

A Policy Driven Approach to Email Services

Saket Kaushik

Paul Ammann

Duminda Wijesekera

William Winsborough

Ronald Ritchey

George Mason University

Outline

- Spam: a problem
- Current and proposed solutions
- Our approach: policy-controlled email transmission
- Current mail transfer protocol
 - Description and inadequacies
- Overview of our approach
 - Policy architecture
 - Extensions to SMTP

Spam: A Problem

■ STATISTICS:

- >30 billion email messages sent per day, ~ 120 million email users in US¹.
- >2 million mail transfer agents (other studies).
- >50% of all emails sent are spam¹.
- Economic costs between \$10 b - \$87 b annually¹
- “Spam is about to kill the ‘killer app’ of the Internet.” – Orson Swindle (FTC commission)

1. Deborah Fallows: Spam, How it is hurting email and degrading life on the internet.

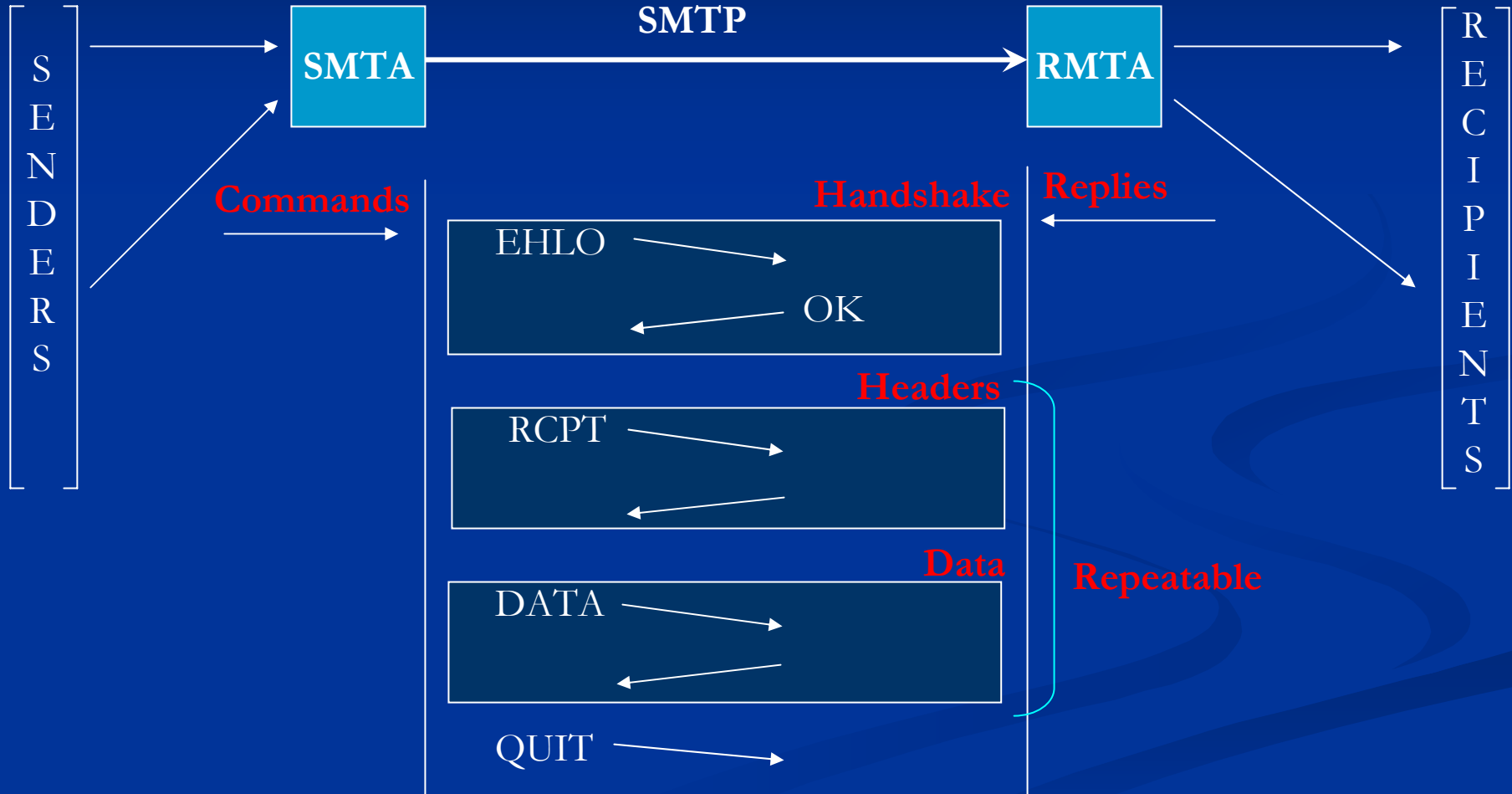
Current and Proposed Solutions

- Legal
 - Local laws and international agreements
- Technical
 - Spam filters (content based approach)
 - Turing tests (human participation)
 - Metadata-based reputation (e.g., Project-Lumos, Razor)
 - Sender authentication (e.g., E-caller ID)
- Economic
 - Cost-based solutions (e.g., E-stamps / Attention Bonds)

