Deployment of DKIM with DNSSEC

Master's thesis

Rickard Bondesson

ricbo974@student.liu.se
+46(0)730 – 23 95 16

Agenda

- Email
- Spoofing
- Countermeasures
- DKIM
- The reliability of the DNS
- Deployment
- Testing
- Statistics
- Conclusions
- Questions

Email

- Important function
- Message
  - Header
  - Body
- Envelope

RFC2822

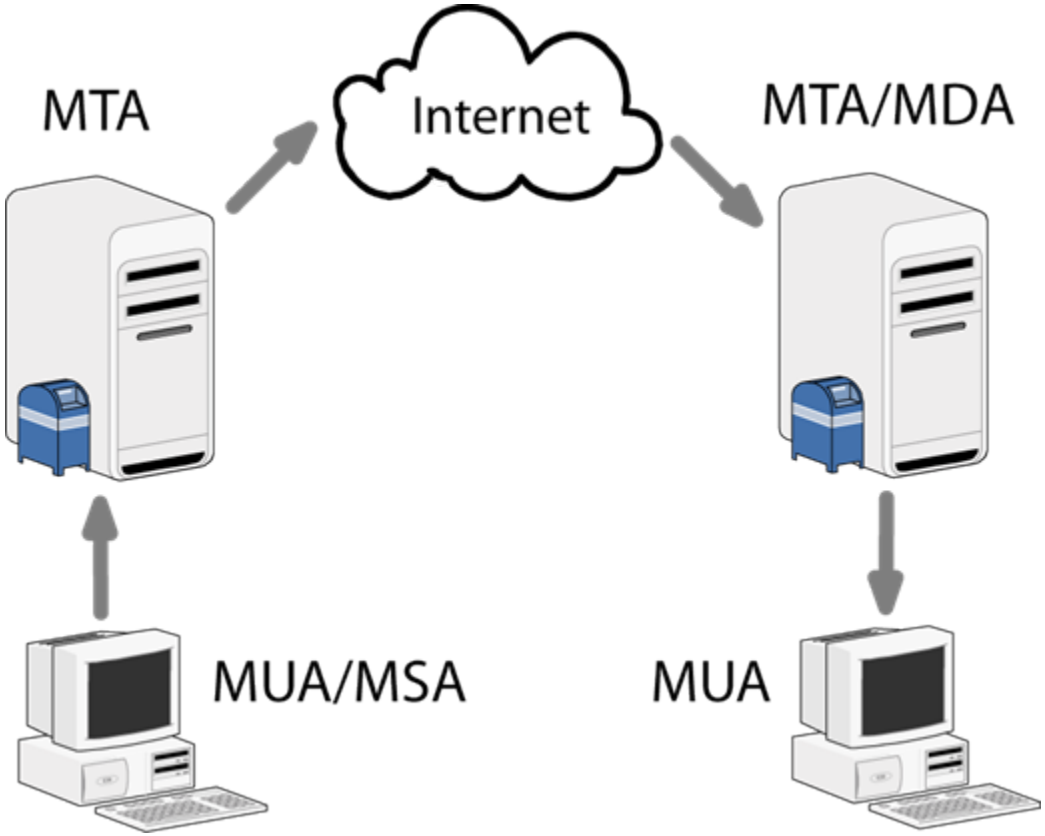
```
Date: Mon, 23 Jun 2008 11:50:27 +0200
From: alice@exempel1.tset.se
Reply-To: alice@exempel1.tset.se
To: bob@exempel2.tset.se
Subject: Meeting

Hi again!

The meeting is cancelled due to sickness.

Yours truly
Alice
```

Email system



SMTP

- HELO mta.domain.se
- MAIL FROM: user@domain.se
- RCPT TO: user@someotherdomain.se

