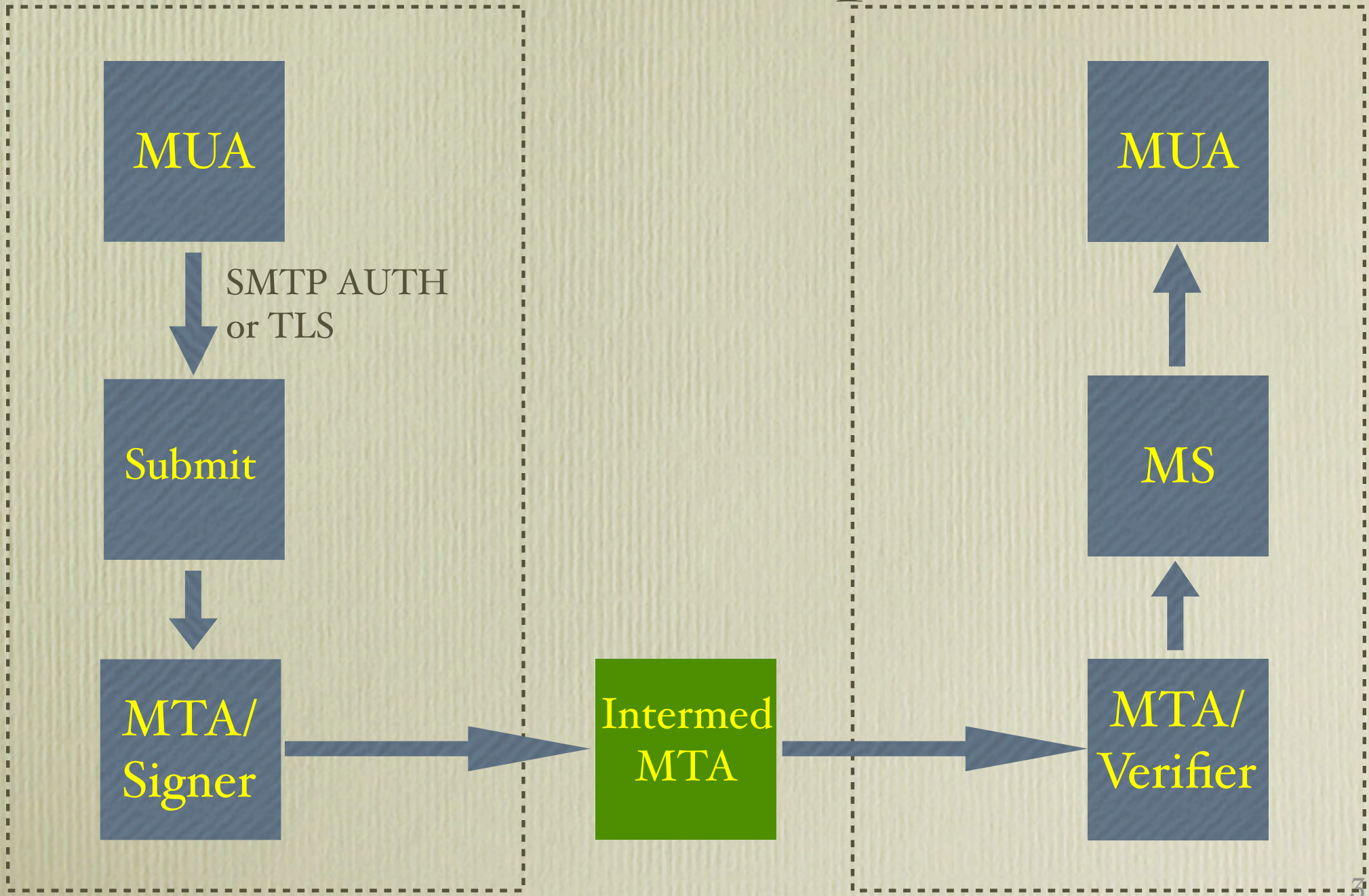
DomainKeys Identified Mail Overview (-01)

Eric Allman
Sendmail, Inc.

