DNSSEC and DKIM Deployment in .SE

Patrik Wallström

Project Manager, R&D

.se

History of DNSSEC in .SE

Procect start

1999 - 2005

Dry run

2006

Commercial deployment - .SE DNSSEC

2007 -

.se

DNSSEC with Applications

End-user applications

- Web browsers
- MUA
- SIP
- IM

Server applications

- MTA
- OpenSSH
- PGP
- SSL
- XMPP

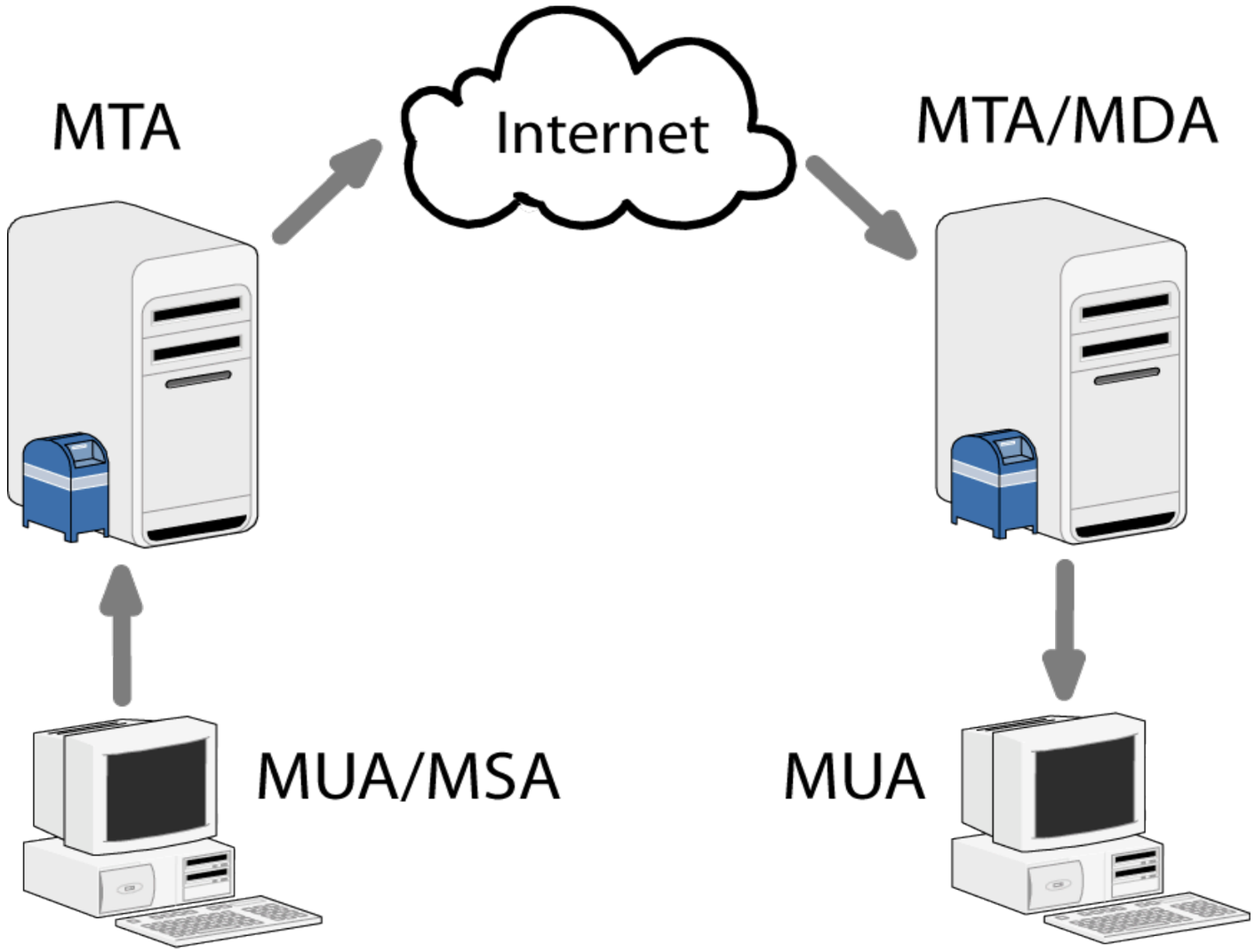
.se

Why DKIM?

