Bounce Address Tag Validation (BATV)

D. Crocker
J. Levine
Sam Silberman
Tony Finch

IETF
San Diego
2004
BATV – Detecting forged MailFrom

- Digital signature
  - Key based on RHS domain

- Permit multiple schemes
  (Sorry, but no choice)

- Meta-syntax on LHS (local-part) for parameters
  - Permits finding mailbox without understanding sig
  - Hard limit of 64 bytes for total of local-part

mailbox@example.com  $\rightarrow$

batv=mailbox/scheme/parms@example.com
Bounce Address Evaluation Venues

Original Relay

Bounce Receipt

MTA

MDA

MTA

MTA

MTA

Bounce Generation

MSA

MDA
Base Scheme – PSB0

- Private Signed Bounce zero
  - Detected invalid received bounces
  - Interpreted only by issuer
  - Limited replay protection

\[
sig-val = \text{key-id} \\
\text{encrypt (<addr-spec>, timestamp, random-string )}
\]
Approach for Public Key Scheme

- Based on content standard, when available
- Use all of the mechanism, but tune computation to MailFrom limitations
  - E.g., hash the signature into a short string.