

DKIM

last chance for mail service ?

TFMC2

01/2006

Mail service status

- More and more spam, fishing, spoofing, virus
- More and more energy in spam fighting
- More and more messages lost because :
 - Imperfect automatic filtering
 - User error while removing spam
 - Delivery report unusable (too many return for spoofed email)
- Trust in mail service is low now.

Authentication

- Authentication is not the ultimate solution but a pre-requisite to dissuade from many abuse.
- PGP and S/MIME in a wide area are in defeat :
 - too complex for users
 - need to deploy private keys to end users
 - S/MIME : expensive PKI, sharing trusted CA model is only commercial, ...

Sender Policy Framework

- A kind of « reverse MX ».
- Do not authenticate message itself but the message server origin.
- Altered by forwarders so require one of :
 - SRS (Sender Rewriting Scheme)
srs0+yf09=Cw=orig.org=alice@forwarder.org
 - *SMTP Responsible Submitter* extension :
MAIL FROM:<ann@orig.org> SIZE=1000
SUBMITTER=<bob@forwarder.org>

DKIM

- Signs message with asymmetric cryptography (similar to PGP and S/MIME)
- Neither certificate authority nor “web of trust”. Trust being based on the domain administrative delegation model. Public keys are published using DNS.
- In most case messages are signed by the MSA : so private keys are stored by that MTA, no distribution to end user

DKIM

- Signs body and some headers
- New header **DKIM-Signature** :
- Public key stored in DNS
 - **_domainkey** subdomain
 - selector subdomain
 - DKK new RR type, fall back to TXT

Example

The signer

The signature
algorithm

Access method
to the public
key

```
DKIM-Signature: a=rsa-sha1; q=dns;  
d=example.com;  
i=user@example.com;  
s=jun2005; c=nowsp; l=12345  
t=1117574938; x=1118006938;  
h=from:to:subject:date;  
b=dzdVyOfAKCdLXdJoc9G2q81eXSlEniSb  
av+yuU4zGeeruD001szzVoG4ZHRNiYz
```

Canonicalization
algorithm

Length of body
used for signature

Validity period

Headers part of
the signature

B64 encoded
signature value

Query DNS for :

jun2005._domainkey.example.com

Sender Signing Policy 1/2

- If a message contain a valid DKIM signature and if sender and signer are the same, the message is valid.
- What happens else ?
- SSP is a way for the sender to publish information so the signature verifier can decide if the message is suspicious or not

SSP2/2

- Use DNS (DKP or TXT RR)
- Result is one of
 - Some message of this entity may not be signed
 - Any message must be signed by the originator
 - Any message must be signed by originator or behalf a third party (mailing list, outsourcing,...)
 - Check individual level
 - Sender never signs message

DKIM versus S/MIME

- Not any expensive PKI deployment needed
- Depend on DNS security
- Not designed for end user to end user signature
- No private key for end user
- No change on existing MUA
- Signature validation by one of the receiving MTA
- Headers part of the signature
- Sender Signing Policy

Diapositive 10

C1

DKIM signature can't prove the signer agreement on content because private key is not under exclusive control of the signer. In fact S/MIME as real difficulties to be deployed. That's why some firms propose a virtual smart card key server to centralize keys and S/MIME verification proxy. In such configuration the S/MIME architecture is not so far from DKIM, isn't it ?

CRU; 30/01/2006

DKIM threats analysis

- Discussion about DKIM are huge because needs and implications concern all the Internet.
- A lot of critics about DKIM along the mailing list archive
- DKIM threats is a draft that summarize it :
<http://www.ietf.org/internet-drafts/draft-fenton-dkim-threats-02.txt>

Some identified limits

- DNS pollution
- Exploit body length limit
- Canonicalization abuse
- Use of revoked key
- Signed message replay
- DOS attack against DNS or signer verifier
- Compromise of MTA signing server
- Look-alike domain names (O/0 I/1,)
- Short time domain names

