



IBM Research Antispam Task Force

# Spam Reduction through Sender Verification

Barry Leiba  
IBM T.J.Watson Research Center

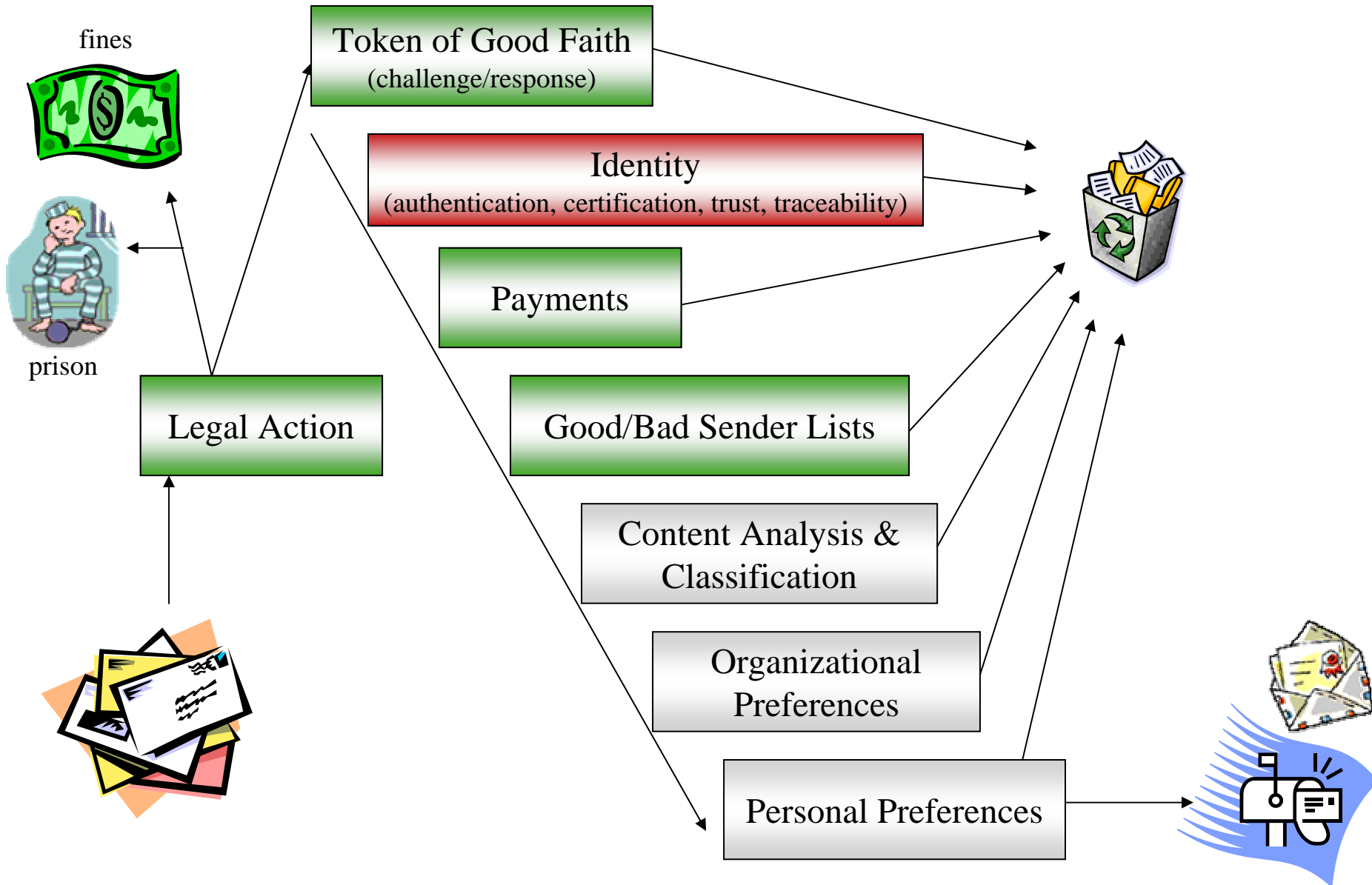
November 2004

© 2004 IBM Corporation

## Sender Verification Goals

- Determine with a reasonable degree of certainty that the message was sent from where it says it was.
- Increase efficacy of “good” and “bad” sender lists.
- Increase accountability and enable legal efforts.
- Enable more effective use of challenge/response or payment systems.
- Reduce the opportunity for “phishing”.
- Reduce “bad bounces”.

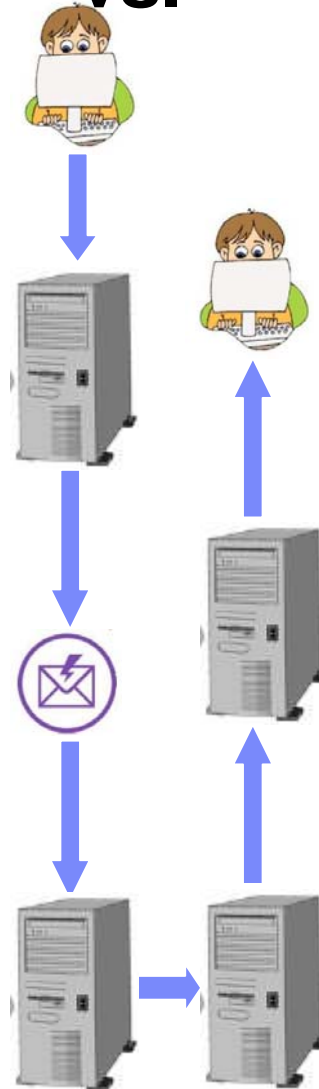
# The Anti-Spam Gauntlet



## IP Address

- Best at entry from Internet
- Immune to modifications
- Difficulties with forwarding
- Can't be layered
- Simpler implementation
- May be unclear or inflexible with verification
- Works through DNS
- Only signs for domain
- Controlled by sending domain

vs.



## Signature

- Works well at any point
- Susceptible to modifications
- Works well with forwarding
- Can be layered
- Requires certs & cert mgmt
- Explicitly says what is verified
- Uses DNS or PKI
- May allow signing for user
- Controlled by sending domain

## Limitations

- We only validate what we **say** we validate.
- Spammers and phishers can simply admit who they are – to the infrastructure.
- If spamming domain doesn't participate, we can only scrutinize.
- It's **very important** for major legitimate domains to participate.
- Still possible to fool the end user.
- **Requires** changes to MUAs.

# Testing Requirements

- Non-participating legitimate sender.
- “Participating” spammer.
- Transient failures
  - Can’t do DNS lookup or access key server
- Non-transient failures
  - Header modifications
  - Appending to message body
- Performance with forwarders & mailing lists.
- Anonymous mail – free speech issues.
- Solid enough to hold up in court?

## There Are No Silver Bullets

- Diverse approaches are promising and can help.
- Most introduce additional problems or concerns.
- None of them will solve the whole problem.
- Each has fanatical supporters who disagree.
- Partisans of “Silver Bullets” argue unproductively.
  
- **Open standards are key** to implementing anti-spam mechanisms.
  
- **Multiple approaches must work well together!**