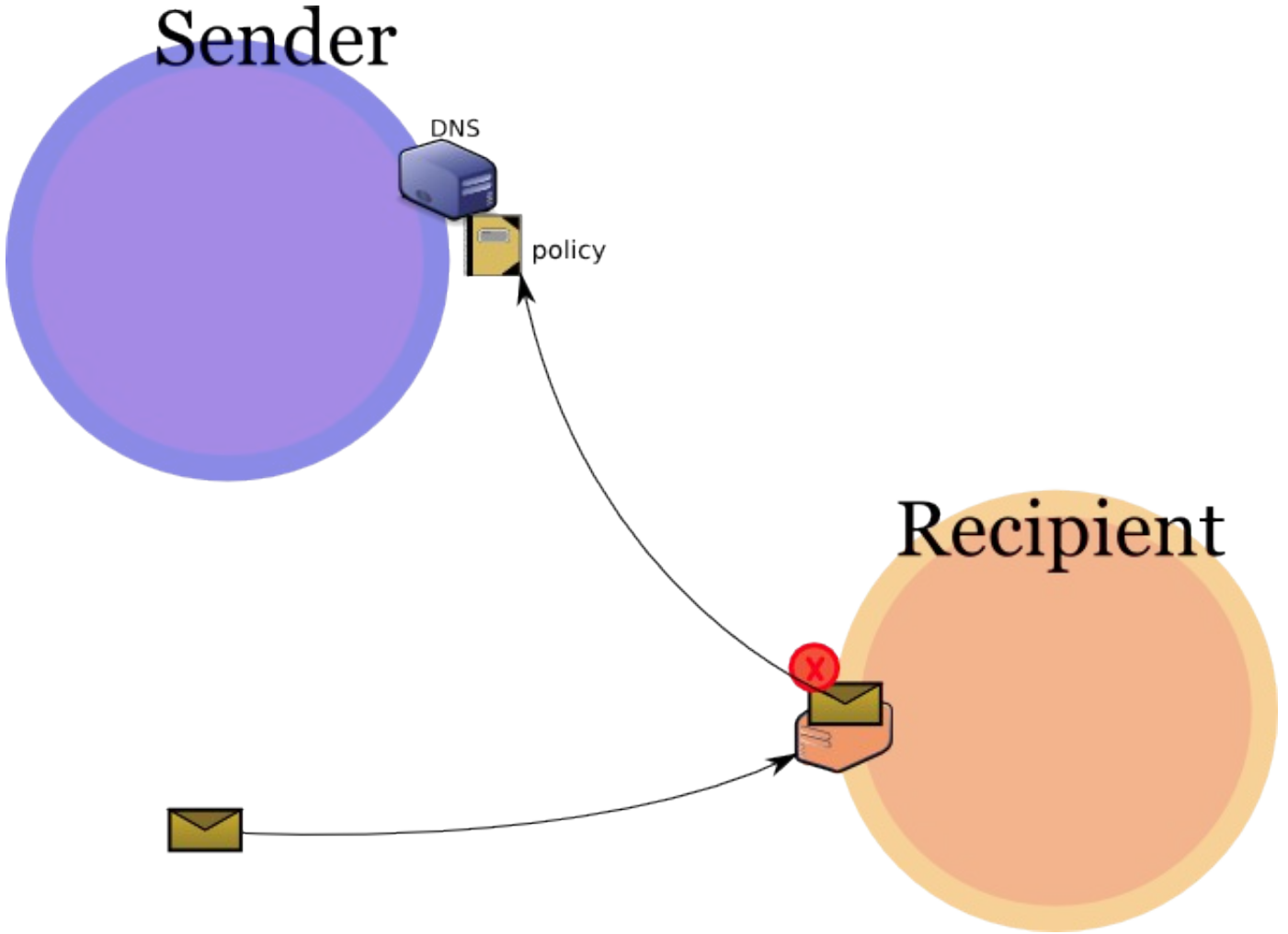


ISP.com email streams – dkim signing outbound

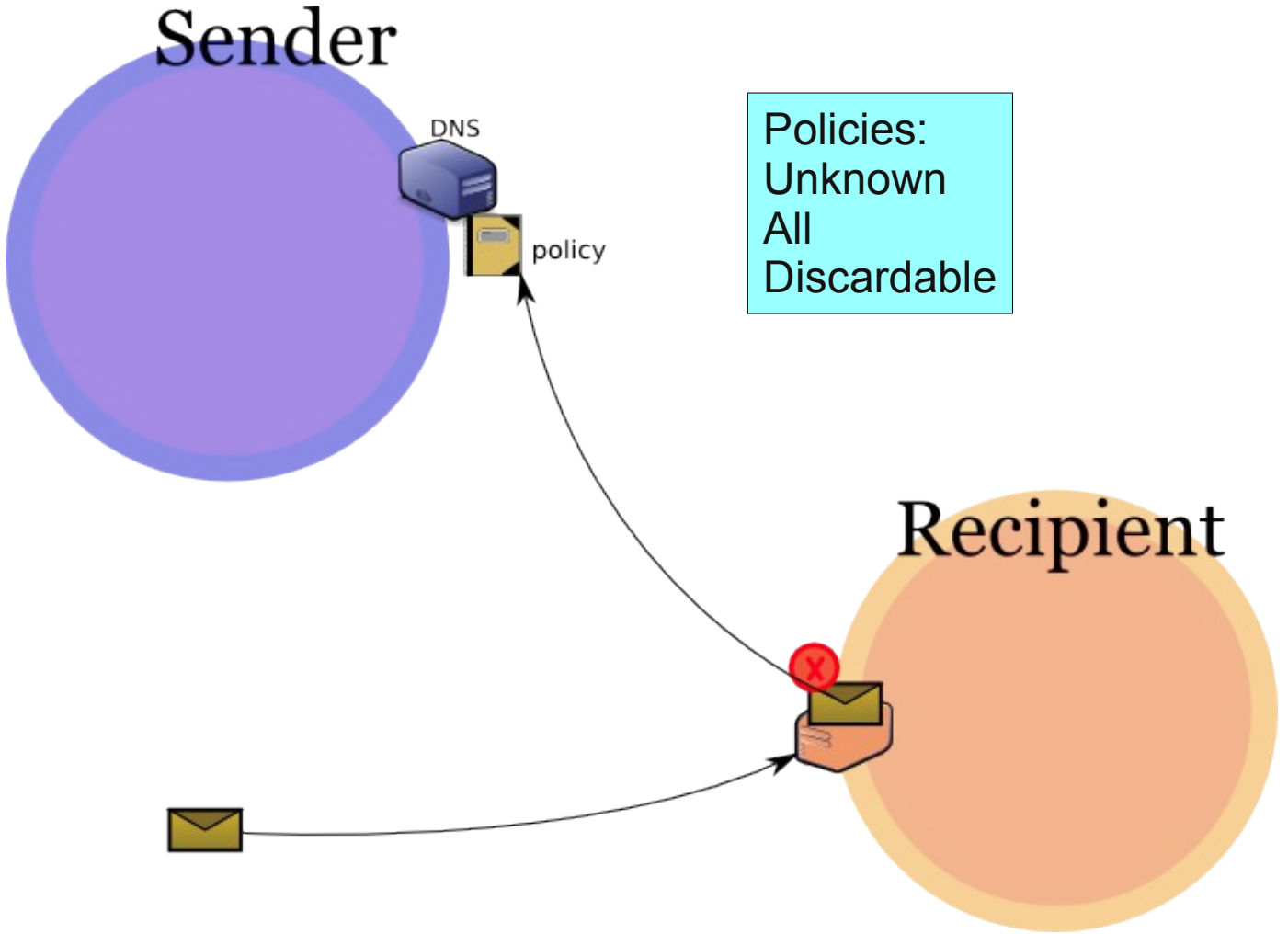



Yahoo! Inc. - Press Release - Mozilla Firefox <2>
File Edit View History Bookmarks ScrapBook Tools Help
Yahoo! Inc. - Press Release
Yahoo! Mail
YAHOO! PRESS ROOM
Search
Web Search
Company Info
Press Resources
Product Info
Contact Us
FUN FACT: There are more Yahoo! Mail users around the world than two 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)



