DKIM WG IETF-67

DKIM Originating Signing Policy

Douglas Otis
Doug_Otis@trendmicro.com

http://www.ietf.org/internet-drafts/draft-otis-dkim-dosp-02.txt

What Does DKIM-Base Not Accomplish?

- Accountability for unsolicited bulk email
- Safe white-listing with independent envelopes
- Authorizations outside the signing domain
- Validation of rfc2821 MailFrom addresses or SMTP clients
- Autonomous administration of provider relationships
- Independent vanity email-address domain authorization
- Minimized number of DKIM keys
- Correlation of the signing domain with the SMTP client

What can "Domain Associations" Accomplish?

- Eliminate any reason to:
  - Exchange DKIM private keys
  - Use CNAMEs at key/selector leafs
  - Delegate DNS zones to email providers
  - Deprecate email-addresses beyond signing domain

- Allows safe white-listing
- Assures rfc2821 MailFrom address for DSNs
- Policy & authorizations can extend beyond signing domain
- Relationships with providers are autonomously managed
- Freedom to authorize vanity email-domains independently

What Associated Identities are Assured?

Is the email-address valid or trustworthy?

- rfc2822 From ('F' & 'LF' annotation)
- rfc2822 Resent-* & Sender ('O' & 'LO' annotation)
- rfc2821 MailFrom ('M' protects DSNs)
- rfc2821 Ehlo ('E' protects white-list signing-domains)

Annotation or DSN Protection:
<base32(sha1(signing-domain))>._DKIM-x.email-domain
<base32(sha1(local-part))>._DKIM-Lx.email-domain

White-listing Protections:
<base32(sha1(ehlo-domain))>._DKIM-E.signing-domain
(Label confirmed by element in answer.)

Rare Association Hash Collision Fix

- Flag wildcard records as “Default” ('D')
- Return confirmation of label validity
- When not confirmed nor default record, query “_default”
- Confirmation wildcards permit use of CNAMEs

Example Association Records:

*._DKIM-x
TXT “v=0.0; f=A:D;” (never sends mail)

s5qs7wwt62yx6yowseuzjntou633vtez._DKIM-x
TXT “v=0.0; a=example.com; f=A;” (always signs)

Suggested Policies

DKIM-F & DKIM-LF rfc2822.From
DKIM-0 & DKIM-LO rfc2822.Resent-* or Sender
DKIM-M rfc2821.MailFrom
DKIM-E rfc2821.Ehlo

d= domain-list not assuring valid email-address
a= domain-list assuring valid email-address
l= local-part
f= flags:
- A - All initial messages signed by listed domains
- D – Default record
- L - Local-Part policy is published
- N - Not signing
- O - Only compliant services employed
- T - Trusted Designated Local-Parts
- V - Valid Designated Local-Parts

Why Use an Association Mechanism?

- Email-providers won't require customer's private DKIM keys
- DNS delegation or external CNAME records never needed
- All originating domains can leverage single DKIM signature
- Protects signing-domains used for white-listing
- Assures rfc2821.MailFrom domain for DSNs
- Far safer and more reliable than address-path registration
- Permits annotation of messages signed by other domains
- Permits trust based on UTF-8 (EAI) local-part addresses
- Permits autonomous management with large-scale use
- Minimizes use of DNS resources (replaces separate keys)
- Better retains:
  - Choice of providers
  - Authorization of vanity email-domains with different providers

Strong/Weak Points of DOSP

- Strong:
  - All originating domains can assert separate policies
  - Unlimited scalability with minimal DNS transactions
  - Private Key sharing completely avoided
  - Prevents abuse of signing-domains when used to white-list
  - Autonomous management of domain associations
  - Deterministic DNS lookups and labels
  - Indicates when stringent compliance can be expected
  - Indicates when message can be trusted based upon domain
  - Indicates when email-address is valid within different domains
  - Safe use of TXT Resource Records without added overhead
  - Exceeds SSP-Req-02 except the 6.3 (7) prohibition
- Weak:
  - NXDomain will not end a search for policy
    (fixed by incorporating _DKIM-x within SHA1 hash & new RR)

Questions?