Messaging Anti-Abuse Working Group

DKIM Implementation

MAAWG Training Series

Segment 1 of 4 on DomainKeys Identified Mail

From the onsite training course at the MAAWG 18th General Meeting
San Francisco, February 2010

Messaging Anti-Abuse Working Group

DKIM Implementation – Video Segments

Segment 1 20 mins.	Segment 2 20 mins.	Segment 3 18 mins.	Segment 4 35 mins.
Theory	Theory	Practical	Practical
• General DKIM Architecture • What DKIM Is and Isn't	• DKIM Protocol Details • Separate Mail Streams & Signing Practices	• Planning • Keys and Policies	• Signing Software • Verifying Software • Testing, Other Topics • Q&A

Segment 1 Covers

Theory:

- General DKIM Architecture
- What DKIM Is and Isn't

Dave Crocker
MAAWG Senior Advisor
Principal, Brandenburg InternetWorking
dcrocker@bbiw.net

Messaging Anti-Abuse Working Group

DKIM Implementation – *"What"*

Dave Crocker

Brandenburg InternetWorking

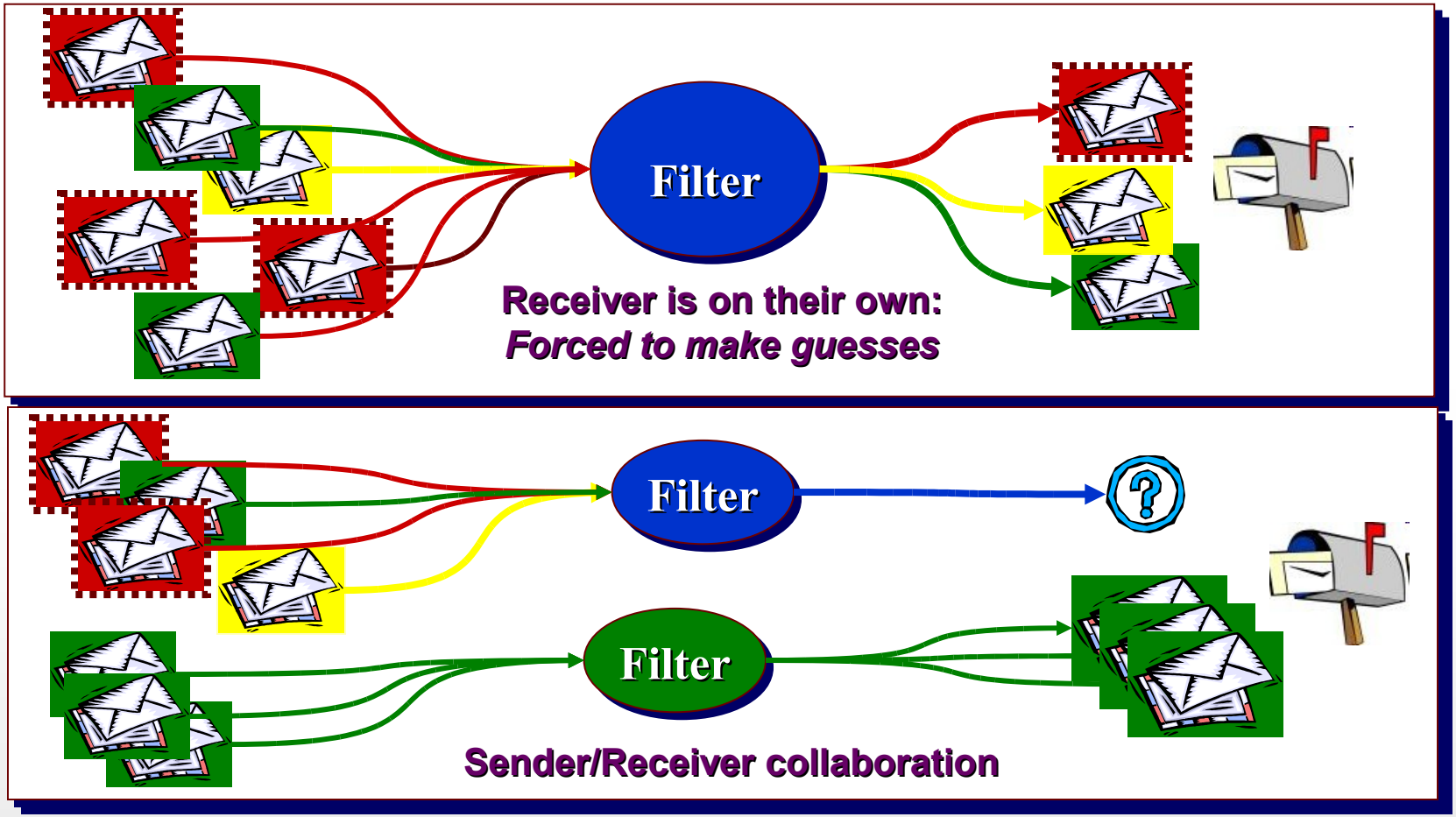
and

Senior Technical Advisor, MAAWG

Agenda –
What: DKIM in Trusted Email

- Trust vs. Mistrust
- What is DKIM and What is it for?
- DKIM Service Architecture
- Signature Basics
- ADSP
- Reporting Basics

