



# DomainKeys Identified Mail (DKIM) and PKI

**Jim Fenton <[fenton@cisco.com](mailto:fenton@cisco.com)>**

# DKIM Background

- **DKIM is a proposal for e-mail message signatures being standardized by IETF**

- **Key distribution is based on DNS**

**A field in the signature specifies the location of the key**

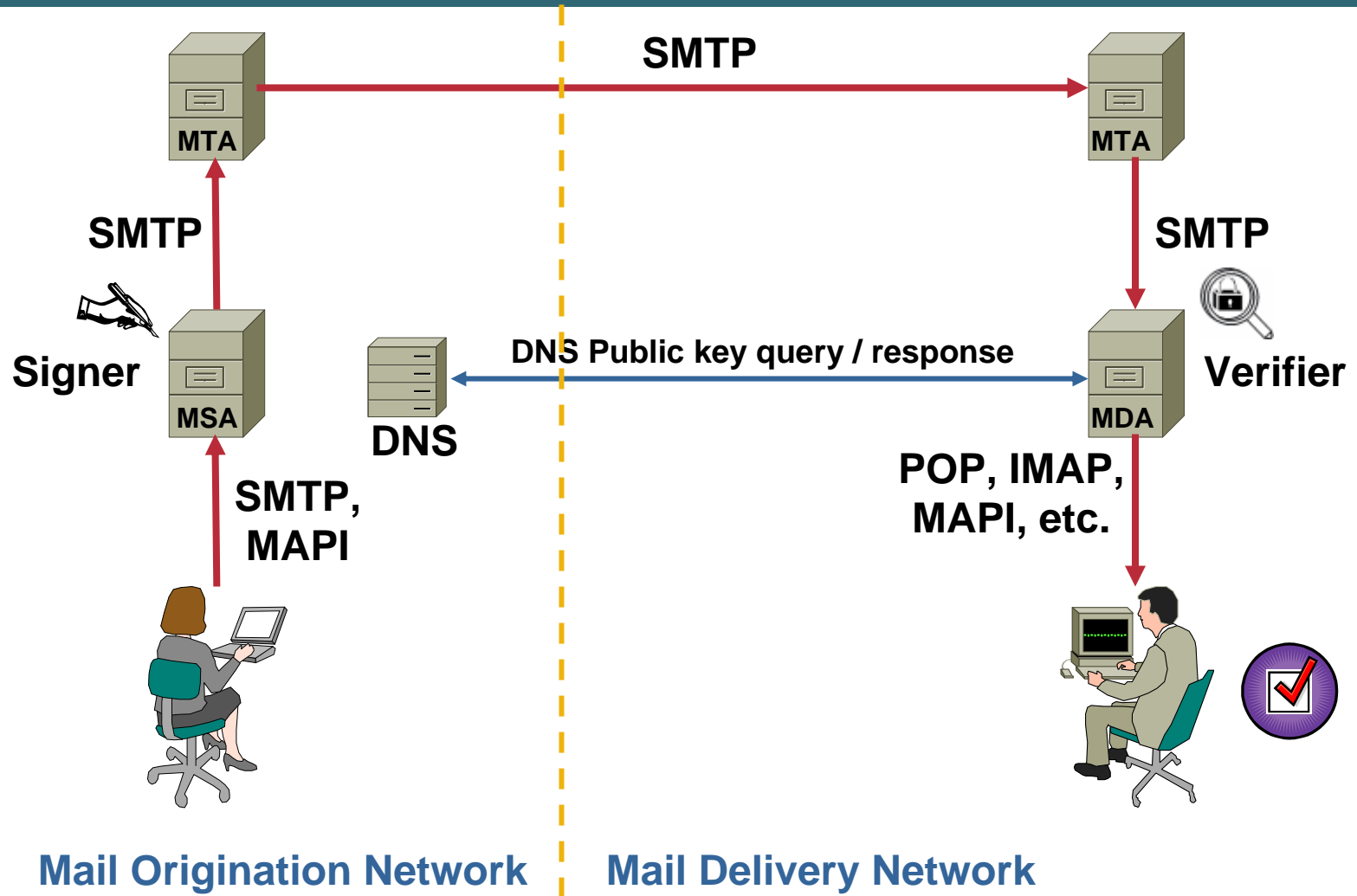
**Keys are stored in the `_domainkey` subdomain of the signer's DNS hierarchy**

- **Raw keys, not certificates, are used**

- **Signatures represent the signing domain, not the actual author**

**However, the domain owner may delegate signing authority**

# Deployment Model – Simple Case



# “Frequently” Asked Questions

- **Why not use an existing signature standard such as S/MIME?**
- **If not, why not use certificates for key management?**

# What About S/MIME?

- **The signature semantics are wrong**

**S/MIME signatures represent the author, not the domain owner**

**S/MIME (and PGP) signatures are still useful for signing message content with the “usual” semantics**

- **Transparency of signatures is important**

**DKIM signatures will be applied for all mail from some domains**

**Users (senders and recipients) may not expect this**

**Help desk load is a concern – and impedes deployment**

# What About Certificates?

- **Concern about disenfranchising some domains by the requirement to get a cert**
  - **Could be costly for third world**
- **Must be able to revoke signing authority quickly**
  - **Frequent updates to a potentially very large CRL**
- **Size matters**
- **New requirement that domain owner be in trust chain**
  - **Different from current low-assurance certificates**

# Revocation issues

- **Delegation of signing authority is needed to support important use cases**
  - Outsourced applications (benefits, etc.)**
  - E-mail marketing**
  - Mobile users who can't/don't submit messages to domain**
- **Some domains will issue signing keys to some users**
- **What happens when a user with a key leaves the domain?**
  - Keyholder may be terminated for cause (e.g., abuse)**
  - Very rapid (within minutes) revocation required**

# Conclusion

- **DNS provides a useful pseudo-PKI for DKIM**
  - Light weight transaction**
  - Cached by the infrastructure**
    - Although we do need to consider infrastructure burdens**
  - Easily revoked**
  - Under direct control of the domain**