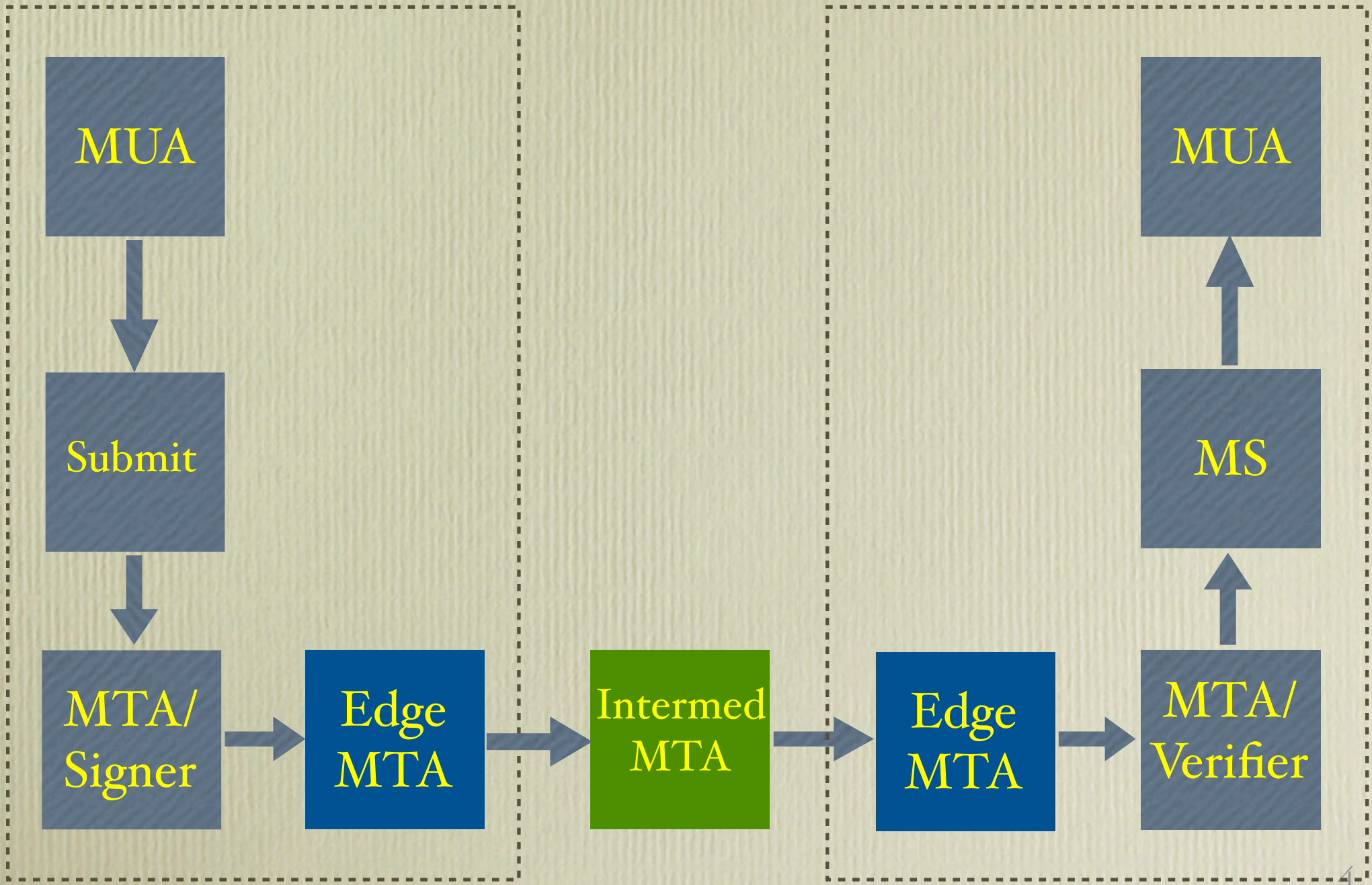
Overview of DKIM

- Cryptography-based protocol, signs selected header fields and message body
- Intended to:
  - Enable reliable domain name based reputation lookups
  - Allow good senders to provide evidence that they did send a particular message
  - Dramatically increase the difficulty of forgers masquerading as those good senders (requires Sender Signing Policy)
- Not an anti-spam technology by itself

