Email Privacy:
Gaps and IETF Opportunities(?)

D. Crocker

Brandenburg InternetWorking

4 August 2014

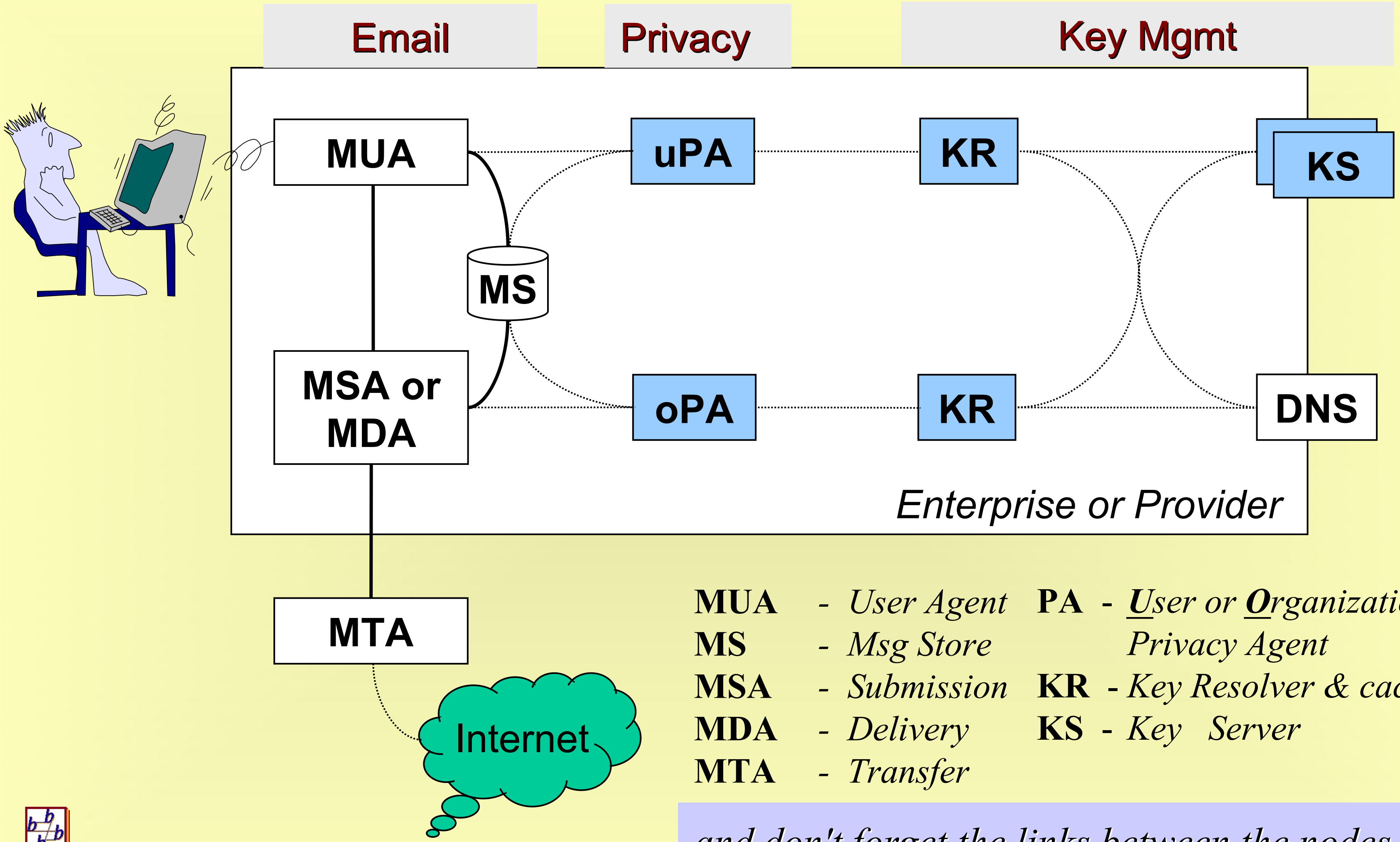
Considerations for future work

- **Suddenly very active space**
  - 35+ projects for email
  - 100+ projects for "messaging" and VOIP
- **Current projects not targeting IETF process**
  - But eventually, some will
- **How will be be able to *(eventually)* help?**
  - Let's *start* discussions, to anticipate this
  - Get email and security folk on a common page
  - Opportunities, frameworks, vocabulary, components
  - Beyond *"TLS Everywhere"* ™

