

DomainKeys Identified Mail (DKIM)

D. Crocker

Brandenburg InternetWorking
dcrocker@bbiw.net

dkim.org

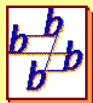
- ✿ Multi-vendor spec
 - Derived from Yahoo DomainKeys and Cisco Identified Internet Mail
- ✿ IETF revised spec and working group is done!

- ✿ Msg header authentication
 - DNS identifiers
 - Public keys in DNS
- ✿ End-to-end
 - Between origin/receiver administrative domains.
 - Not path-based



DKIM Goals

- ✿ Validate message content, itself
 - Not related to path
- ✿ Transparent to end users
 - No client User Agent upgrades *required*
 - But extensible to per-user signing
- ✿ Allow sender 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
 - New RR type, fall back to TXT
- ✿ Namespace divided using selectors
 - Allows multiple keys for aging, delegation, etc.
- ✿ Sender Signing Policy lookup for unsigned or improperly signed mail