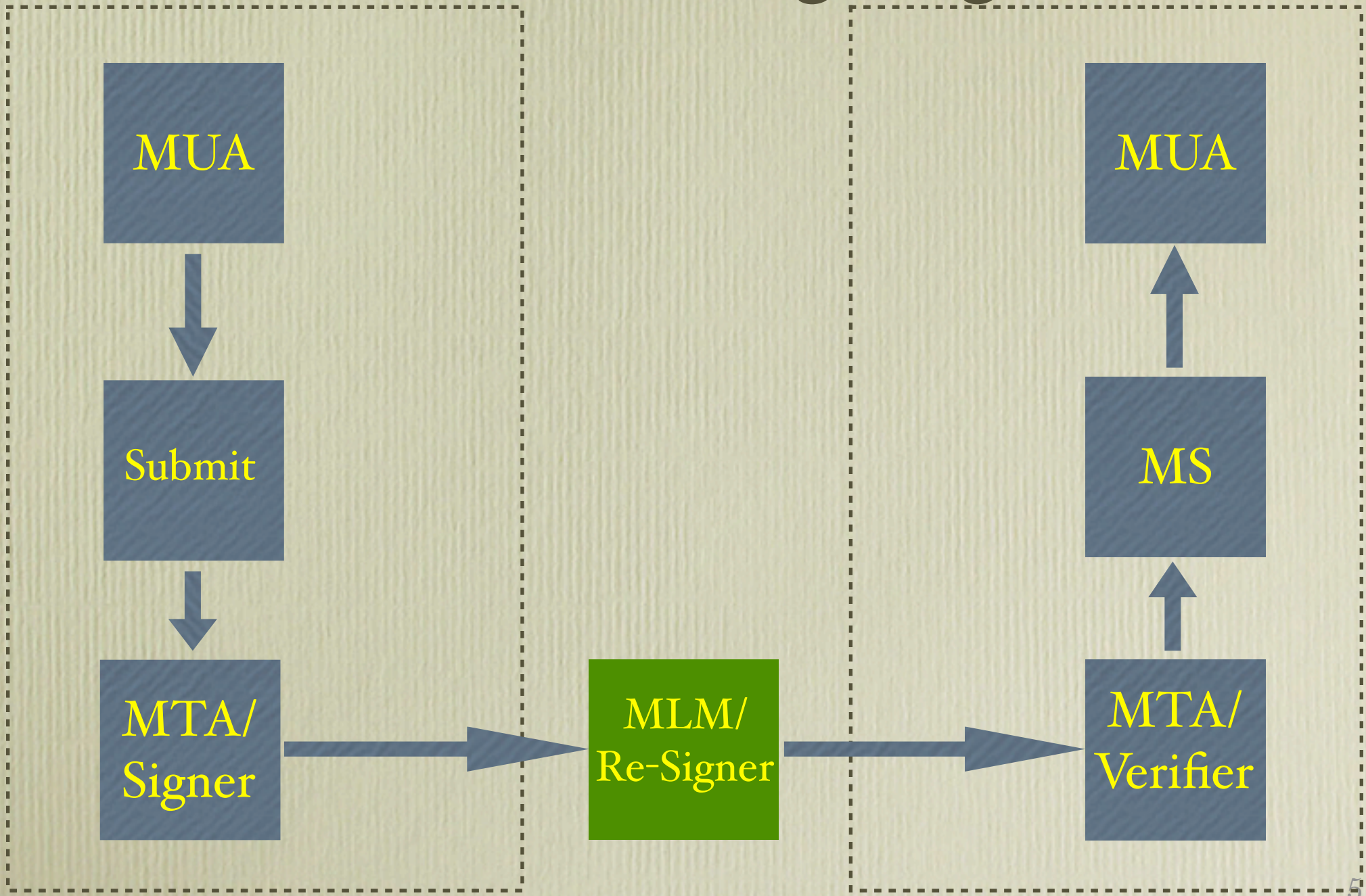
Model (Simple)