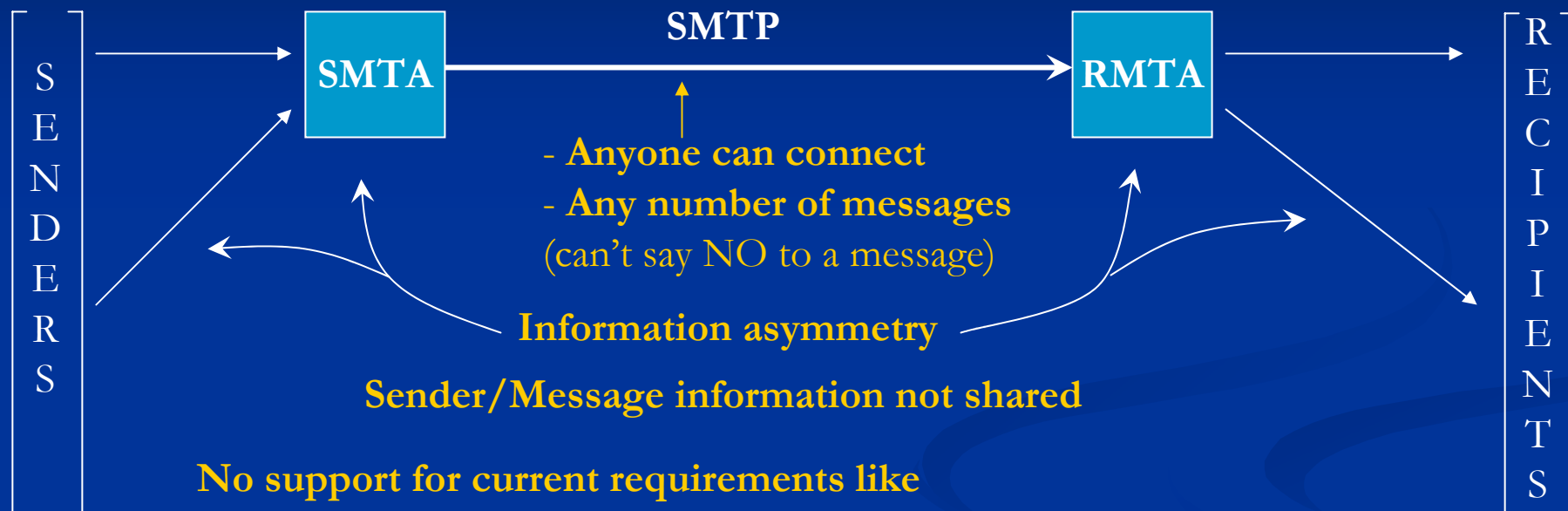
A Holistic Approach

- Email pipe has several components
- Each is operated by a party motivated by its own interests
- Component behavior will be governed by policies written by interested parties
- Protocol extensions support greater control on the part of down-stream parties
- Mechanisms such as reputation services help to motivate cooperation in faithfully enforcing policies

