

DKIM

(DomainKeys Identified Mail, RFC 4871)

Roman Valls Guimerà

What is it ?



A way to sign and verify messages at MTA level using **public/private keys** and **DNS TXT RRs** to distribute the public key

Authenticates the **source** and its **contents**

NOT PKI based: No need to build a CA (optional)

Does not break other systems: asymmetric adoption

Sending part:

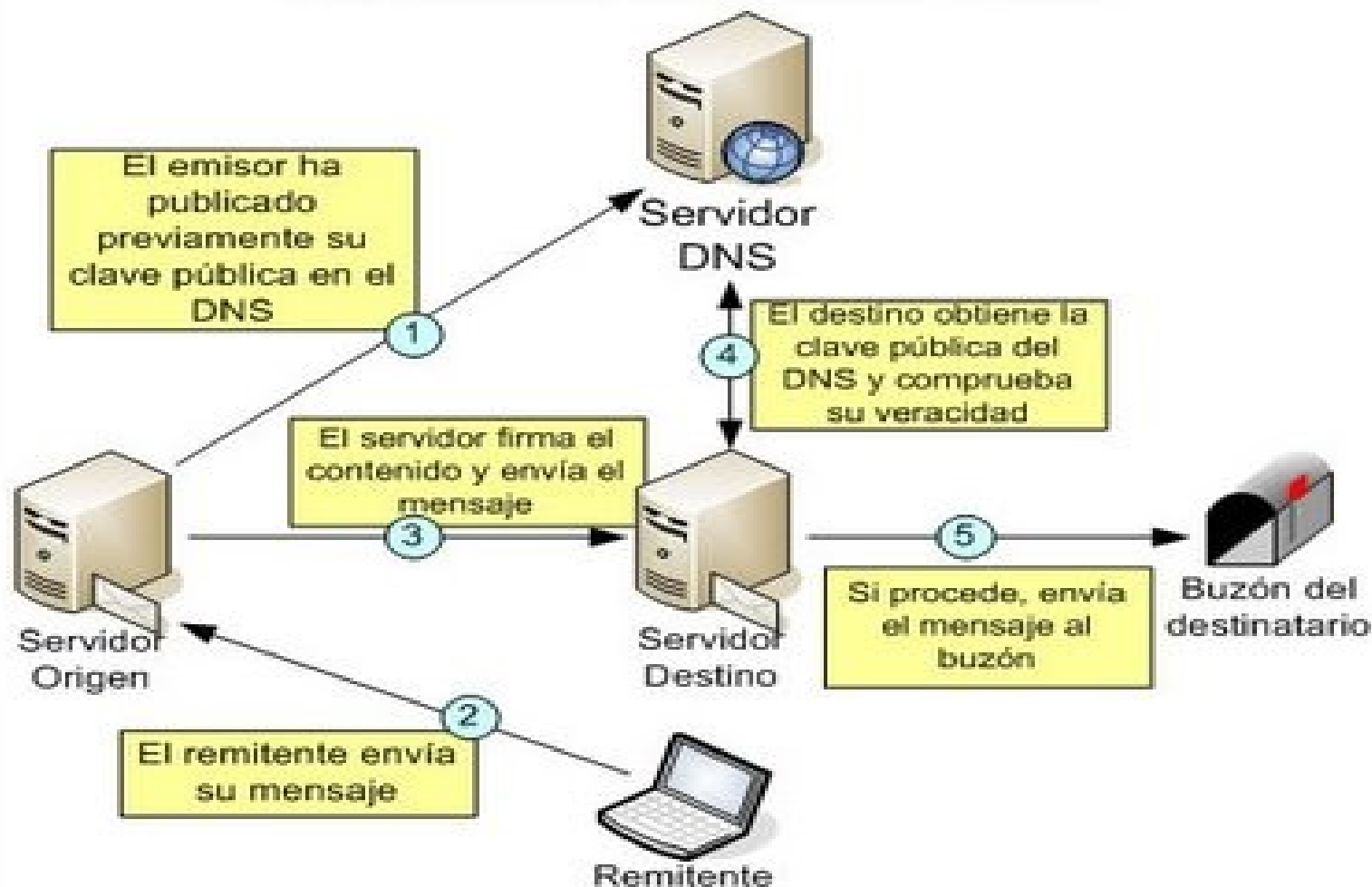
- 1) Signs the message (headers **& contents**)
- 2) Remember: Public domain key present on DNS
- 3) Clients send messages as always, the MTA will do the work

Receiving part:

- 1) Extracts signature and selector from headers
- 2) Queries DNS for public key on remote DNS and checks validity
- 3) Site-specific policy is applied (reputation system)

Overall picture

Esquema de funcionamiento de DKIM.



