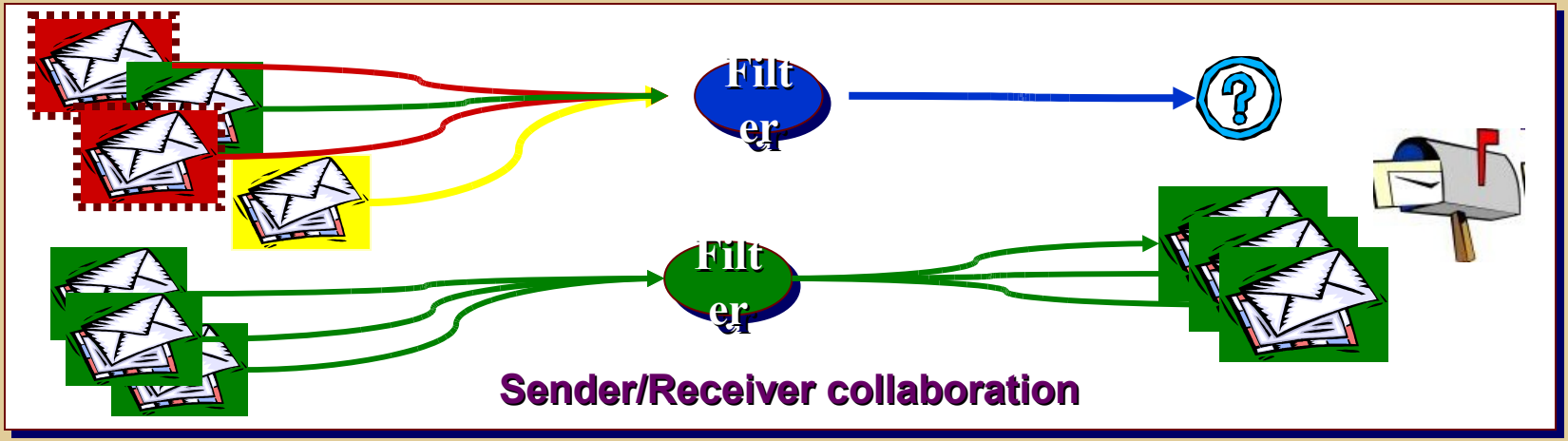
The Truth About: Trust and DKIM

Dave Crocker
Brandenburg InternetWorking
bbiw.net

APCauce – Kuala Lumpur – March 2010

Mistrust vs. Trust



To repeat: Mistrust vs. Trust

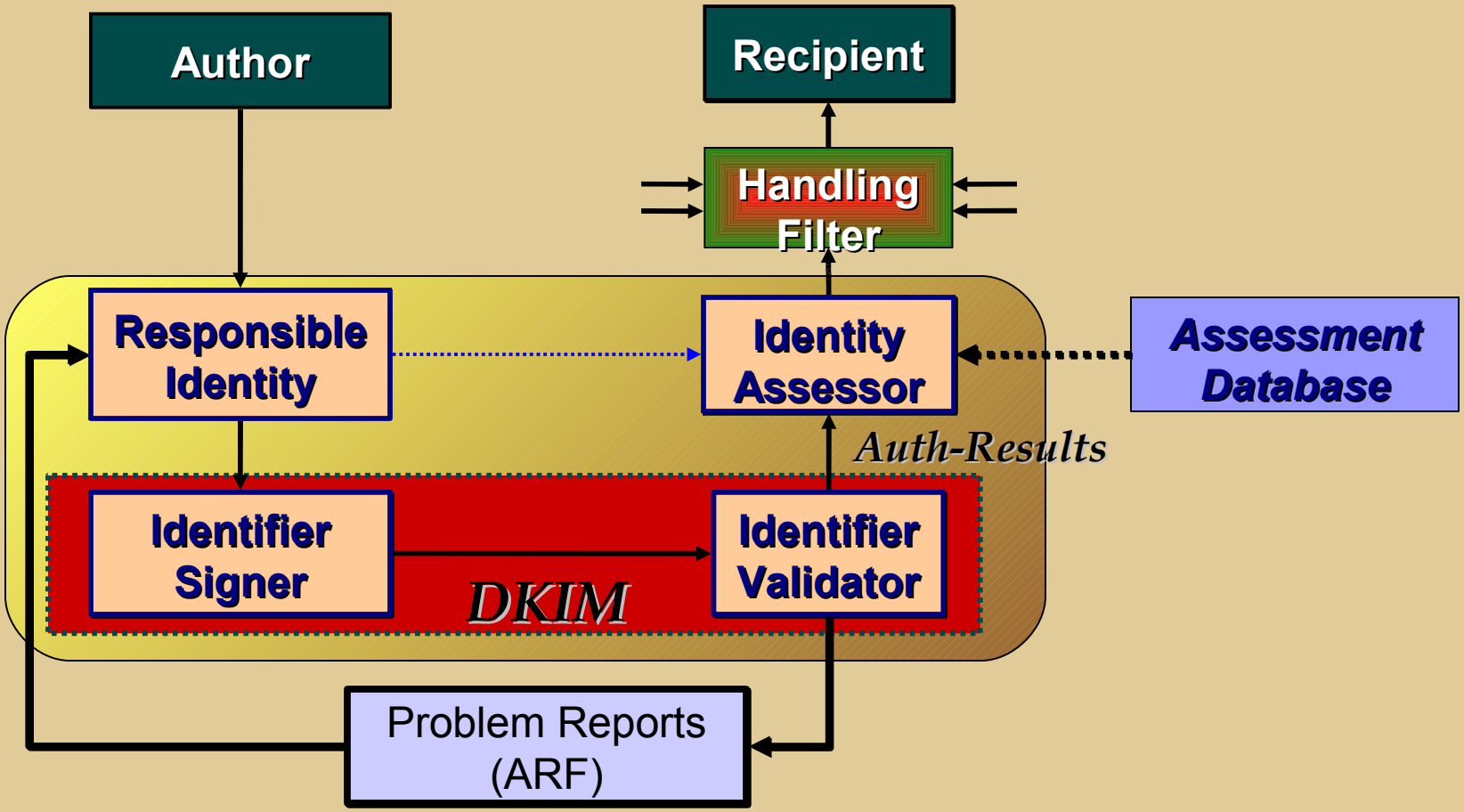
- **Mistrust**
  - Sender actively trying to trick receiver
  - Mail is usually spoofed
  - Heuristics, to distinguish valid from spoofed
- **Trust**
  - Sender is collaborating, at least for identifier
  - With valid identifier is valid, assessment (reputation) not confused by “noise” of bad actors

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.

Trust Service Architecture



Differential Handling, with Trust as a Component

Stream Risk	Organizational Trust: Low	Organizational Trust: Medium	Organizational Trust: 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*

Identifying Mail Streams

- **An organization has multiple "types" of mail**
  - Corporate
  - Transactions (purchase order, order confirmation...)
  - Proposals
  - Marketing mass mailings
  - Customer Support
- **Allow different reputations to develop under different labels**

- **Label them with different DKIM d= subdomains**
- **For example:**
  - corp.example.com
  - transact.example.com
  - bulk.example.com
  - free.example.com
  - paid.example.com
  - uk.example.com
  - faculty.example.edu
  - student.example.edu

ADSP: Author Domain Signing Practices

- **Exploring mistrust**
  - Worry, if there is no signature based on From: field domain…
- **Domain owner can publish practices for signing with From: field domain**
- **DNS TXT record under**
  - _adsp._domainkey.<from domain>

Protecting Spoofed "Brands"

- **ADSP protects the wrong information**
  - Too easy to work around
  - End users do not see From: field address
- **Instead, perhaps we should…**
  - Link brand name to domain name via registry
  - For messages appearing to be from Brand, confirm From: field domain name

References

- **DKIM home page – http://dkim.org**
  - DKIM 3-slide Teaser
  - DKIM Service Overview – RFC 5585
  - FAQ
  - Wikipedia entry on DKIM
  - Development, Deployment and Operations
  - Discussion Lists

- **DKIM Signatures – RFC 4871 + RFC 5672**
- **ADSP – RFC 5617**
- **Auth-Results – RFC 5451**
- **ARF – http://mipassoc.org/arf/ http://www.ietf.org/dyn/wg/charter/marf-charter.html**