Email Transmission: SMTP Protocol



Inadequacies

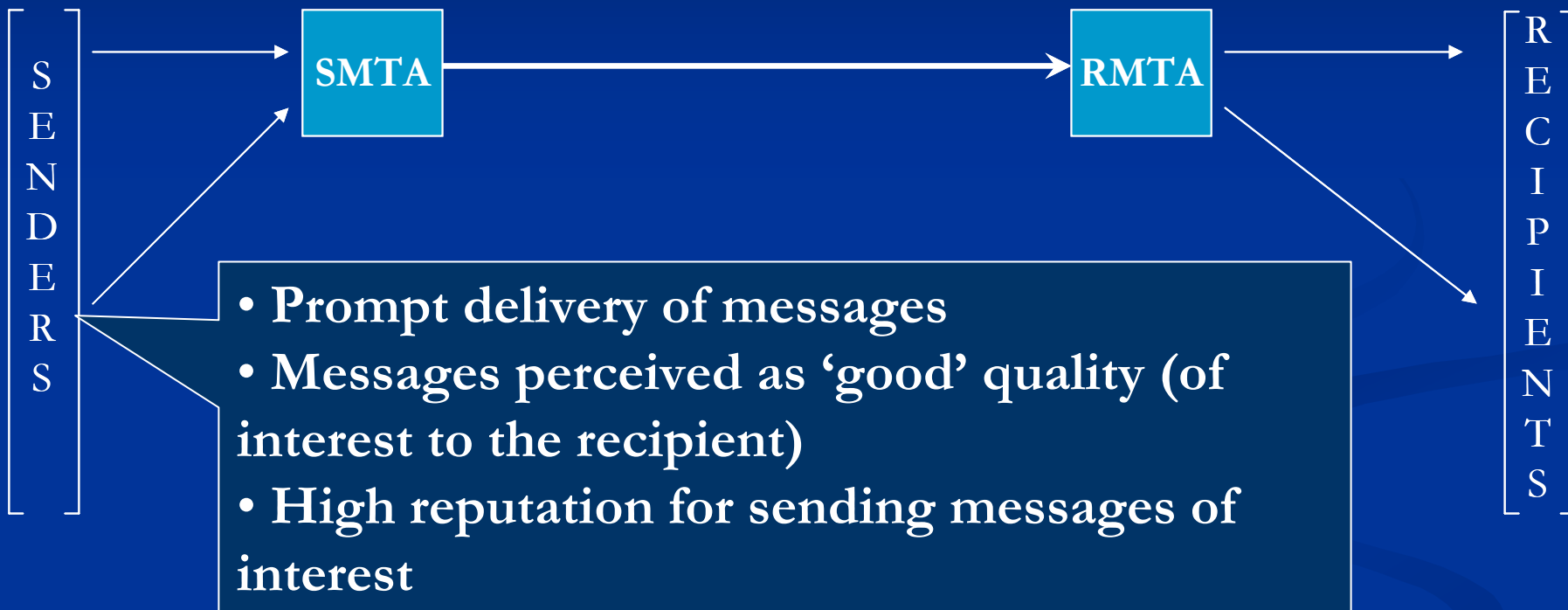


No support for current requirements like

- Filtering 'low quality' messages OR prioritizing 'good' messages.
- Email reputations OR sharing of benefits across mail agents.

Such mechanisms are being used in practice. Protocol does not fit with what is being done or desired to be done.