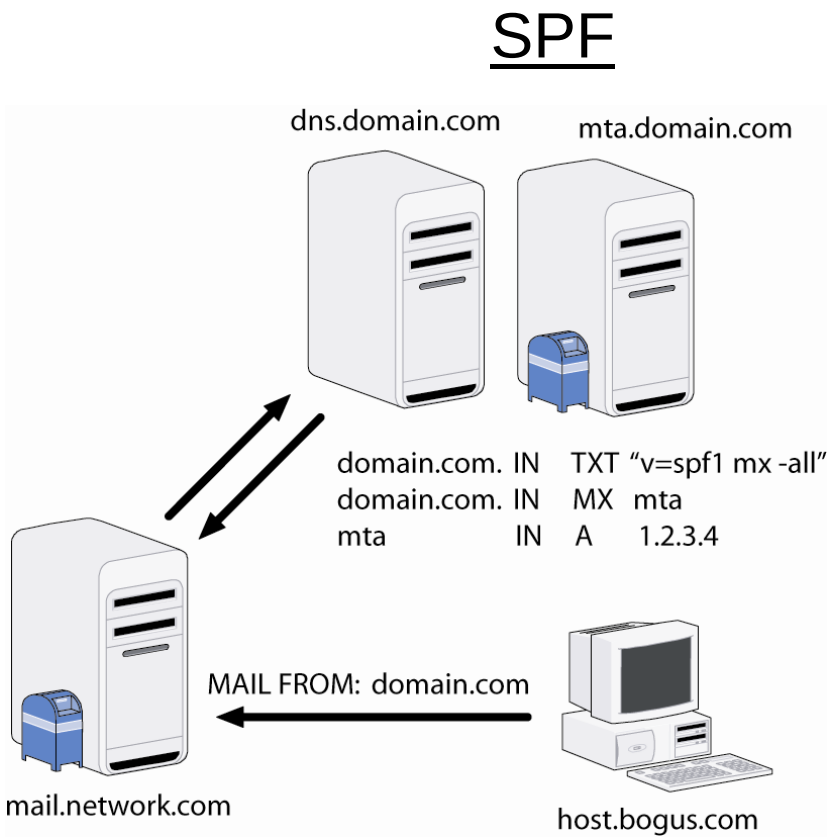
- + Authentication
- + Encryption

Spoofing

- Spam
- Phishing
- False email headers

Countermeasures

- Sender authentication
  - SPF
  - ADSP
  - SenderID
  - Black-/grey/whitelisting
- Content authentication
  - S/MIME
  - PGP
- DKIM and DomainKeys



DKIM

- Pros
  - Transparent to non-supporting users
  - Smooth transition
  - User anonymity
  - No new public-key infrastructure
  - Broken signature is like no signature (ADSP?)
  - Does not solve the problem with spam, but protects the email domain name
- Cons
  - Computational overhead
  - Some threats

DKIM - Canocalization

- Modification during transit
- Prepares the email before signing
- Does not affect the original email
- Two types: simple and relaxed
  - Simple header canocalization
  - Relaxed header canocalization
  - Simple body canocalization
  - Relaxed body canocalization

.se

DKIM - Signing

- Choose what headers to sign
- Create a hash of the email body
- Create a hash of the selected headers
- SHA1 or SHA256
- Sign hash with RSA

DKIM - Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
   d=exempel1.tset.se; s=ex1; t=1216375318;
   bh=F49+TW8nMriWgjHxXsVGiPa+xLNWevC3bGAT+Zl8Qag=;
   h=Reply-To:From:To:Subject:Date:Message-ID:MIME-Version:
   Content-Type:Content-Transfer-Encoding; b=AsmD11IU0TwqQwK
   9fGWIlV7TPtBRgEzcFwuhgbvaoipwcI9hA8M1TzE025rPzbLlJbEJKz8T
   2WSfmg7BbmSQ4rklSaq5ou1BrwxGTQWn/I37sOPhzg+pRfAjq7IWo6Zys
   OOgDkbCcOjL46kECDFQBWSvgKD3oOID4FOj5huSdzw=
```

.se

DKIM – Public key

- Publish the public key in the DNS
  - *selector._domainkey.domain TXT*
  - Key management
  - Key revocation

- Example:

