Apps: Architecture
SAAG: Security
*   Considerations*

Architecture

L. Levison
D. Crocker

PRIME: **Privacy Respecting Internet Mail Environment**

Internet Engineering Task Force Ninety-Two

Threats

- – Is purported creator/submitter of message is the actual?
- Service provider spoofing
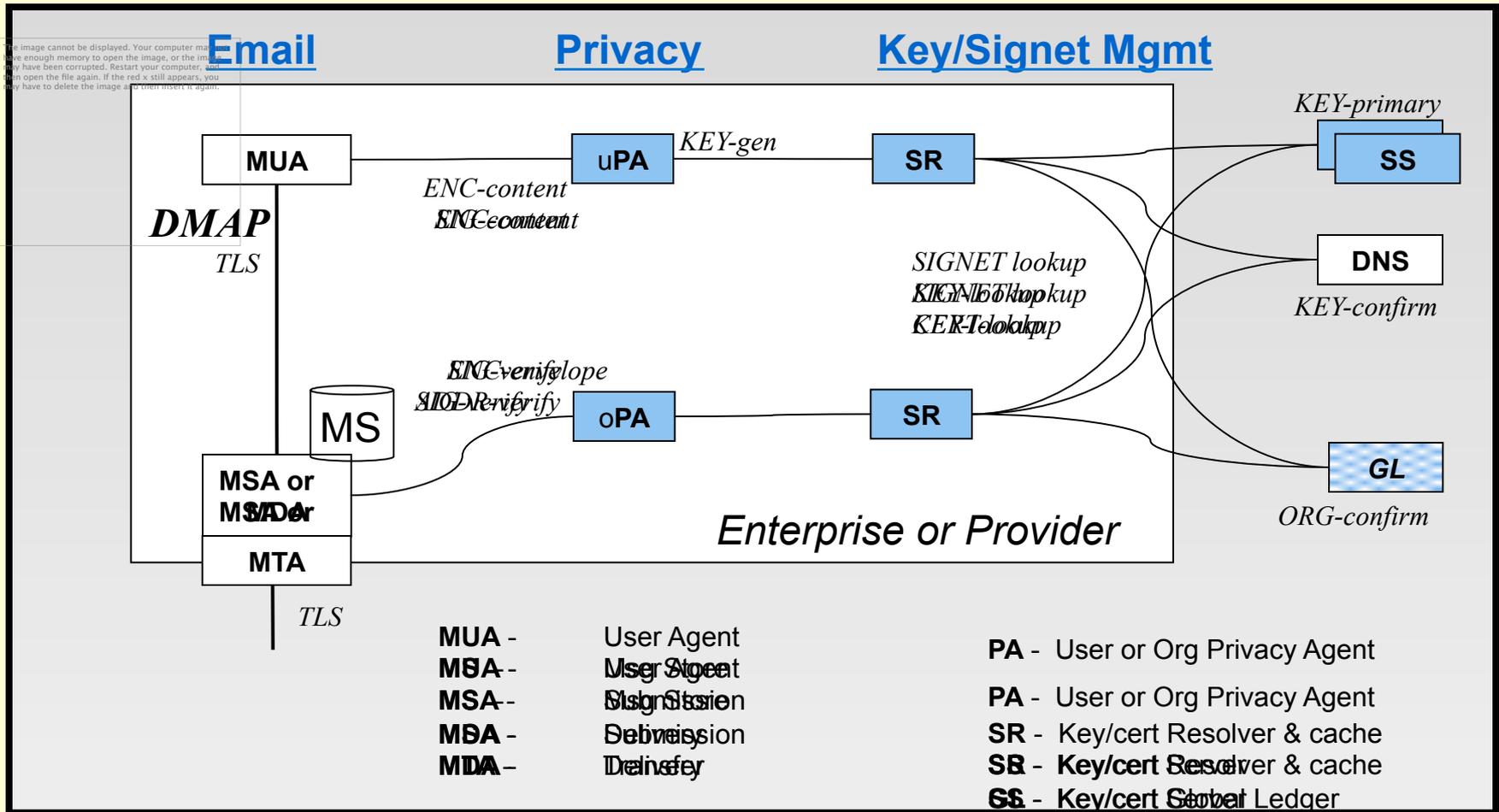 - – Is intended provider (mail, key, DNS) is the actual provider?
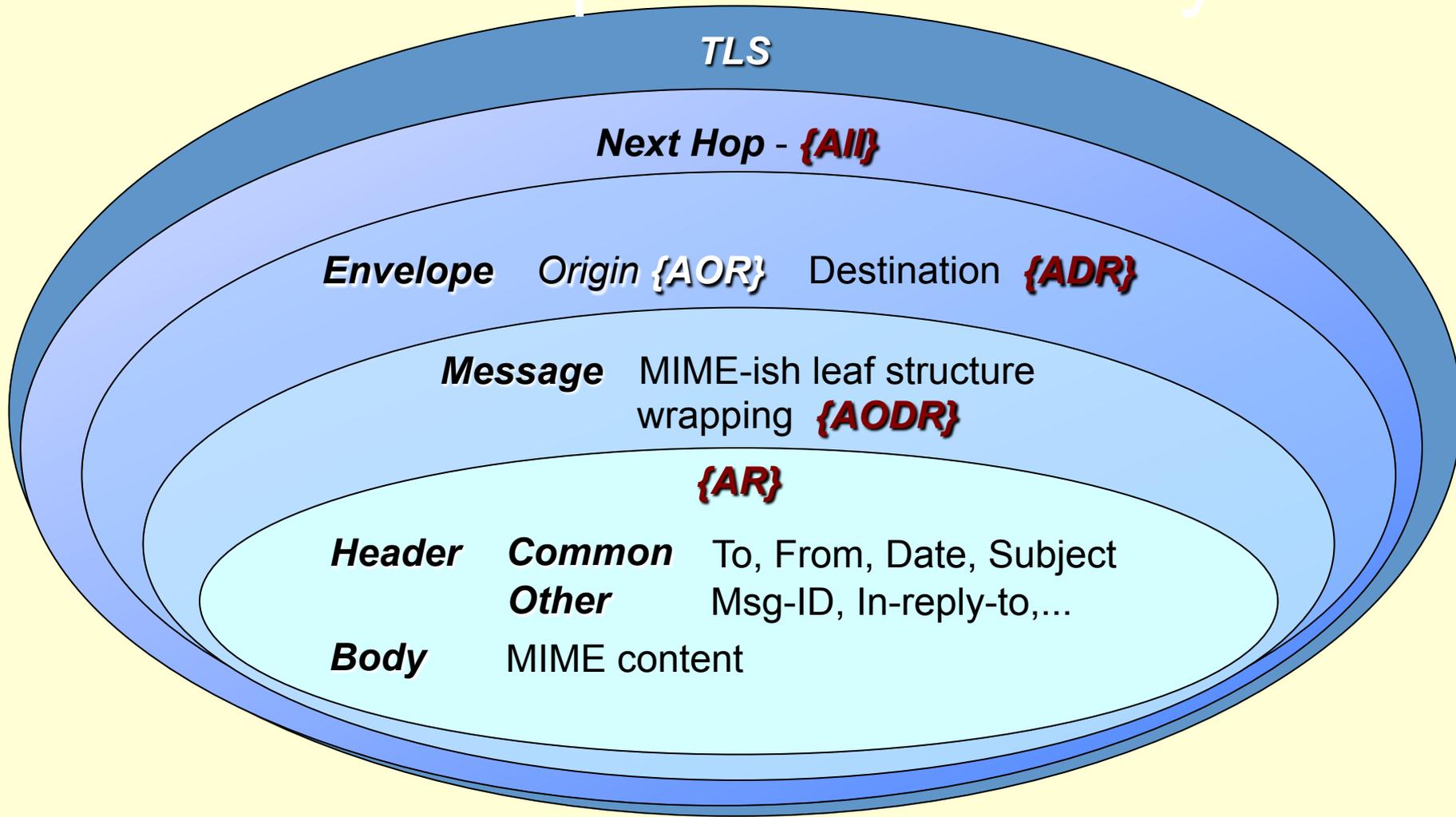
analyses; relationships and activity