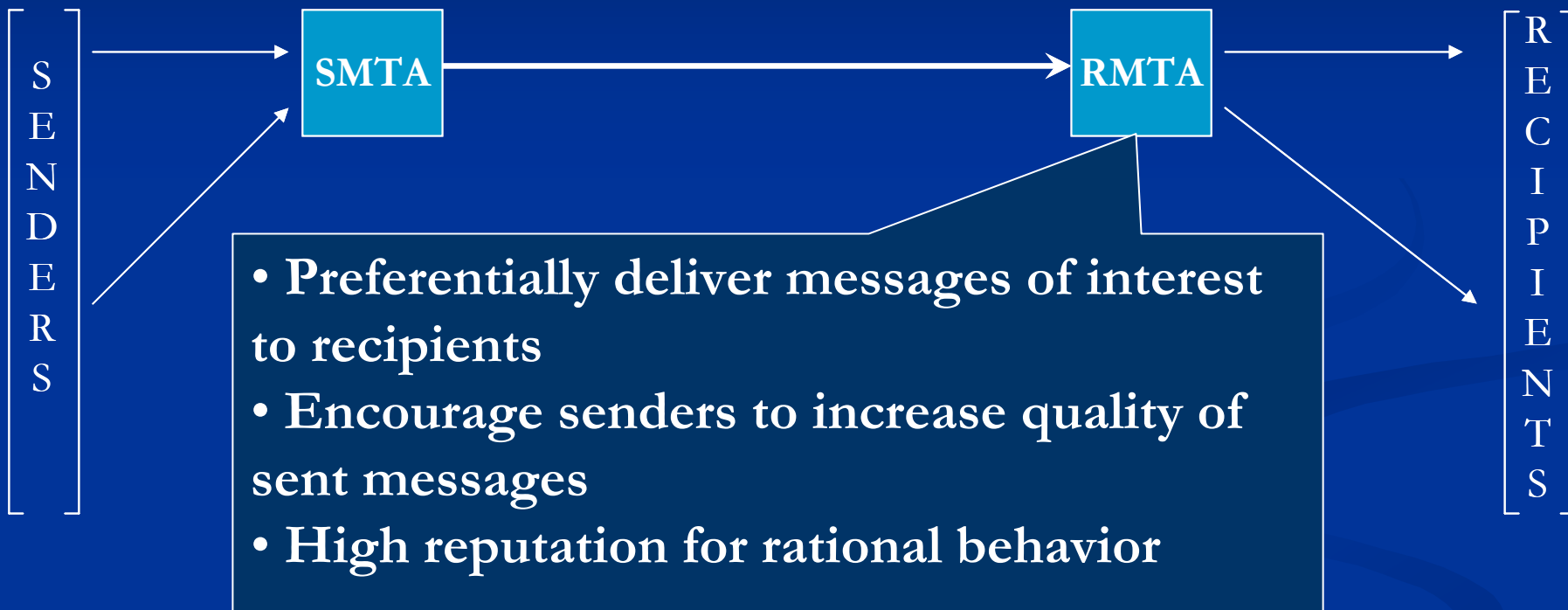
Interests of Each Party



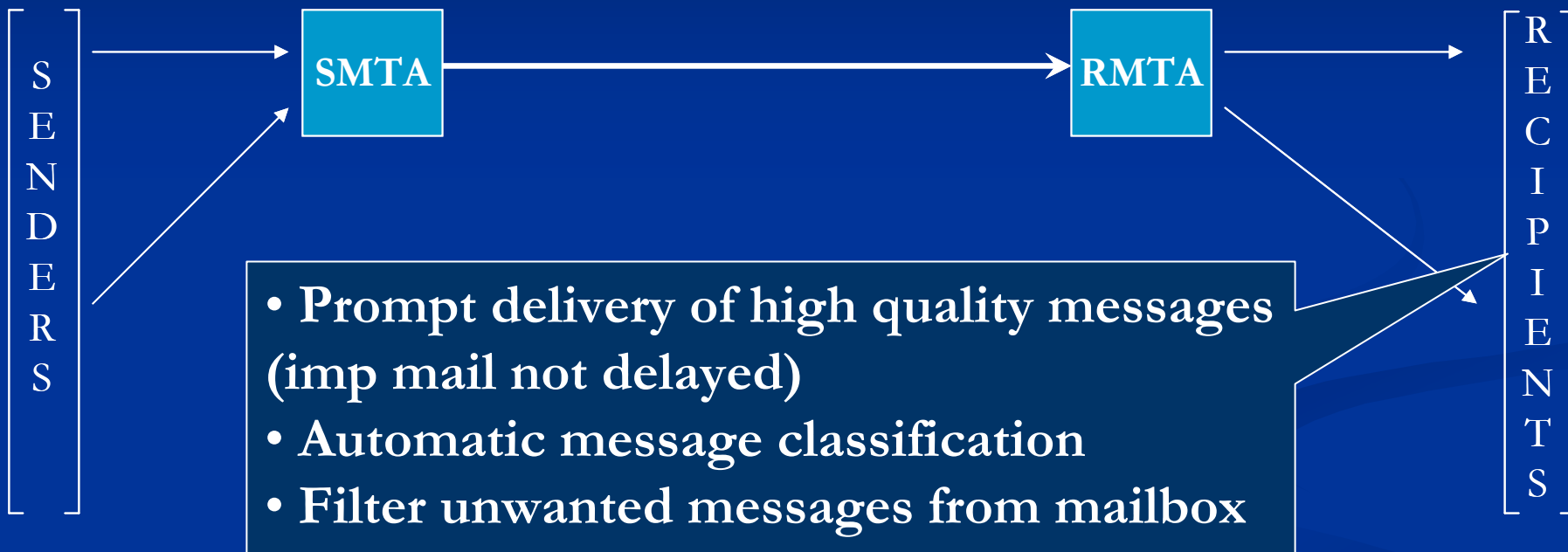
Interests of Each Party



Interests of Each Party



Interests of Each Party



Quality of Messages

- Message quality is 'high' if
 - considered so by the recipient **after reading it**
- Decision whether to transmit must be made based on *estimators* of quality
 - sender reputation, authentication, bonding
 - addition of metadata improves quality of estimate