- Already using DNS as key storage
- Validation occurs normally in the MTA
- Thus running in a controlled server environment
- Not an already widely deployed standard

.se

SMTP Overview



.se

SOHO Routers

Tests of Consumer Broadband Routers

Joakim Åhlund & Patrik Wallström

February 2008

Test Report:
DNSSEC Impact on Broadband Routers and Firewalls

Ray Bellis, Nominet UK & Lisa Phifer, Core Competence

September 2008

.se

DKIM-Milter 2.8.0 beta

Initial patch for DKIM-Milter 2.6.0 by John Dickinson

Patch uses libunbound to use DNSSEC
- retrieve a DKIM key from DNS
- acquire a domain's policy record using DNS queries

Published on opensource.iis.se and sent to DKIM-Milter maintainer

http://sourceforge.net/projects/dkim-milter/

.se

More work?

Murray S. Kucherawy announced 2.8.0 with a comment about writing a new draft, “**dkim-sec**” ...

The result for any DNSSEC-aware query basically comes down to one of these four:

- evaluation not completed ("unknown")
- signer not using DNSSEC ("insecure")
- signer using DNSSEC, successful ("secure")
- signer using DNSSEC, unsuccessful ("bogus")

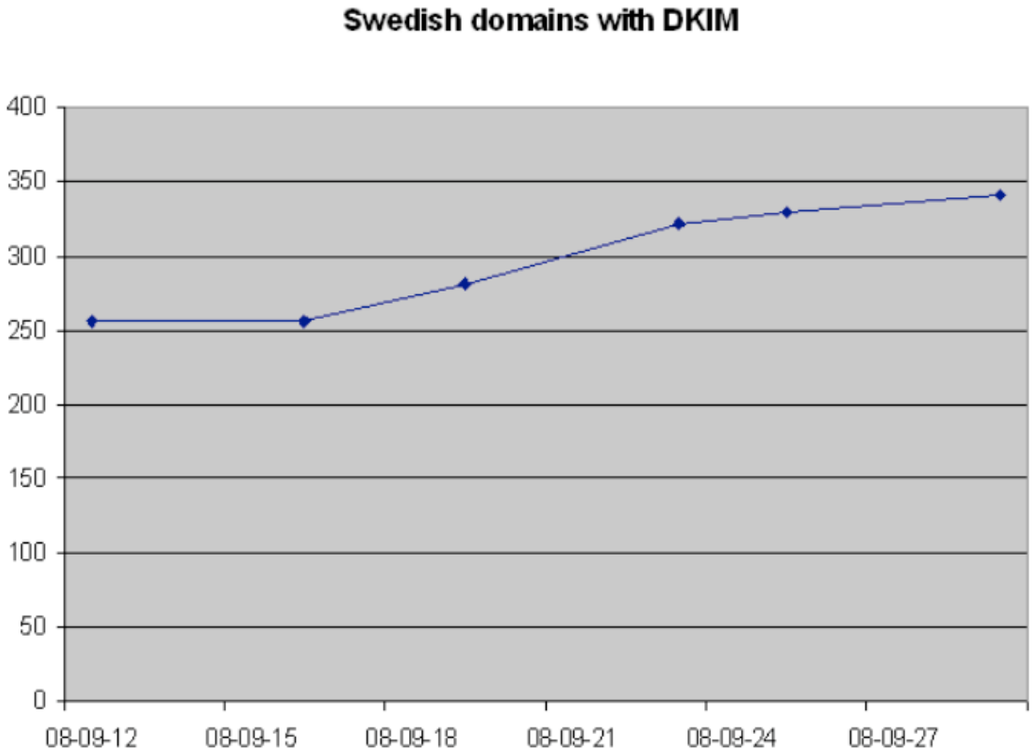
.se

More work?

