DomainKeys Identified Mail (DKIM)

D. Crocker ~ bbiw.net

dkim.org

- Consortium spec

  Derived from Yahoo DomainKeys and Cisco Identified Internet Mail

- IETF published revision – RFC 4871

Allows an organization to claim responsibility for transmitting a message, in a way that can be validated by a recipient

- Validate identifier and msg data integrity
  - DNS identifiers
  - Public keys in DNS
- End-to-end
  - Between origin/receiver administrative domains
  - Not path-based

DKIM Goals

- Based on message content, itself
  - Not related to path
- Transparent to end users
  - No client User Agent upgrades *required*
  - But extensible to per-user signing
- Allow signature delegation
  - Outsourcing
- Low development, deployment, use costs
  - Avoid large PKI, new Internet services
  - No trusted third parties (except DNS)

Technical High-points

- Signs body and selected parts of header
- Signature transmitted in DKIM-Signature: header
- Public key stored in DNS
  - In _domainkey subdomain
  - Uses TXT RR
- Namespace divided using selectors
  - Allows multiple keys for aging, delegation, etc.