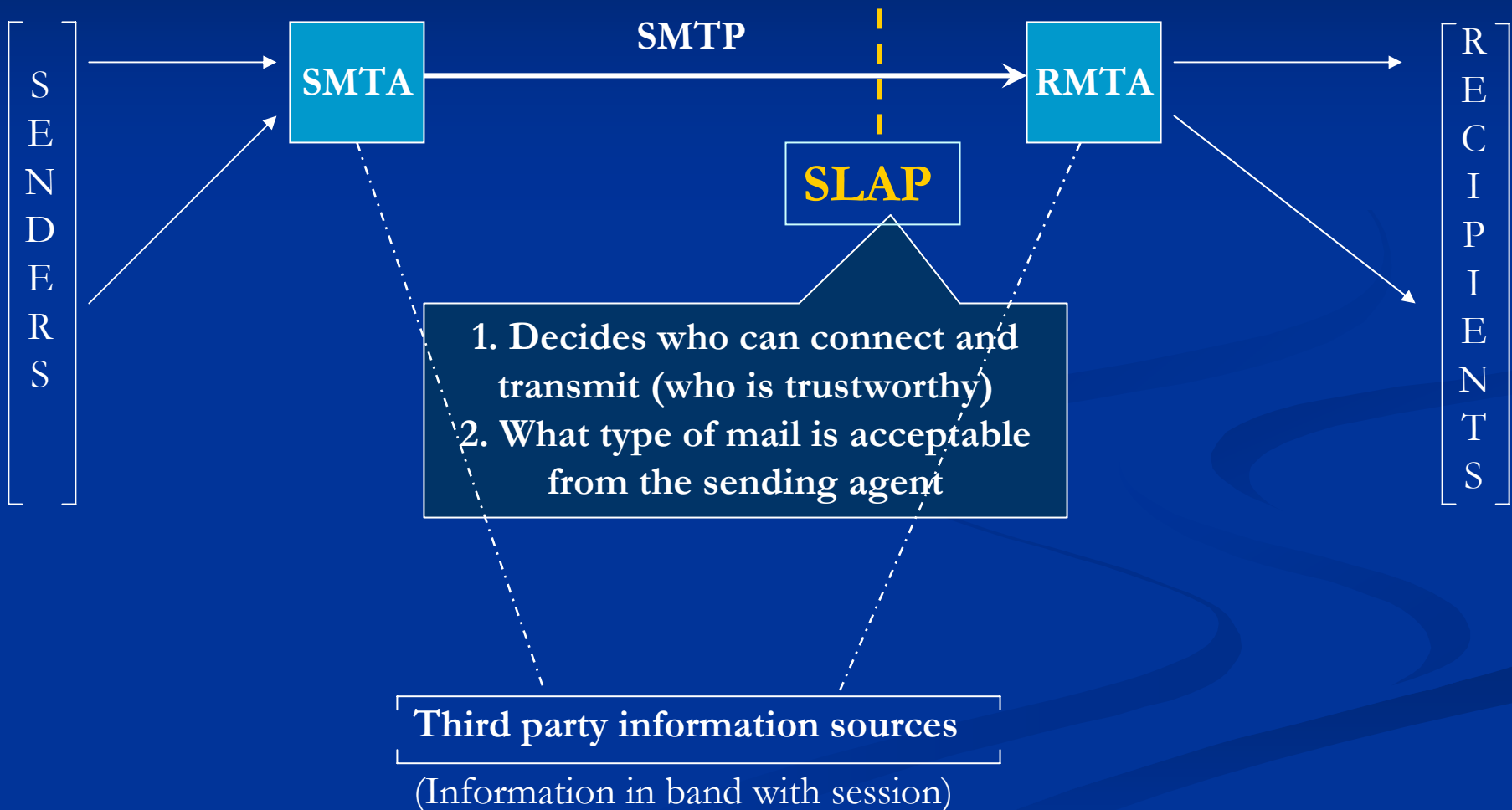
Sender Authentication

- Strong authentication might not be possible
- 2-level sender authentication (supported by bonds/reputations/ sunk costs) may be good enough
- We assume sender authentication will be soon available for email. Hence:
 - “Senders will either have a history or be treated as a newbie”
- Question: Which message to read in a huge set of source authenticated messages?

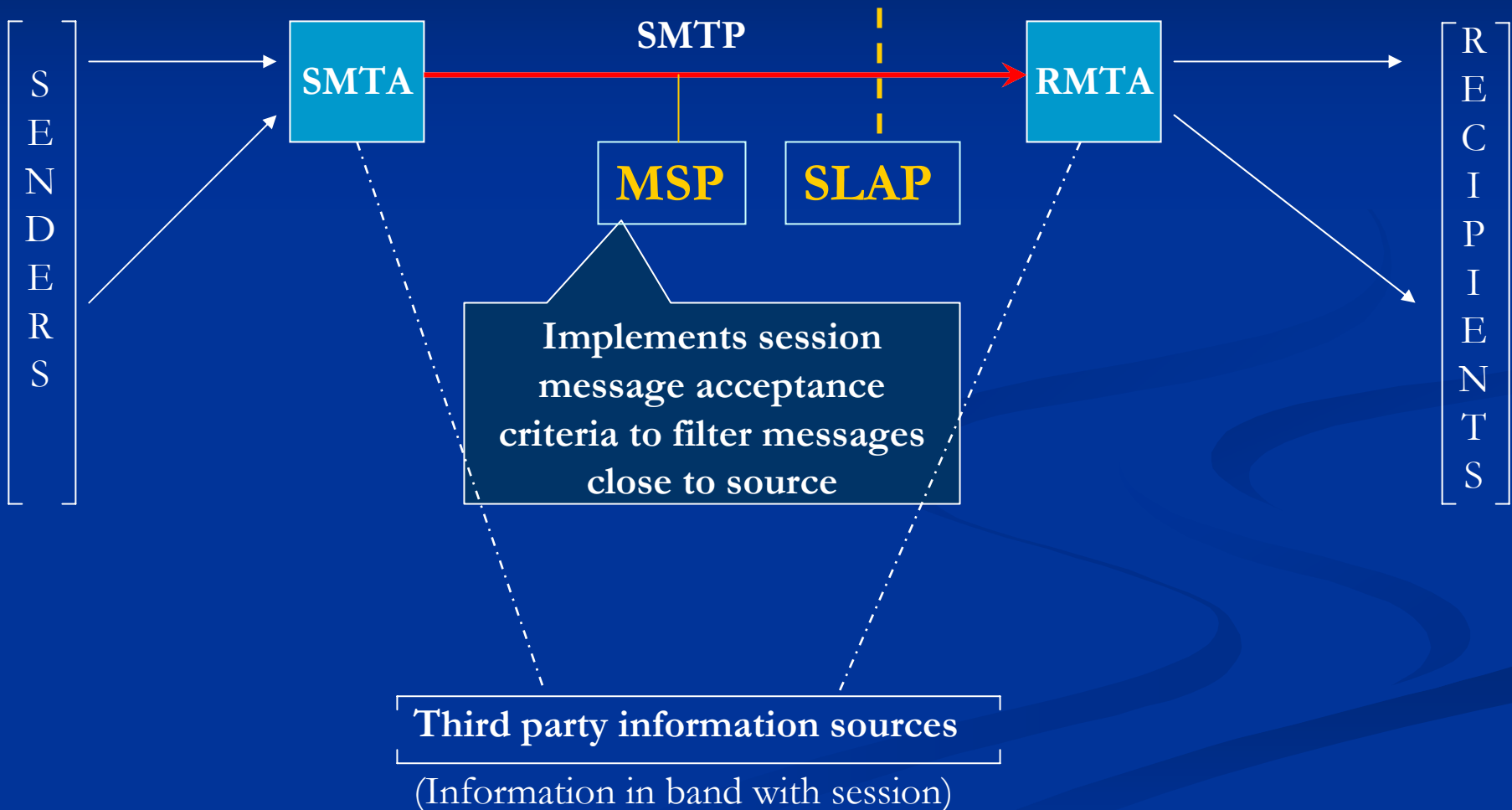
Control Decisions

- Each agent has interests as well as partial control of the pipe
- Following decisions can be made for routing a message:
 - Forward/send message
 - Add assertions to a message (increase in quality)
 - Drop or kill a message
 - Delay a message (prioritize higher quality messages)