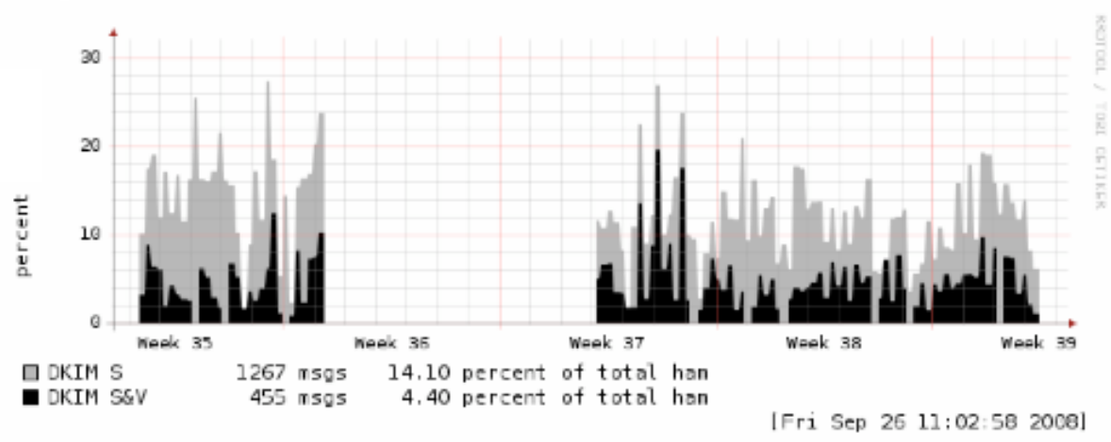
```
Therefore, I believe we need four new configuration settings.  In
particular (with invented names so far):

InsecureKey
       - specifies what to do with insecure keys
       - possible values:
             - ignore (no action; default)
             - neutral (degrade a "pass" to "neutral")
             - fail (degrade a "pass" to "fail")

BogusKey
       - specifies what to do with bogus keys
       - possible values:
             - ignore
             - neutral
             - fail (default)

InsecureADSP
       - specifies what to do with insecure keys
       - possible values:
             - apply (default)
             - ignore

BogusADSP
       - specifies what to do with bogus ADSP records
       - possible values:
             - apply
             - ignore (default)
```

.se

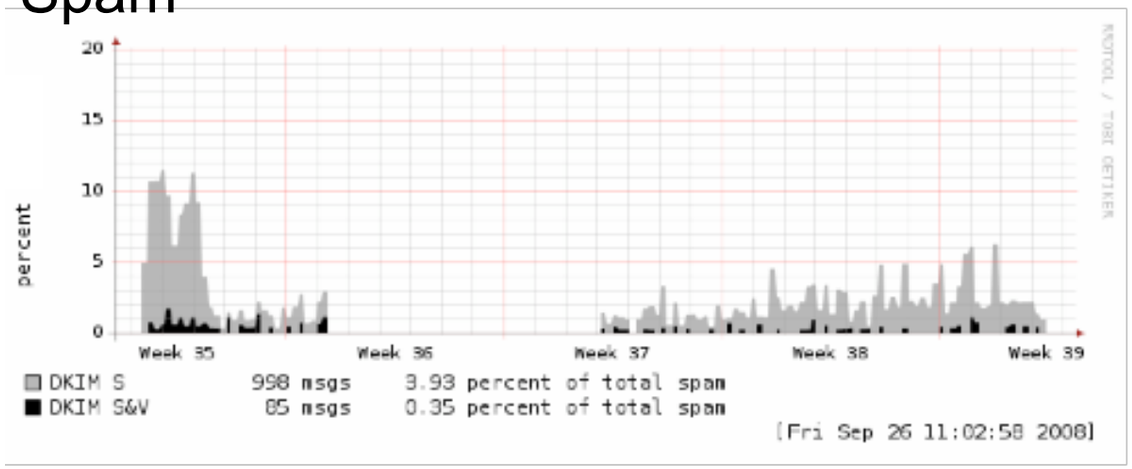
Statistics



Ham



Spam



.se

Report on using DKIM with DNSSEC

Work for .SE done by Rickard Bondesson

To be published as his Final Thesis at Linköping University:

Deployment and analysis of DKIM with DNSSEC

ISRN LIU-IDA/LITH-EX-A--08/055--SE

.se

Thank you

patrik.wallstrom@iis.se

.se