Basic Email Message Components

- **Envelope** *(rcpt to, mail from)*
  - Difficult to deliver if dest address not in the clear...
- **Header**
  - User *(to:, from:, cc:, date:, subject:...)*
  - Ops *(received:, return-path:...)*
- **Content** *(body)*
  - Attachments
  - Structure

Basic Email Privacy Components



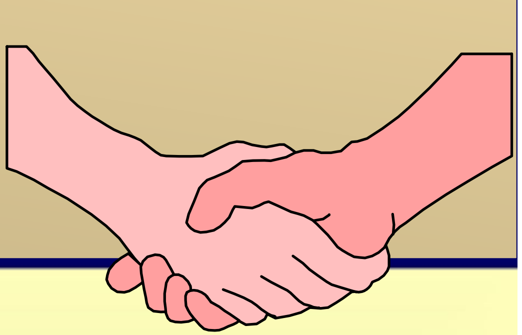
MUA	- *User Agent*	**PA**	- *User or Organization Privacy Agent*
MS	- *Msg Store*		
MSA	- *Submission*	**KR**	- *Key Resolver & cache*
MDA	- *Delivery*	**KS**	- *Key Server*
MTA	- *Transfer*		

and don't forget the links between the nodes...

Starting the Discussion...

- **A brainstorming effort**
- **Priming the pump**
- **Get your juices flowing**
- **A few (good) ideas**
  - So, ok, what are *your* suggestions...?

Key Management

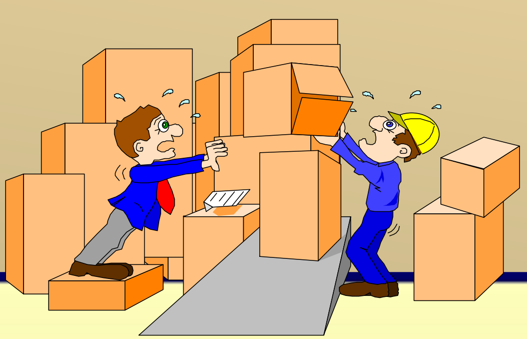


- **Assignment**
  - Probably mostly (human) usability issue; so... not for IETF?
  - New object -- more than a key and less than a (trust) certificate
    - Has identity-related attributes, eg., enhanced vcard & *not* X.509
- **Discovery**
  - DNS-based key lookup, eg., `mailbox._at.example.com`...?
  - TOFU?
- **Validation**
  - Multiple, independent sources?
  - Certificate transparency? (Where/how?)
- **Availability**
- **Revocation**
- **Rollover**

Key Management

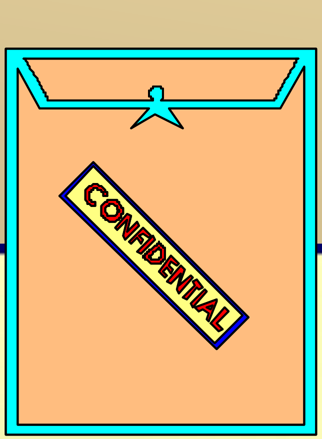
- **Mobility/Multi-platform/Distributed ops**
  - Access to keys from multiple platforms/venues
  - Access when disconnected
  - "Keybook" (like address book)
    - Standard format, for replication/exchange
    - Standard for access to remote keybook
    - Distinct 'personal keys' protable copy, with private keys
- **DNS Privacy**