Mistrust vs. Trust



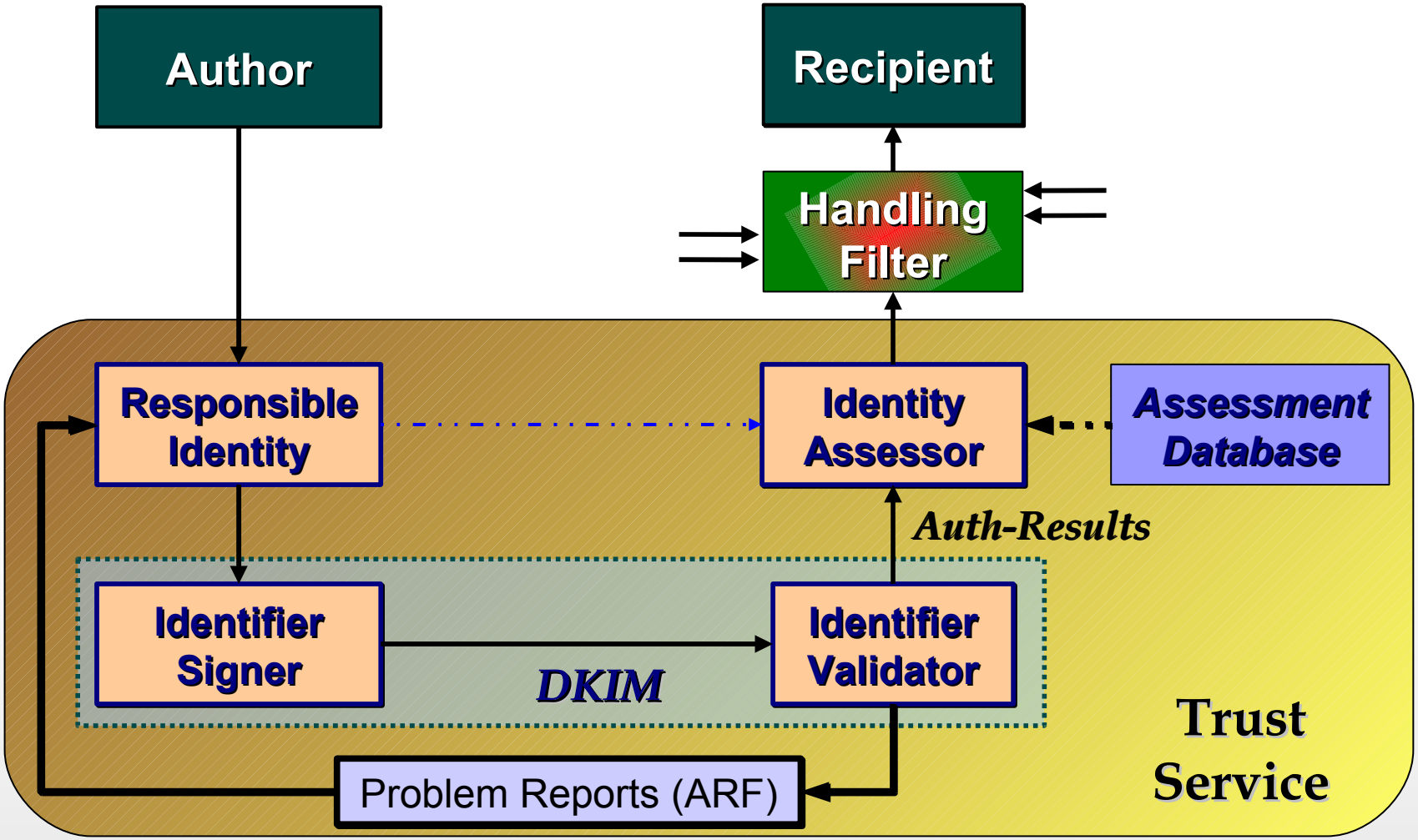
Differential Handling, with Trust as a Component

MAAWG

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



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.

DKIM Service Architecture