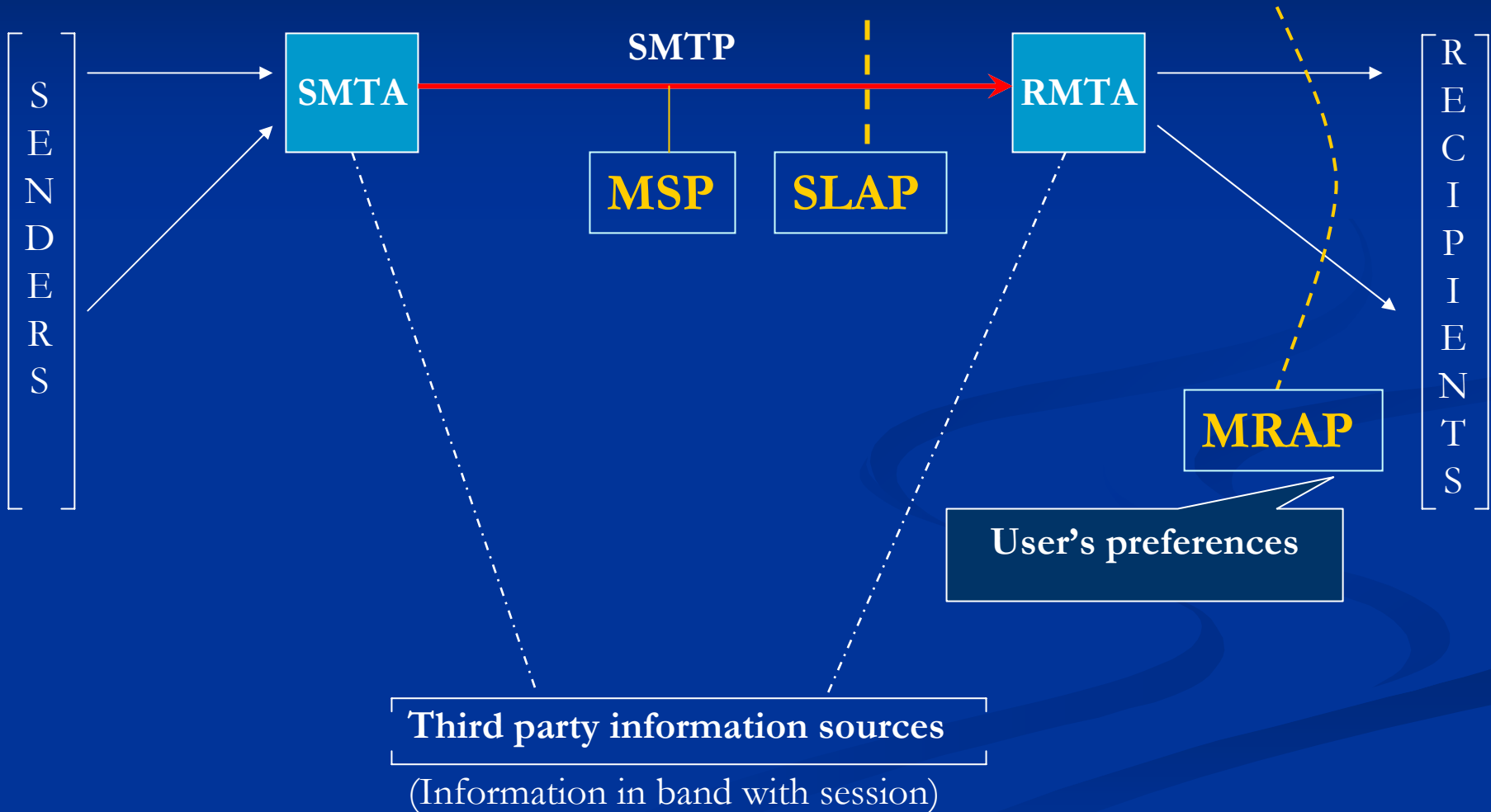
The Policy Architecture



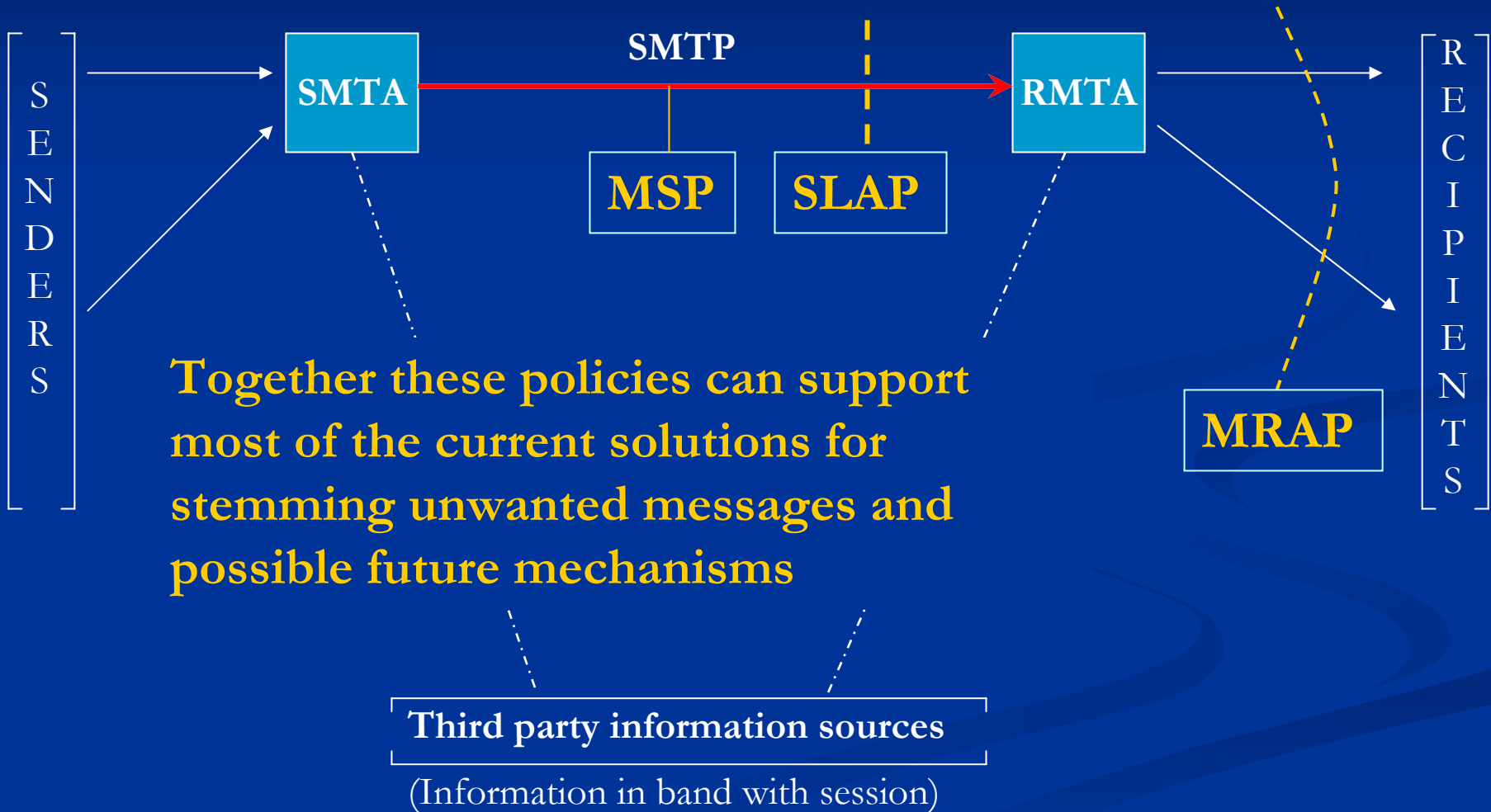
The Policy Architecture



The Policy Architecture

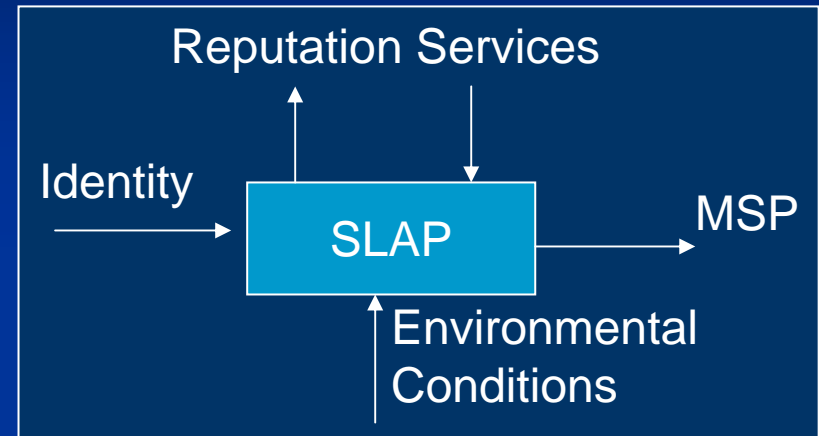


The Policy Architecture



Service Level Agreement Policy (SLAP)

- SLAP allows RMTA to accord a service level for an SMTA
- Supports evaluation of reputation/history
- Supports prioritization/rejection of messages
- Ability to add information to each received message (about its trustworthiness)