Email Processing



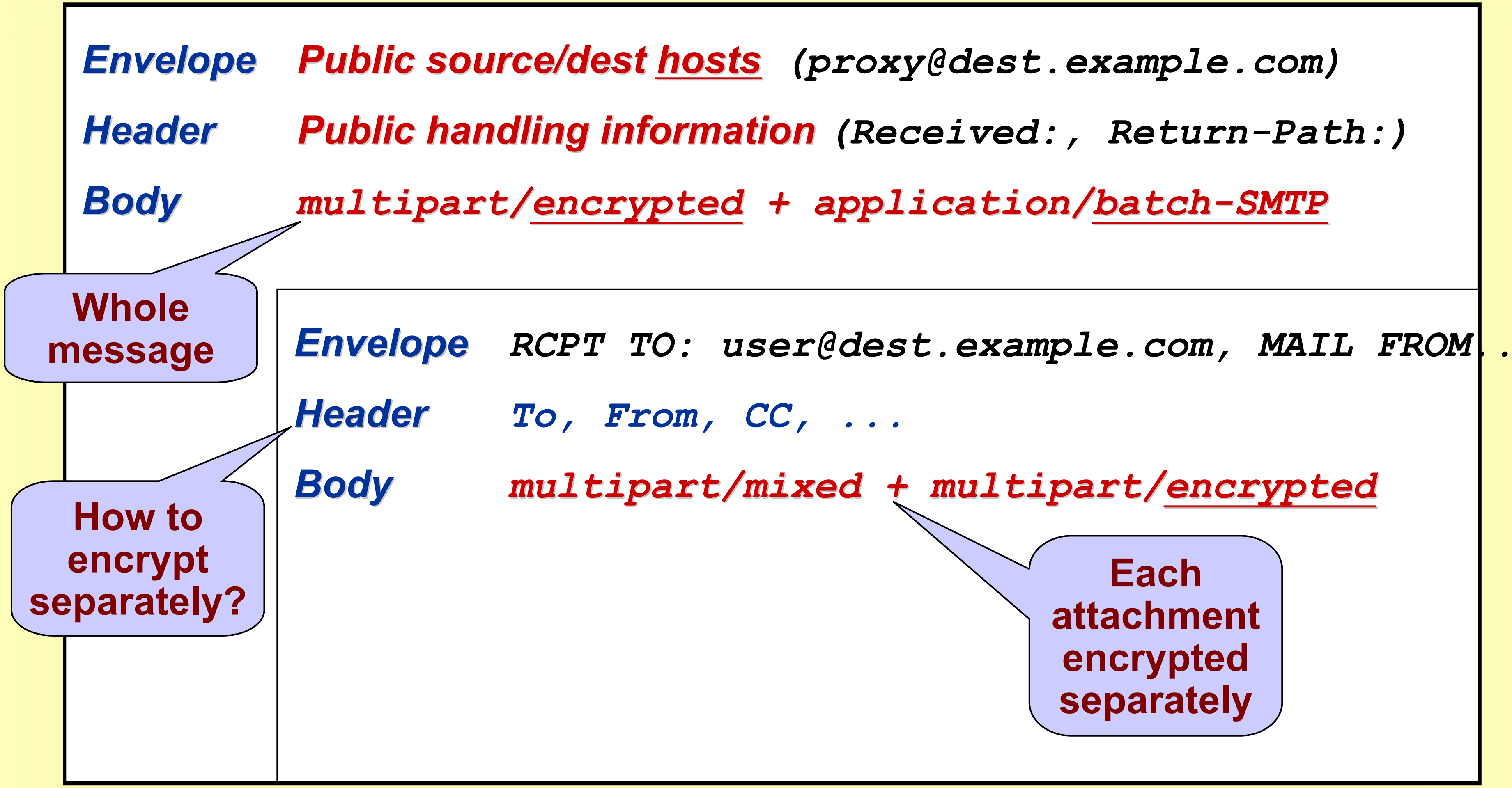
- **Compose**
  - Mostly usability?
- **Address**
  - Integrate keybook and DNS key lookup
- **Submit**
  - Per-component *and* whole-message encryption
  - Message packaging to support combined PGP & S/MIME recipients
- **Transmit**
- **Deliver**
- **Access**
  - Retain per-component encryption -- any imap changes?
- **Disposition**
  - File, reply, forward

Message Packaging



- **Onion packaging?**
  - Limit info in the clear during transit
  - Public SMTP Envelope, to get to MDA
  - Private, encrypted envelope, based on BSMTP (RFC 2442)
- **Header**
  - Public, for ops handling fields
  - Private, encrypted for user-user information,
- **Content**
  - Per-attachment encryption, for efficient access to IMAP server

Perhaps do SMTP as...



Envelope *Public source/dest hosts* `(proxy@dest.example.com)`

Header *Public handling information* `(Received:, Return-Path:)`

Body `multipart/encrypted + application/batch-SMTP`

Whole message

Envelope `RCPT TO: user@dest.example.com, MAIL FROM..`

Header `To, From, CC, ...`

Body `multipart/mixed + multipart/encrypted`

How to encrypt separately?

Each attachment encrypted separately