```
ex1._domainkey.exempel1.tset.se. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6oekzH849jUK1EYJnfUM72
OlhpaTxqBhvNu3UTGsbRywFWBHCPfoeHAZKnYhN+pLAXuJ49oUNO1kybAqUfxPM
OpTbupY0zVdaJCtcMHi7j7rFgSrRi8nH55Frhq4aiS00ocdw1po0p72c7TkTNm5
E1Q2jZ4pGpjEXJtjzb9YckwIDAQAB"
```

.se

DKIM - Verification

- Recreates the signature and compares
- The result can be placed in:

```
Authentication-Results: exempel2.tset.se; dkim=pass
    (1024-bit key) header.i=@exempel1.tset.se;
    dkim-adsp=none
```

.se

DKIM – The reliability of the DNS

- The public keys need to be reliable
- Vulnerabilities in the DNS
  - Packet Interception
  - ID Guessing and Query Prediction
  - Name Chaining
  - Betrayal By Trusted Server
  - Denial of Service
- The attacker can publish a spoofed DKIM public key

DKIM - DNSSEC

- Digital signatures
- Detect modifications from third part
- Secure the source of the DKIM public key
- Trust anchor to every island-of-trust
- Sign all the way up to the root
- Does not protect against Denial of Service

.se

DKIM – Threat analysis

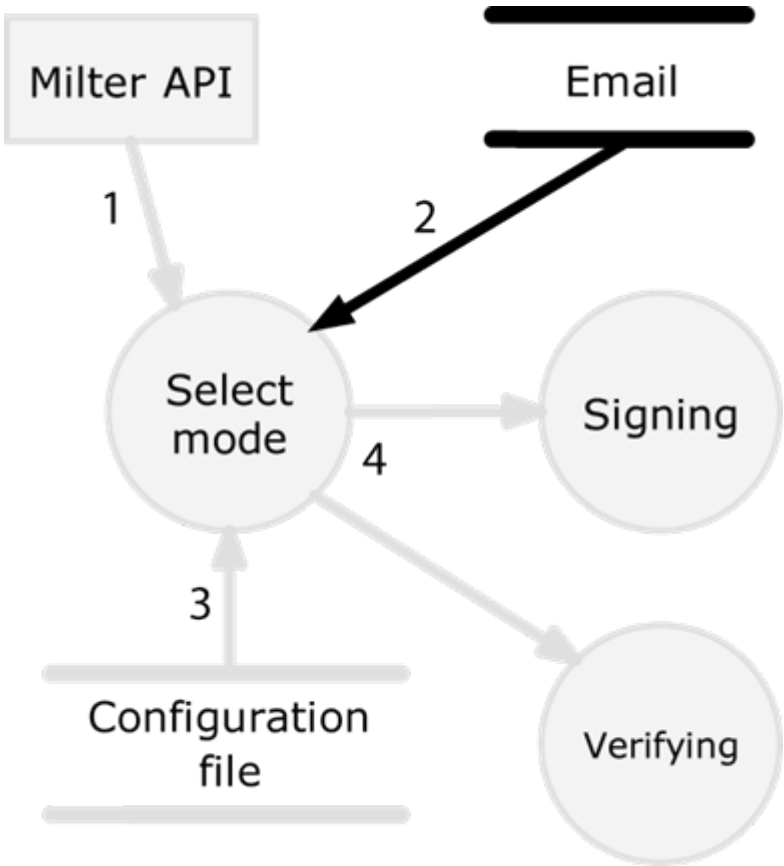
- Reply of old messages
- Real users sends bad email
- Usage of similar domain names
- Usage of a trusted user name
- Add information if the length parameter is in use
- Modify or add unsigned headers
- Make use of the canocalization algorithm

.se

DKIM - Deployment

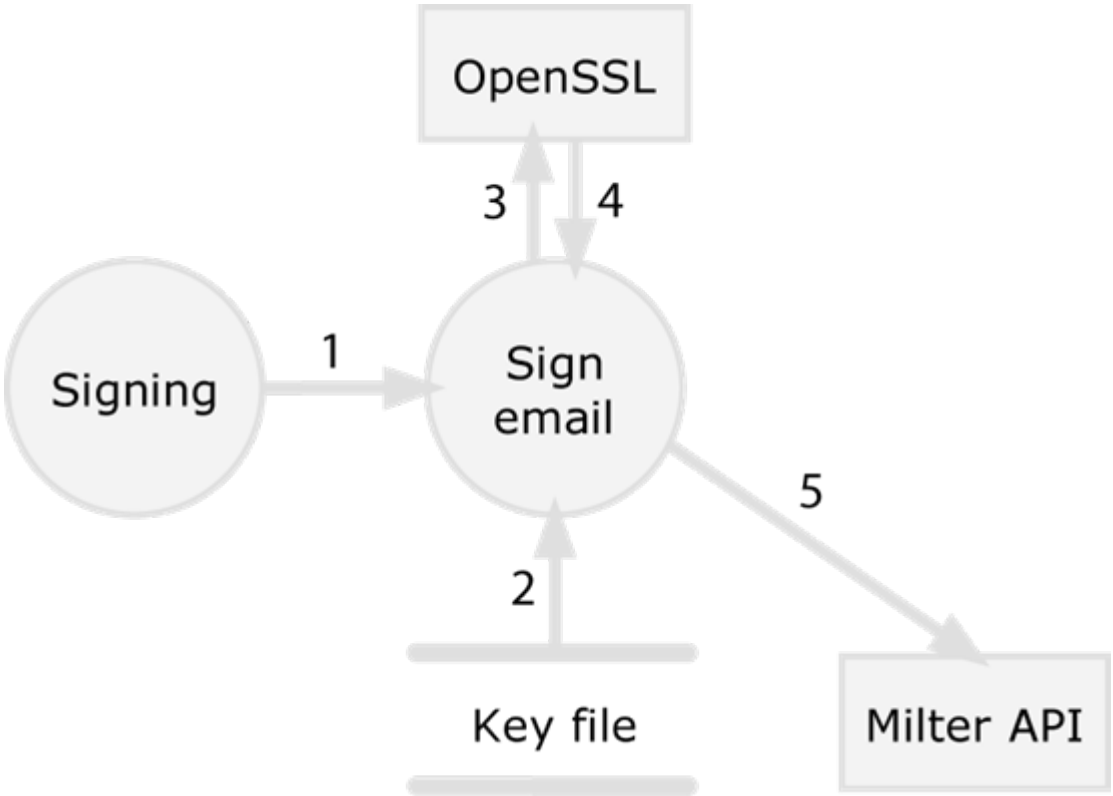
- DKIM Milter
- Patched to handle DNSSEC
- Runs two mail servers
  - Sendmail
  - Postfix
- IMAP + TLS
- SMTP-AUTH + TLS

DKIM Milter - DFD



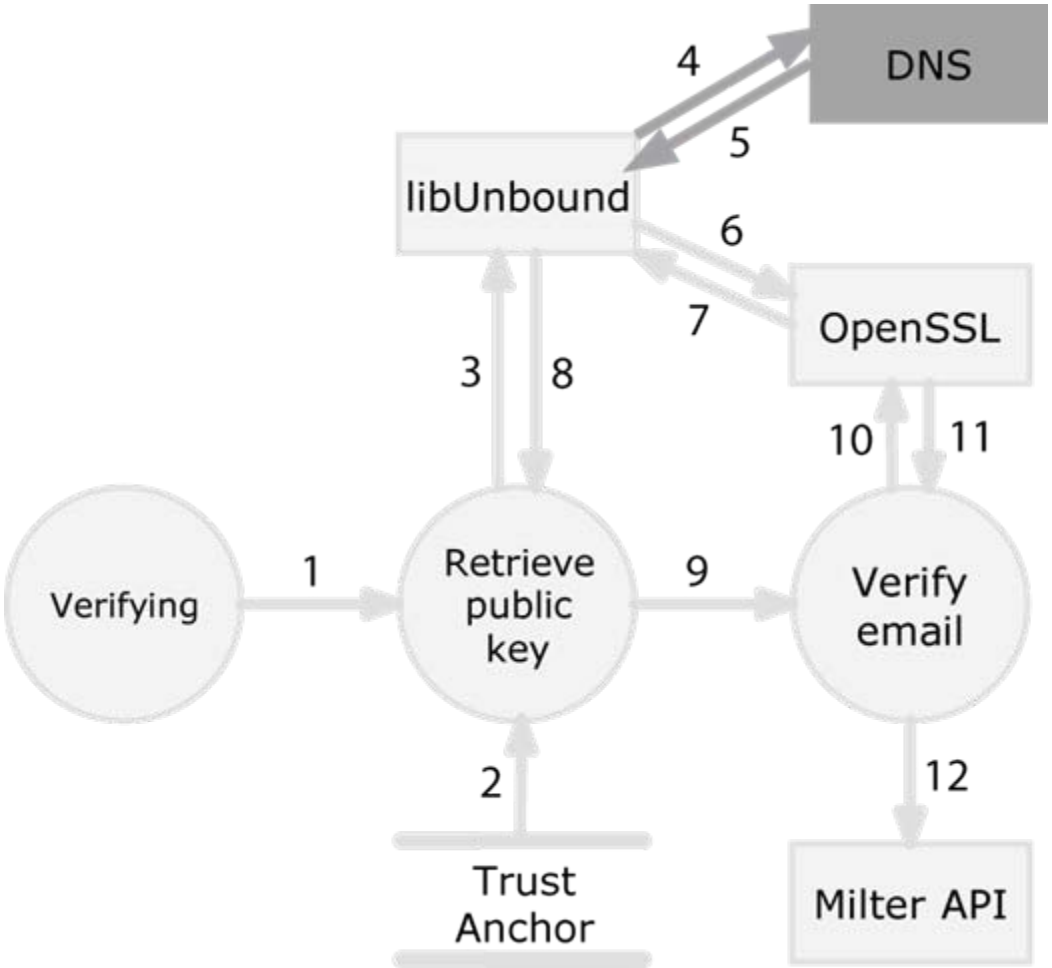
.se

DKIM Milter - DFD



.se

DKIM Milter - DFD



.se

DKIM Milter - Tests

- Function testing
  - Does the patch work?
- Domain testing
  - What happens with unexpected input?
- Basic email routing
  - Masquerading
  - Aliasing
  - Forwarding
  - Mailing lists

DKIM Milter - Results

- Function testing
  - OK
- Domain testing
  - OK
- Masquerading
  - No, if it happens after signing

.se

DKIM Milter - Results

- Aliasing
  - OK
- Forwarding
  - OK