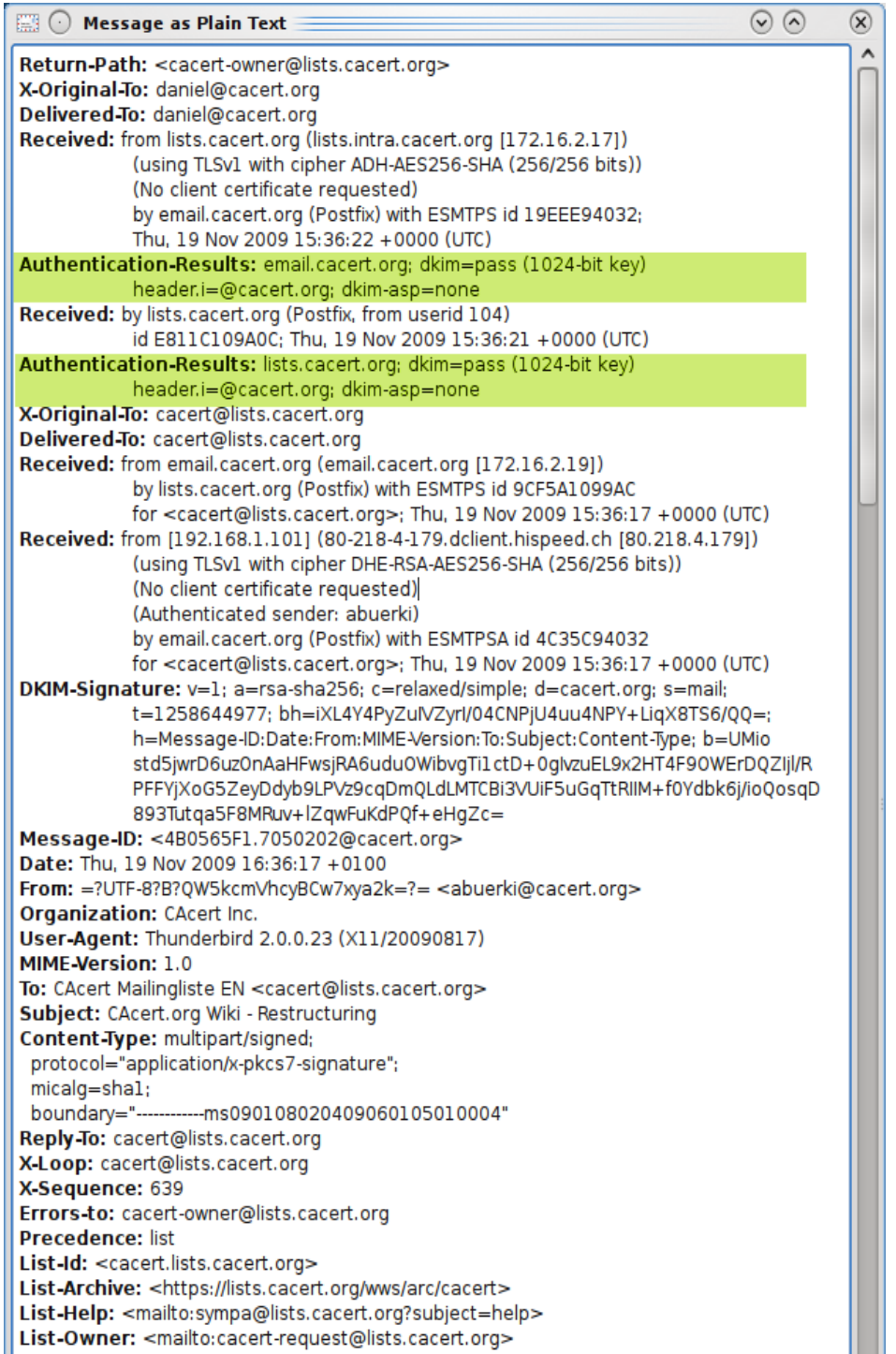
DKIM (near) Future – Reporting Failures

- 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



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

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

Presentation Credits and Licensing

Niels Heidenreich - SpamInbox - Fickr - 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/

Uzvards – Snail Mail - Flickr - http://www.flickr.com/photos/uzvards/2481348414/

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

Daniel Black – All other diagrams and screenshots