What DKIM is NOT by itself



An antiphishing tool

An antispam tool

An end-user tool

Not intended to replace S/MIME nor PGP

BUT can be **useful** for:

Reputation systems, ergo:

Antispam engines

Antiphishing engines

Basic reputation system



```
score DKIM_VERIFIED -0.3
score DKIM_SIGNED 0
score DKIM_POLICY_SIGNALL 0
score DKIM_POLICY_SIGNSOME 0
score DKIM_POLICY_TESTING 0
```

DKIM-based whitelisting of domains with # good reputation:

```
score USER_IN_DKIM_WHITELIST -8.0
whitelist_from_dkim *@intl.paypal.com paypal.com
whitelist_from_dkim *@*.paypal.com
whitelist_from_dkim *@paypal.com
whitelist_from_dkim *@*.paypal.be (...)
```

Basic reputation system (cont.)



```
# DKIM-based whitelisting of domains with less than perfect
# reputation can be given fewer negative score points:
score USER_IN_DEF_DKIM_WL -1.5
score ENV_AND_HDR_DKIM_MATCH 0
def_whitelist_from_dkim *@google.com
def_whitelist_from_dkim *@gmail.com
def_whitelist_from_dkim *@gmail.com (...)
```

Let's get into it



Two-slide config mini-howto



- 1) openssl genrsa -out rsa.private 1024
openssl rsa -in rsa.private -out rsa.public -pubout -outform PEM
- 2) Paste PEM key on DNS zone with format on next slide
- 3) apt-get install dkim-filter && vi /etc/dkim-filter.conf

```
Domain      escert.upc.edu
KeyFile     /etc/ssl/private/dkim/private.key
Selector    2007
InternalHosts /etc/mail/dkim-milter.internalhosts
```

4) /etc/postfix/main.cf:

```
# DKIM
smtpd_milters = inet:localhost:8891
milter_macro_daemon_name = SIGNING
milter_default_action = tempfail
milter_protocol = 3
```

Example DKIM BIND TXT entry



```
2007._domainkey      IN TXT "dkim=all; t=y; k=rsa;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD  
Wnq+ESaf8dAWoXKN6V8XiiSfhgztMKzsTNJE4fvZSUJGu  
oN6vXzD8m04k4kgrJvJJ87PBTBKf7jtbQU1bi0+kVcD4Gy  
JK+HxrKUKWFY1z2JPTH8EbGW2nsBy1kNzjqfmO8czfKo  
cgiltnV4FO/fvIX6/eLaL5EAzmH90wdPzlrQIDAQAB"
```

Alternative:

<http://www.sendmail.org/dkim/wizard>

Check: Is all of it working ok ?



WEB: <http://www.sendmail.org/dkim/testChecker>
Mail (dkim-reflector): dkim-test@testing.dkim.org

☐ Subject: DKIM reflector results
From: mail@testing.dkim.org
Date: 10/23/2008 10:26 AM
To: Roman Valls

DKIM Message Reflector Results

Authentication Results

```
testing.dkim.org; v=0.1; dkim=pass, header.i=rvals@escert.upc.edu (
  sig from escert.upc.edu/2007 verified; );
dkim=pass, header.i=rvals@escert.upc.edu (
  sig from escert.upc.edu/2007 verified; );
ssp=pass, header.From=rvals@escert.upc.edu
```

DKIM Processing Output

esCERT to GMail

Authentication-Results: mx.google.com; spf=pass (google.com: domain of rvalls at escert upc edu designates 147.83.152.5 as permitted sender) smtp.mail=rvalls at escert upc edu; **dkim=pass (test mode)** header.i=@escert.upc.edu

GMail to esCERT

Authentication-Results: mail.escert.upc.edu; **dkim=pass (1024-bit key)**
header.i=@gmail.com

Oops, different "Authentication-Results" headers

Will this take down my mailservr?



