MAAWG

Messaging Anti-Abuse Working Group

DKIM Implementation

MAAWG Training Series

Segment 2 of 4 on DomainKeys Identified Mail

From the onsite training course at the MAAWG 18th General Meeting
San Francisco, February 2010

DKIM Implementation – Video Segments

Segment 1 20 mins.	Segment 2 20 mins.	Segment 3 18 mins.	Segment 4 35 mins.
Theory	Theory	Practical	Practical
• General DKIM Architecture • What DKIM Is and Isn’t	• DKIM Protocol Details • Separate Mail Streams & Signing Practices	• Planning • Keys and Policies	• Signing Software • Verifying Software • Testing, Other Topics • Q&A

Segment 2 Covers

Theory:

- DKIM Protocol Details
- Separate Mail Streams and Signing Practices

Dave Crocker
MAAWG Senior Advisor
Principal, Brandenburg InternetWorking
dcrocker@bbiw.net

Public Key – DNS Record

- **Query name combined from**
  - Selector *(for key rotation, s=)*
  - "._domainkey."
  - Signing Domain Identifier (SDID, d=)
- **Stored in TXT**
- **Major parameters**
  - v: Version of the DKIM key record
  - p: Public key data
  - n: Human readable notes

Signing and Verifying

Signing

- **Choose**
  - Private/public key
  - Signing Domain ID (SDID)
  - Selector
  - Header fields to sign
- **Compute hash**
- **Encrypt hash**
- **Create DKIM-Signature: field**

Verifying

- **Compute hash**
  - Note fields listed in DKIM-Signature field h= tag
- **Fetch public key**
  - From s=, d= field tags
- **Decrypt hash**
- **Compare**

DKIM-Signature: header field

- **Primary tags**
  - a: The algorithm used to generate the signature
  - b: The signature itself
  - bh: The hash of the canonicalised body
  - c: Message canonicalization
  - d: The signing domain
  - h: List of header fields that are signed
  - s: The selector

- **Additional tags**
  - t: Signature timestamp
  - v: Version
  - i: Additional information about the identity of the user or agent for which this message was signed

Identifying Mail Streams

- **An organization has multiple “types” of mail**
  - Corporate
  - Transactions (purchase order, order confirmation...)
  - Proposals
  - Marketing mass mailings
  - Customer Support
- **Label them with different DKIM d= subdomains**
- **Allow different reputations to develop**

ADSP:
Author Domain Signing Practices

- **Exploring mistrust**
  - What if no signature based on From: field domain?
- **Domain owner can publish practices for signing with From: field domain**
- **DNS TXT record under**
  - _adsp._domainkey.<from domain>
- **Practices:**
  - unknown, all, discardable

Status

- **Signing**
  - Proposed Standard
  - Updated
  - Minor -bis effort just starting
- **Deployment & Operations doc**
  - Going through final approval
- **ADSP**
  - Published.
- **Pending**
  - Assessment standards that use DKIM???

References

- **DKIM home page –**
  http://dkim.org
  - DKIM 3-slide Teaser
  - DKIM Service Overview – RFC 5585
  - FAQ
  - Wikipedia entry on DKIM
  - Development, Deployment and Operations
  - Three myths about DKIM
  - Examples and analysis, countering the myth that DKIM is expensive
  - Discussion Lists

- **DKIM Signatures –**
  RFC 4871 + RFC 5672

- **ADSP –**
  RFC 5617

- **Auth-Results –**
  RFC 5451

- **ARF –**
  http://mipassoc.org/arf/
  http://www.ietf.org/dyn/wg/charter/marf-charter.html