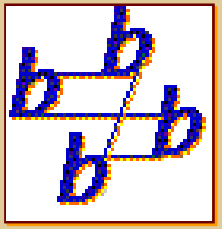
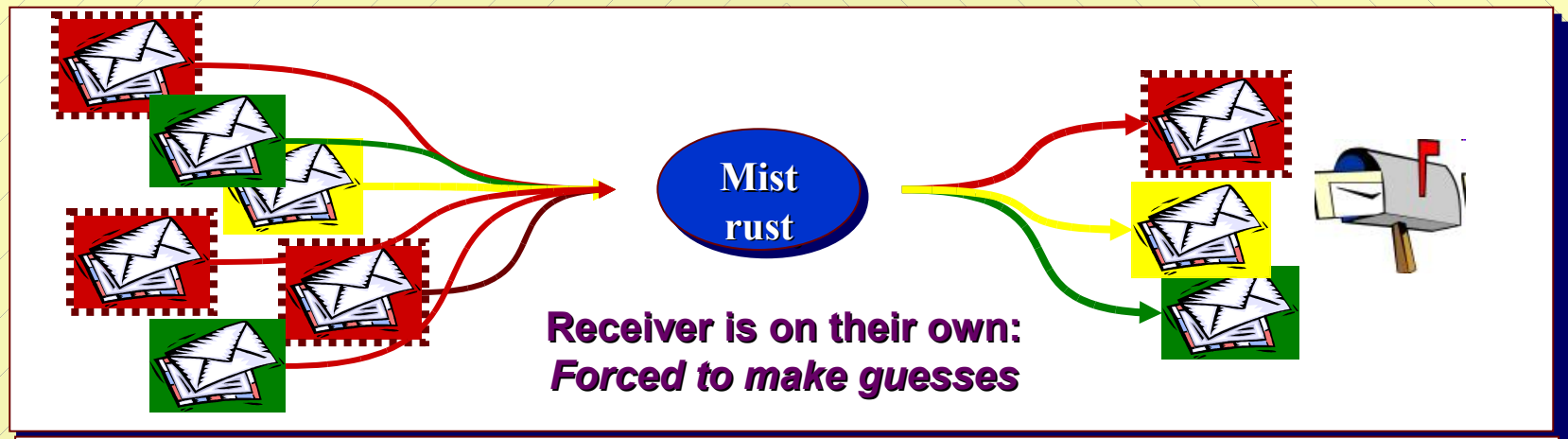


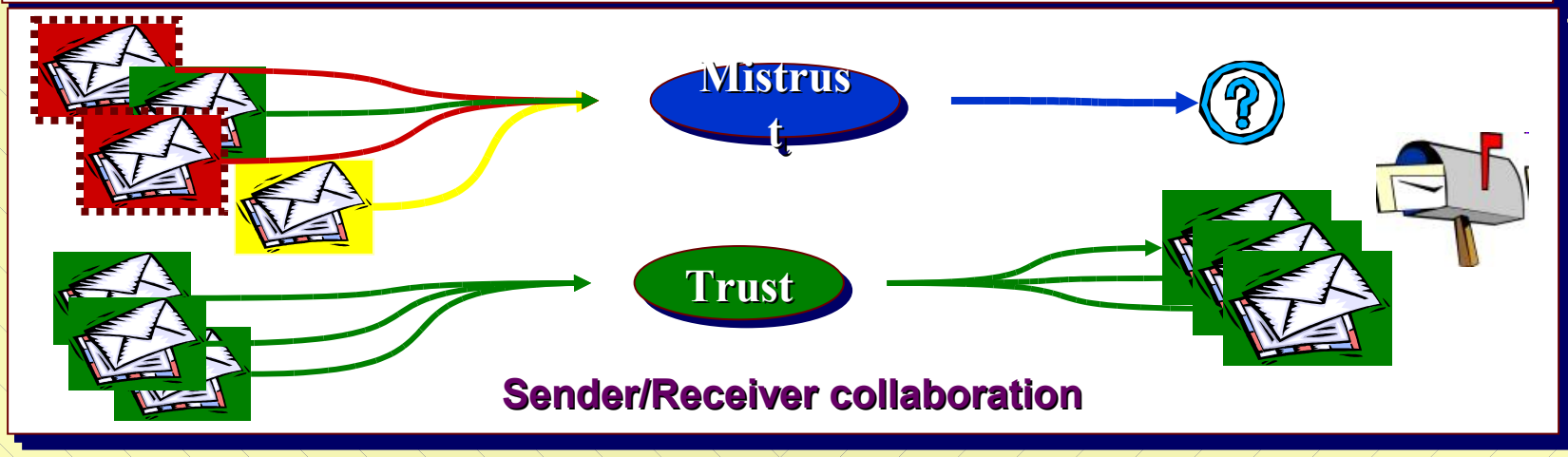
Email Trust
Does Not Look for Miscreants

Dave Crocker
Brandenburg InternetWorking
bbiw.net

SF INET – 7 May 2010

Mistrust vs. Trust





What is DKIM for?