Model (with Edges)



Model (Resigning)



DKIM Design Goals

- Low-cost (avoid large PKI, new Internet services)
- No trusted third parties (key escrow, CA, etc.) required
- No client User Agent upgrades required
- Minimal changes for (naïve) end users
- Validate message itself (not just path)
- Allow sender delegation (e.g., outsourcing)
- Extensible (key service, hash, public key)
- Structure usable for per-user signing

DKIM Technology

- Signature transmitted in DKIM-Signature header field
  - DKIM-Signature is self-signed
  - Signature includes the signing identity (not inherently tied to From:, Sender:, or even header)
- Initially, public key stored in DNS (new RR type, fall back to TXT) in `_domainkey` subdomain
- Namespace divided using selectors, allowing multiple keys for aging, delegation, etc.

DKIM-Signature Header

- Example:

```
DKIM-Signature: a=rsa-sha1; q=dns;
  d=example.com;
  i=user@eng.example.com;
  s=jun2005.eng; c=relaxed/simple;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
    av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- DNS query will be made to:

```
jun2005.eng._domainkey.example.com
```

Ways to Use DKIM

- Lets recievers reliably apply domain-based policies
- Use signing identity for reputation lookups
  - Signers who forge or spam will garner bad reputation
  - Unsigned messages treated as “unknown reputation”
- Reject (or warn) unsigned/improperly signed messages based on Sender Signing Policy
  - Needed to deal with domain name spoofing/phishing
- Mark authenticated senders to end users
  - Has to correlate to what end user sees displayed
  - Best done in MUA, but can be done by server
- Display signing identity to end users
  - Requires MUA support (probably)

dkim-base Changes Since -00

- Canonicalization
  - nowsp eliminated in favor of relaxed
    - relaxed bodies keep CRLF; reduce all wsp to single space
  - Split selection of header & body canonicalization
    - c=relaxed/simple
- Added some IANA considerations
- Grammar, spelling, clarifications, cleanup

DomainKeys Identified Mail Sender Signing Policy

Eric Allman
Sendmail, Inc.

Sender Signing Policy Rationale

- Domain owners want to be able to control the use of their domain name
- Signing alone is not sufficient to achieve this if unsigned messages are deemed to be legitimate by recipients

Sender Signing Policy

- Primary content in today's (-01) version: "o=" tag (outbound mail policy)
  - "~" — domain doesn't sign all messages (neutral)
  - "–" — domain signs all messages; 3rd party signatures (3PS) should be accepted (strong)
  - "!" — domain signs all messages; no 3PS (exclusive)
  - "." — domain never sends mail (never)
  - "^" — do per-user policy lookup (user)
  - "?" — not all signed, no 3PS (weak) (not in -01)
- Does not need to be looked up if "From:" identity matches signing identity

Mailing Lists

- Lists that do not break signatures
  - No special requirements (“naive forwarding”)
- Lists that break signatures
  - Should probably re-sign for the list itself
  - Should run spam and virus checks before retransmit
  - Should verify incoming signatures, possibly reject on failure
  - Not compatible with NO3PS policies
- Note: multiple signatures not defined in spec

dkim-ssp Changes Since -00

- Document restructuring
- Added section on third party signatures and mailing lists
- Technical content unchanged