"We shouldn't put that much stress on a critical service such as email."

"The time that signing and verifying takes, could lead to a DoS on our own servers. Just a surge on SPAM and we're fried"

**Really ?
Did you measure it ?**

Directly on our production server:
mail.escert.upc.edu

XEN virtual machine (without **VT-x** !)

kernel = '/boot/vmlinuz-2.6.24-18-xen'

memory = '512'

Postfix+vmail+amavis+SA+clamav+dovecot+...

DKIM

RSA Private-Key: (1024 bit)

(rsa-sha256)

ZABBIX monitoring

Two (forgotten?) useful standard postfix tools:

Client:

```
smtp-source -s 20 -l 180000 -m 400 -c -f  
rvalls+stress@escert.upc.edu -t rvalls@escert.upc.edu  
mailserver:2525
```

-s 20: concurrent SMTP sessions
-l 180000: Mailsize in bytes
-m 400: Number of mails to send
-f & -t: from & to

Server:

```
smtp-sink localhost:2525
```


First attempt: Kill 'em all



150 concurrent SMTP transactions
1000 mail messages in **1 minute**

start: Tue Oct 28 17:54:08 CET 2008
end: Tue Oct 28 17:55:03 CET 2008

... 18:03: R.I.P

root@escert-dom0:~# xm console mail

```
[106646.515512] Code: c1 f8 05 81 c2 80 d0 3f c0 2b 82 10 07 00 00 8b b2 68 06 00 00 c1 e8 0a 39 cb 8d  
04 40 7f 21 8d 14 18 b9 01 00 00 00 eb 02 01 c9 <0f> a3 16 19 c0 85 c0 74 02 09 cd 83 c3 01 83 c2 01 39  
df 7d e9
```

```
[106646.515592] EIP: [<c01613e6>] get_pageblock_flags_group+0x46/0x70 SS:ESP 0069:e0789dc4
```

```
[106646.515604] ---[ end trace 44a286cd78cf3dae ]---
```