- Mailing lists
  - Yes, if the mailing lists resigns
  - No, if the mailing lists does not resign
    Even if Mailman is configured to not change anything in the email, does it remove the angle brackets in the return address and thereby breaks the signature.

.se

DKIM Milter - Interoperability

- S/MIME
  - In Microsoft Outlook
- PGP
  - In Microsoft Outlook
- SPF
  - In the server with SMF-SPF Milter
- SpamAssassin
  - With SPF and DKIM

DKIM Milter - Results

- S/MIME
  - OK
- PGP
  - OK
- SMF-SPF
  - SPF OK
  - Breaks the signature when they mixes the result headers
- SpamAssassin
  - OK
  - Breaks the signature if some earlier result headers are signed

.se

DKIM Milter - Interoperability

- Test with other implementations of DKIM
  - Send email to addresses which bounces a result back
- Mailing list at GoogleGroups
- Email account at GMail
- Auto-forward of an email account at LiU

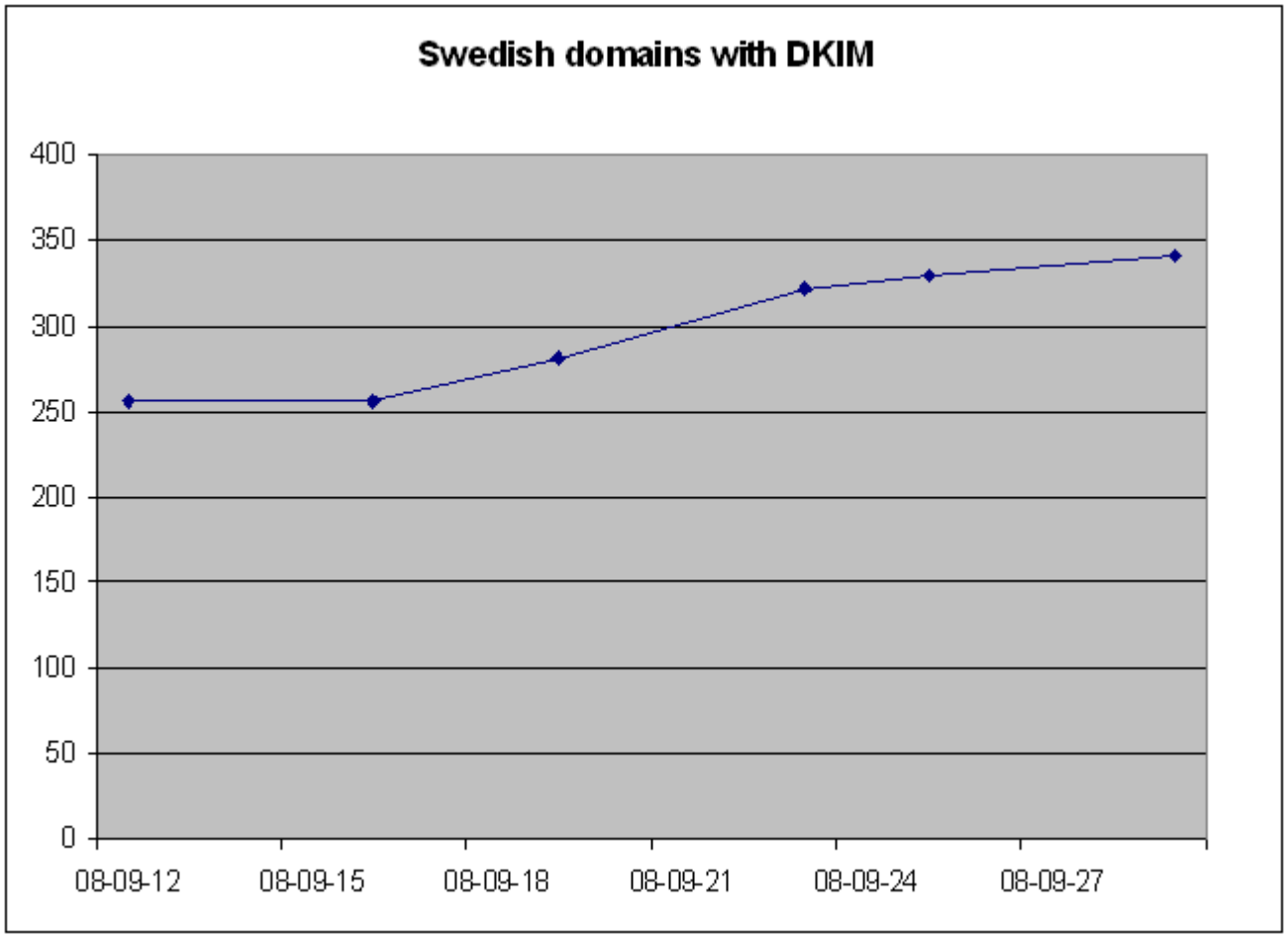
DKIM Milter - Results

- Test with other implementations of DKIM
  - OK
- Mailing list at GoogleGroups
  - OK, they resigns the email.
- Email account at GMail
  - OK
- Auto-forward of an email account at LiU
  - No, they are performing some kind of header sanitation before forwarding the email. Thus breaking the signature.

DKIM - Statistics

- Number of DKIM public keys among the Swedish domains
- Measure at an email server
  - Number of signed respectively signed and verifiable in relation to the number of spam and ham.

DKIM - Statistik



Defence.se
Fabege.se
Handelsbanken.se
OpenDNSSEC.se
Spray.se
UU.se
Yahoo.se

.se

DKIM - Statistics

- Needs a bigger flow of email to properly gather statistics among the email on the Internet

DKIM - Conclusions

- Modification during transit
- Mailing lists often breaks the signature
- There are some security threats
- What headers to sign?
- Policy when the signature is broken?
- Use ADSP
- DNSSEC protects the DKIM public keys
- DKIM is not the only solution and should be used together with example SPF

.se

Thank you for listening

- Questions?