Design Goals

- Distinguished by automated
- Uses layers of message-based end-to-end* encryption
- Provides message confidentiality, tamper protection and reduces the leakage of metadata along the handling path
- Strives to make security dependent on the complexity of a user's password and strength of their endpoint's defenses

* Automation allows the "end" to be a user's device, or server

PRIME Basic Components

Email   **Privacy**   **Key/Signet Mgmt**

MUA

DMAP
TLS

MS

MSA or
MSDAr

MTA

TLS

uPA

KEY-gen

SR

KEY-primary

SS

ENC-content
ENC-content

SIGNET lookup
KEY-lookup
CERT-lookup

DNS

KEY-confirm

ENC-envelope
SIG-verify

oPA

SR

GL

Enterprise or Provider

ORG-confirm

MUA - User Agent
MUA - User Agent
MSA - Sign Store
MSA - Submission
MTA - Delivery
MTA – Transfer

PA - User or Org Privacy Agent

PA - User or Org Privacy Agent

SR - Key/cert Resolver & cache
SR - Key/cert Resolver & cache
SS - Key/cert Server Ledger

PRIME Component Visibility

TLS

Next Hop - **{All}**

Envelope   Origin **{AOR}**   Destination **{ADR}**

Message   MIME-ish leaf structure wrapping **{AODR}**

{AR}

Header   **Common**   To, From, Date, Subject
             Other   Msg-ID, In-reply-to,...

Body   MIME content

Visibility: *A: Author*   *O: Origin*   *R: Recipient*   *D: Destination*

For More Of The

Good Stuff

BarBOF - Thursday evening

Docs
https://darkmail.info/spec

Discuss
https://darkmail.info/forums

Develop
https://darkmail.info/code

FIN