- **Means a message is not spam**
- **Guarantees delivery**
- **Puts a domain name on a message**
- **Validates a message**
- **Authenticates the author or origin of a message**
- **Authenticates the sender of a message**

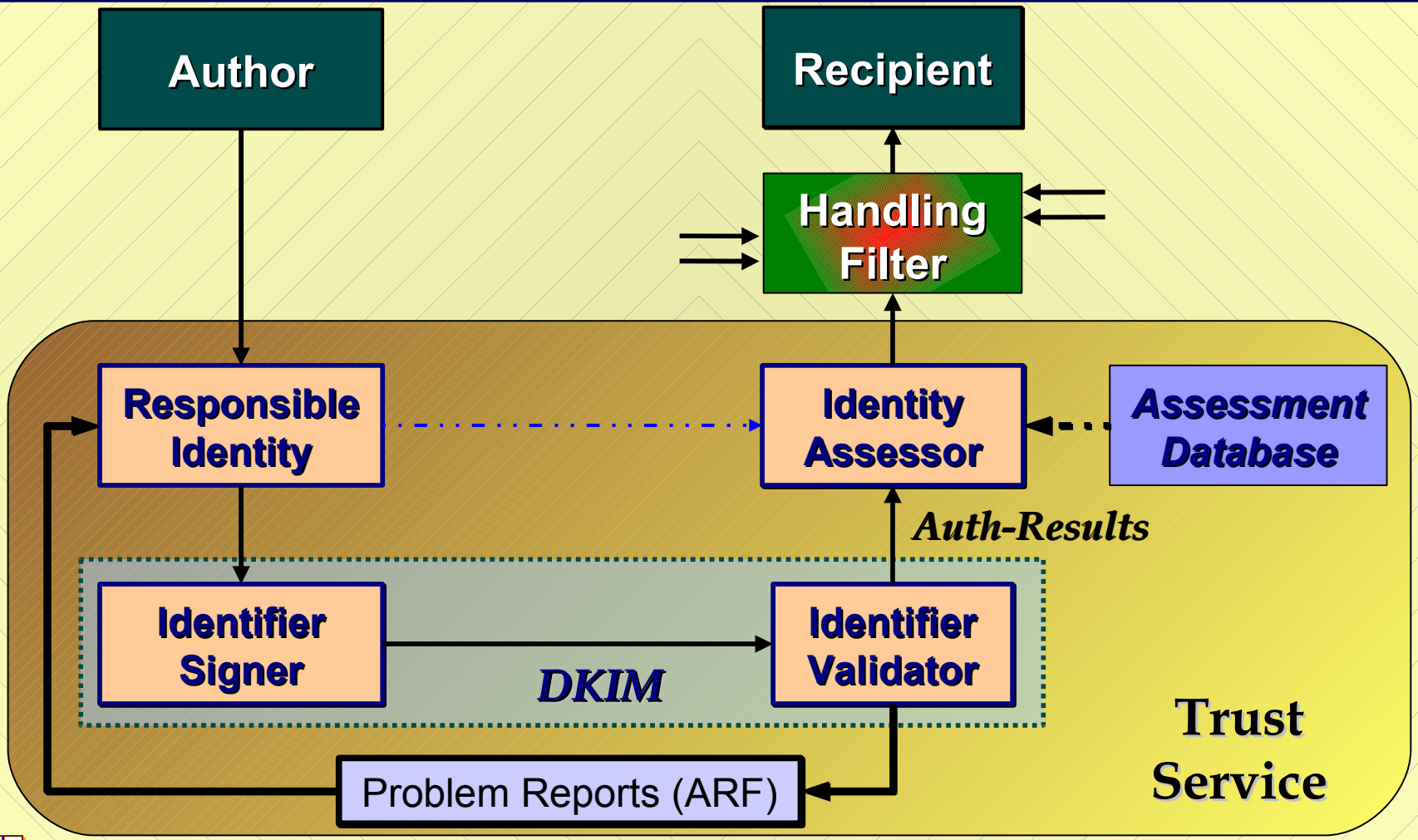
- **What DKIM *really* does**
  - Allows an organization to claim responsibility for transmitting a message, in a way that can be validated by a recipient.
  - The organization can be the author's, the originating sending site, an intermediary, or one of their agents.
  - A message can contain multiple signatures, from the same or different organizations involved with the message.

Differential Handling, with Trust as a Component

Organizational Trust

Stream Risk	Low	Medium	High
Low	**BENIGN**: *Moderate filter*	**DILIGENT**: *Mild filter*	**PRISTINE**: *Accept*
Medium	**UNKNOWN**: *Strong filter*	**TYPICAL**: *Targeted filter*	**PROTECTED**: *Accept & Contact*
High	**MALICIOUS**: *Block & Counter*	**NEGLIGENT**: *Block*	**COMPROMISED**: *Block & Contact*

Trust Service Architecture



Identifying Mail Streams

- **An organization has multiple "types" of mail**
  - Corporate
  - Transactions (purchase order, order confirmation...)
  - Proposals
  - Marketing mass mailings
  - Customer Support
- **Label them with different DKIM d= subdomains to help receiver**
- **Allow different reputations to develop**

Different and Complementary

- **Mistrust**
  - Bayes, Blacklists, etc.
  - Look for mail to **reject**
- **Trust**
  - DKIM, SPF, Whitelists
  - Look for mail to **accept**