root@escert-dom0:~# xm destroy mail

Round 2



150 concurrent SMTP transactions
400 mail messages in **20 seconds**

Wed Oct 29 16:34:21 CET 2008

Wed Oct 29 16:34:42 CET 2008

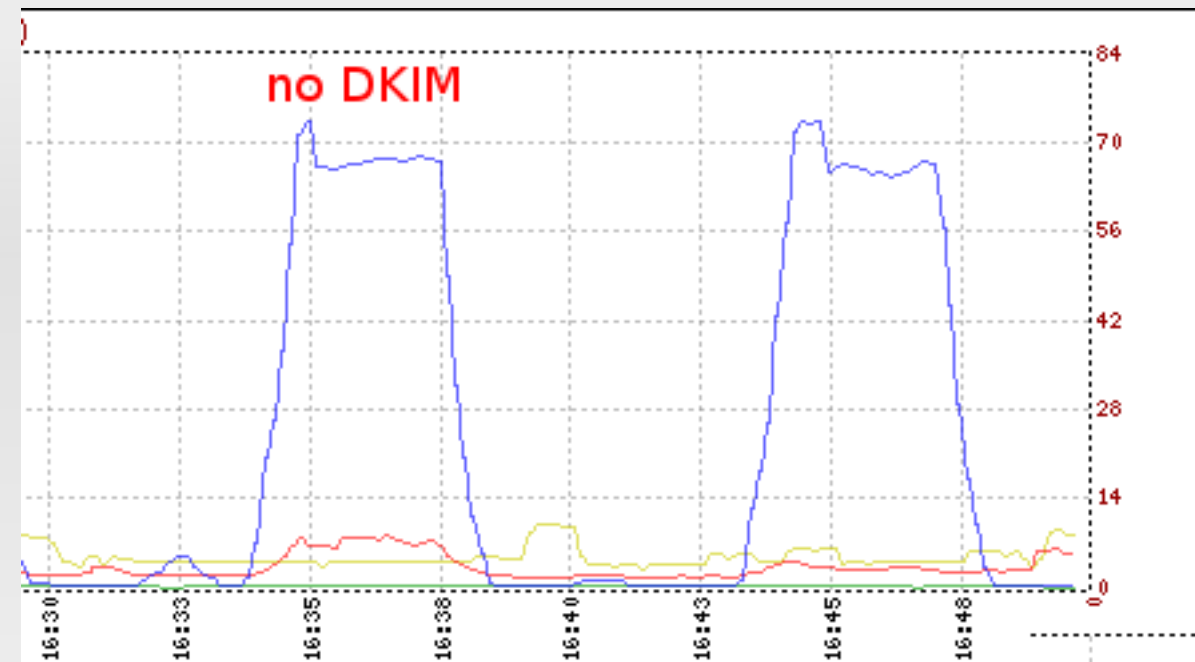
real 0m20.951s

... alive !