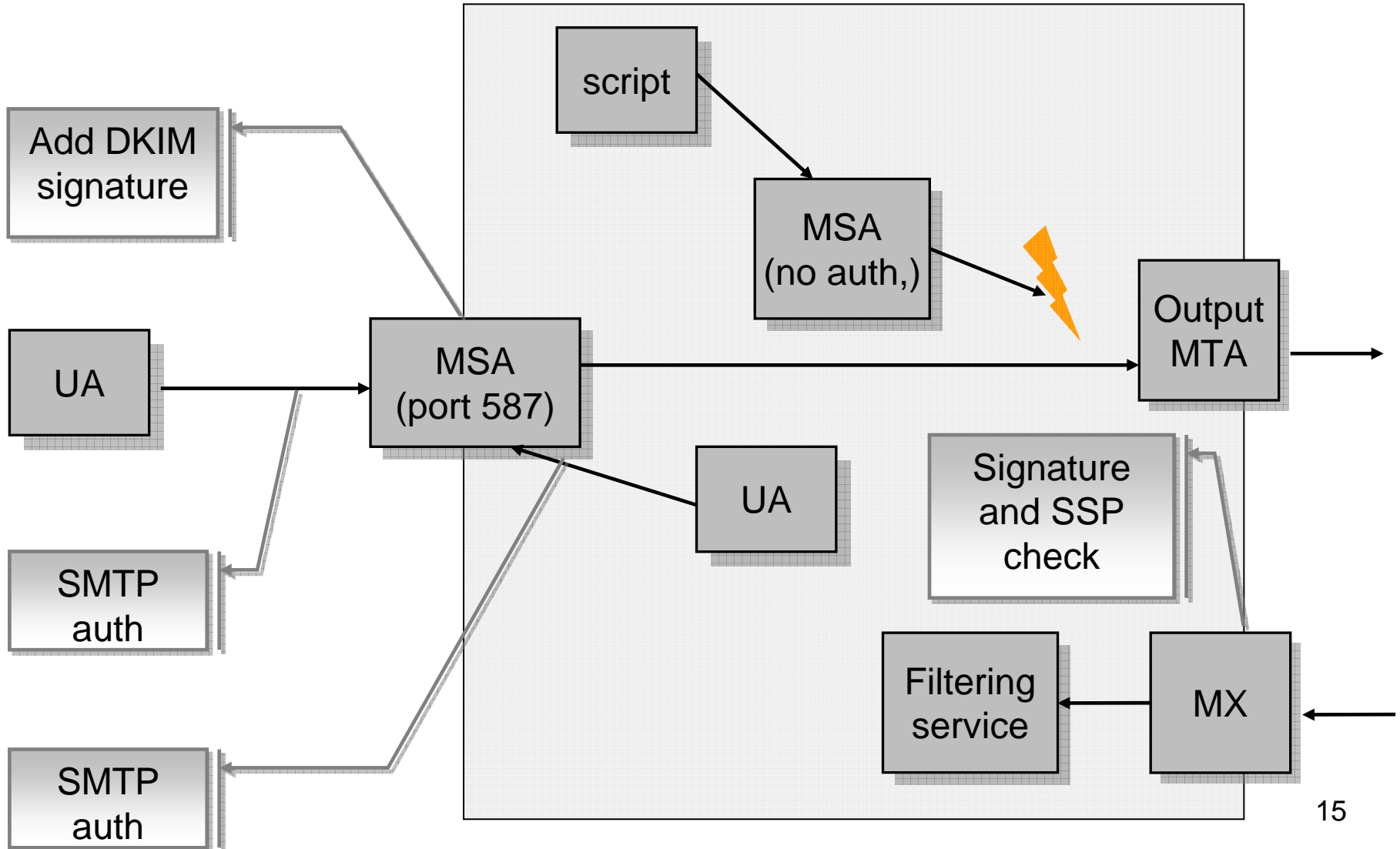
DKIM and ML

- Still an open discussion because no RFC specifies what's a ML.
 - Some says a MLM is forwarder
 - Some says a MLM is a remailer
- A forwarder must just preserve existing signature
- Forwarder is simple but may ease replay attacks and don't solve the question of "ML reputation".
- A remailer may remove existing signature and apply its own one.
- DKIM in a remailer is very complex

Message service architecture

- Signature added by the MSA require any mail received to be authenticated first.
- SMTP-AUTH (port 587) should be used for roaming and non roaming users.
- It make logs more valuable
- It can block botnet/Virus
- Must not block outgoing access to port 587 (is this specified in eduroam ?)
- Internet draft : Email Submission: Access and Accountability

Mail service architecture and DKIM



packages

- **Opensource :**
 - **libdkim W32 from ALT-N**
 - **Dkim-milter from sendmail**
 - **Dkimproxy from Jason Long**
- **Commercial**
 - **Mdaemon ALT-N**
 - **powerMta port 25**
 - **Strongmail strongmail**

Question ?