Results: CPU/RAM without DKIM



no DKIM



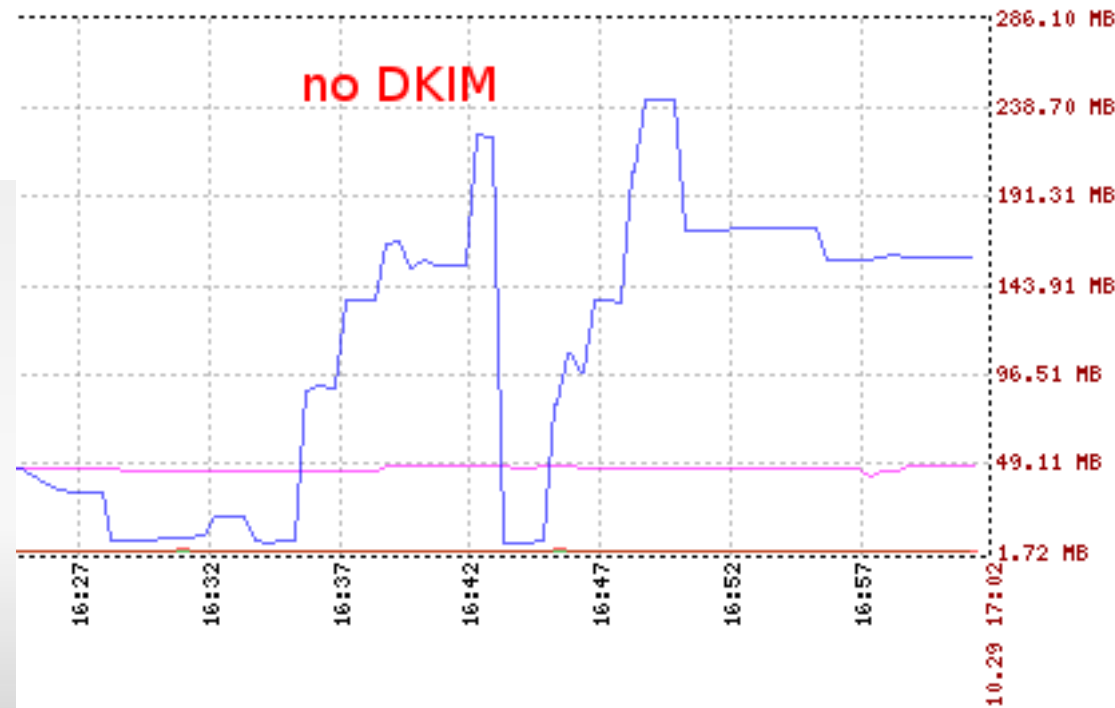
~76% CPU usage

~5 minutes to flush mail queue

~220MB RAM usage

~ 8 min to settle down

no DKIM

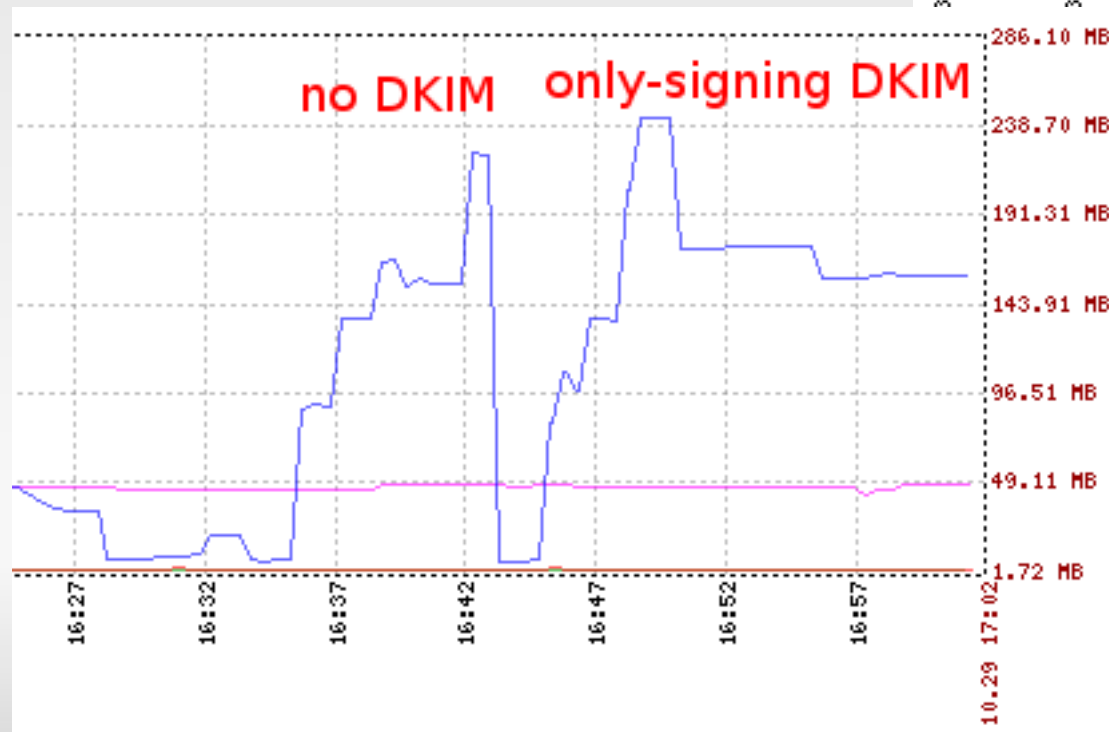
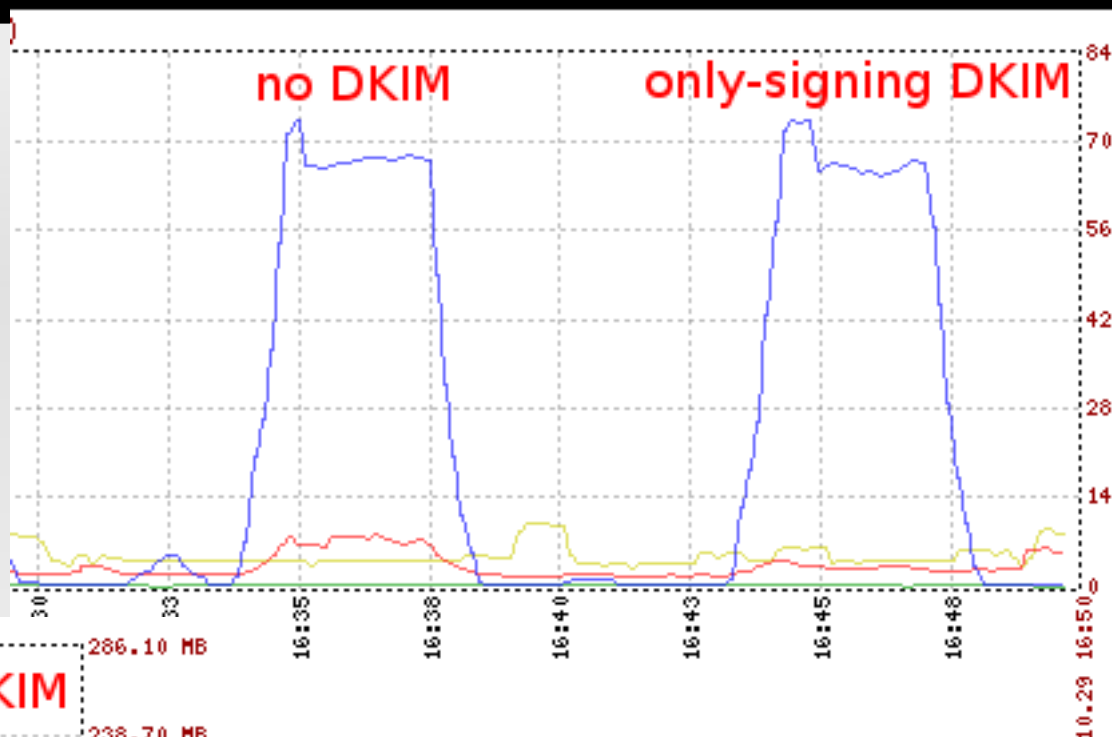


Results: CPU/RAM with DKIM

signing
only



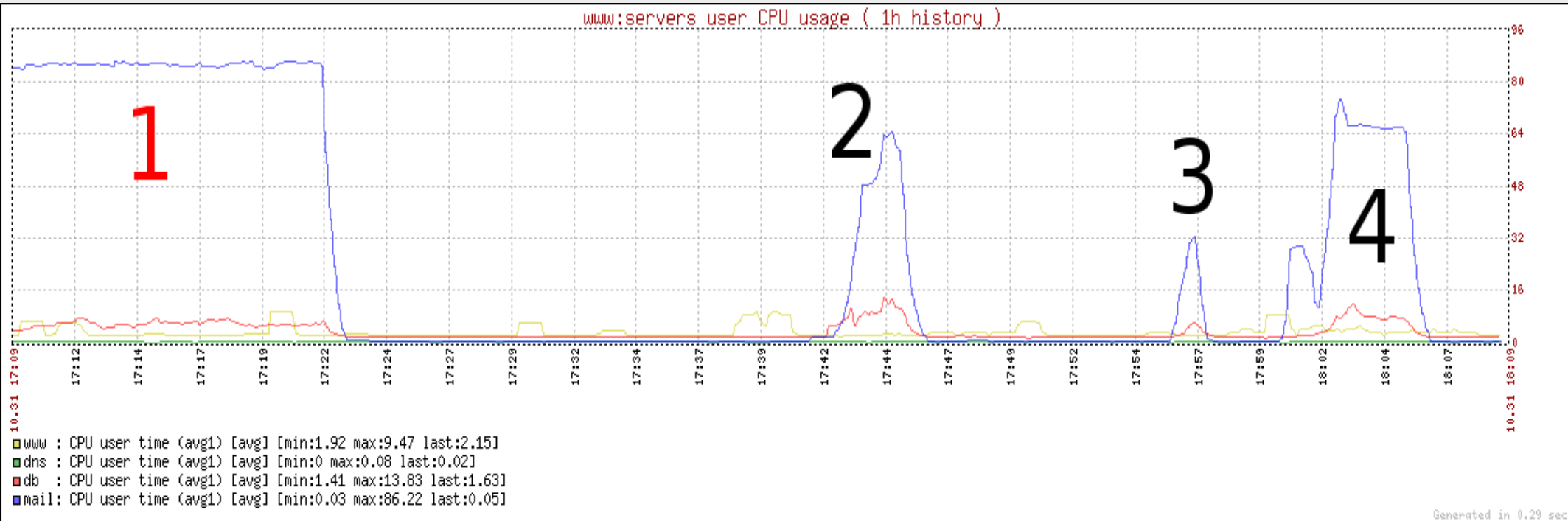
SAME !



nearly the SAME

Results: CPU with DKIM

sign
&
verify



- 1) Amavis+ClamAV+SA+DKIM(sign+verify), 5MB mails
- 2) DKIM(sign+verify) only, 5MB mails
- 3) DKIM(sign+verify) only, 180KB mails
- 4) Amavis+ClamAV+SA, 180KB mails

Google: "DKIM CPU overhead"

"Compared to the CPU overhead of running SpamAssassin and ClamAV, DKIM is lost in the noise"

Statement backed with actual data on this demonstration

Who is using it ? Gmail, Yahoo, PayPal, Ebay... deployment status ?:

<http://utility.nokia.net/~lars/meter/dkim.html>

DKIM proves itself as a simple way to add more points to reputation systems (aka: no silver bullet, but helpful if used wisely)

References



<http://hackandalus.nodo50.org/ftp/spf-dk-hackmeeting-2004.pdf>

<http://www.ijs.si/software/amavisd/amavisd-new-docs.html#dkim>

<http://utility.nokia.net/~lars/meter/dkim.html>