Input: **Sender's identity, Reputations etc.**

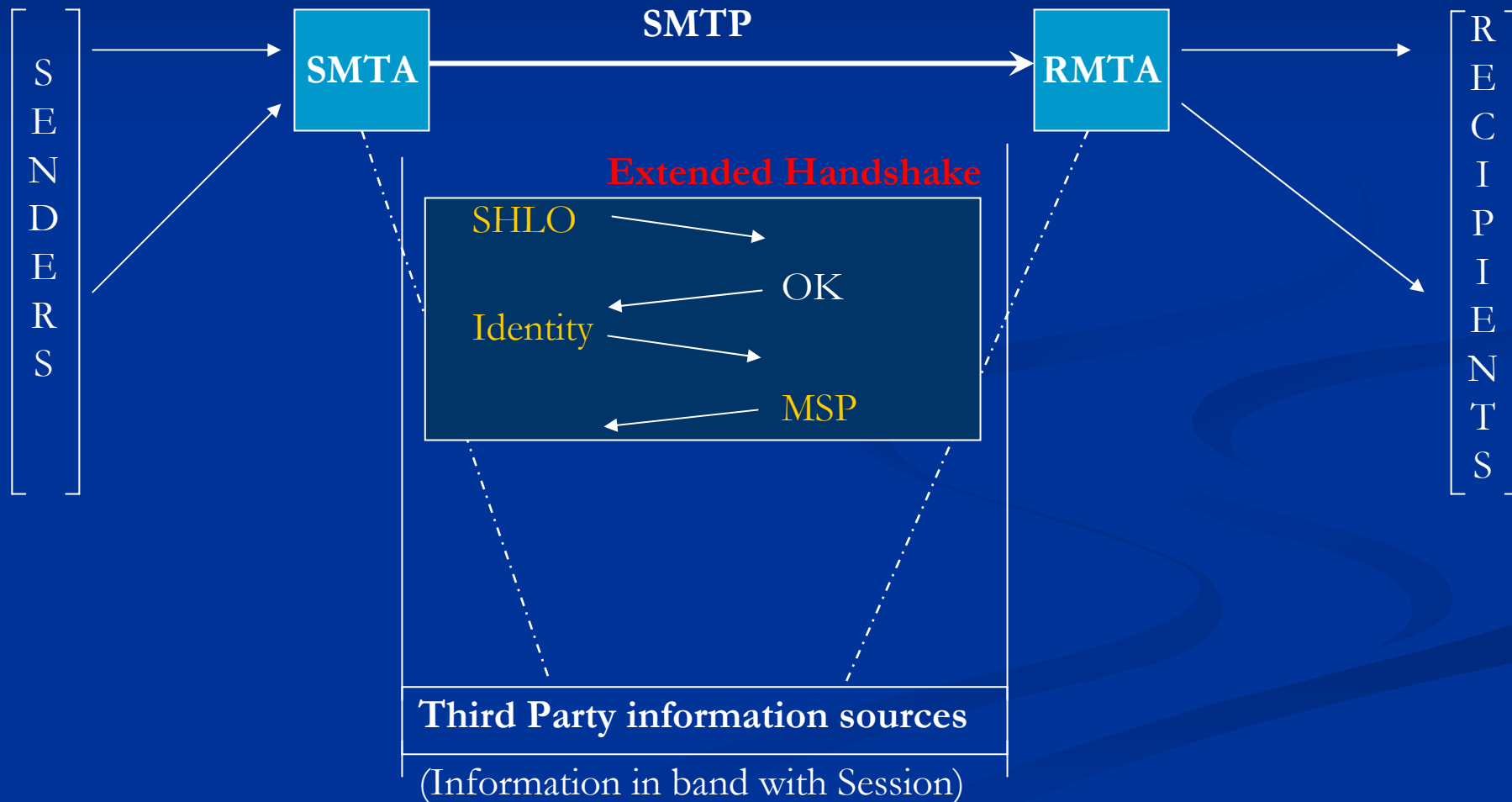
Output: **Message Scheduling Policy (MSP)**

Example SLAP Policy

- RMTA maps SMTA to a *profile* based on SMTA attributes such as its identity, reputation or prior behavior and its own conditions at the time of session request. Possible profiles are Partner, Trusted, Black-listed, Suspect etc.
 - During the handshake, it identifies the profile of SMTA
 - Defines an MSP to control messages transmitted

<i>e.g.: if (profile = Partner)</i>	<i>Accept all messages</i>
<i>if (profile = Black-listed)</i>	<i>Reject connection</i>
<i>if (profile = Trusted & light load)</i>	<i>Accept Bulk</i>
<i>if (profile = Suspect OR Unknown)</i>	<i>Limited # of msgs</i>

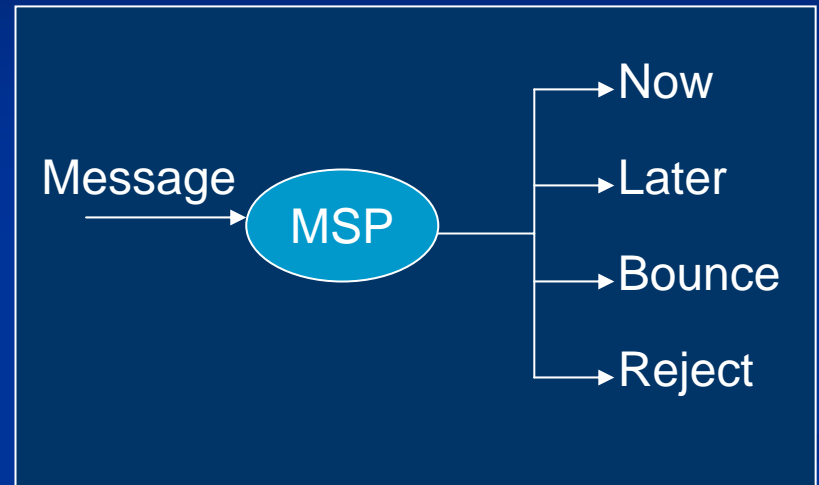
SLAP Extension to SMTP



Message Acceptance Criteria

- Message Scheduling Policy (MSP)

- RMTA's message acceptance rules for the **session**
- Applied only to **message headers**
- Can be applied at RMTA as well as SMTA
- Application can be verified at RMTA in either case



Input: **Message (headers)**

Output: **Scheduling Label**

Example MSP Policy

- SMTA **assertions** about message are used by MSP to decide if and when to accept messages

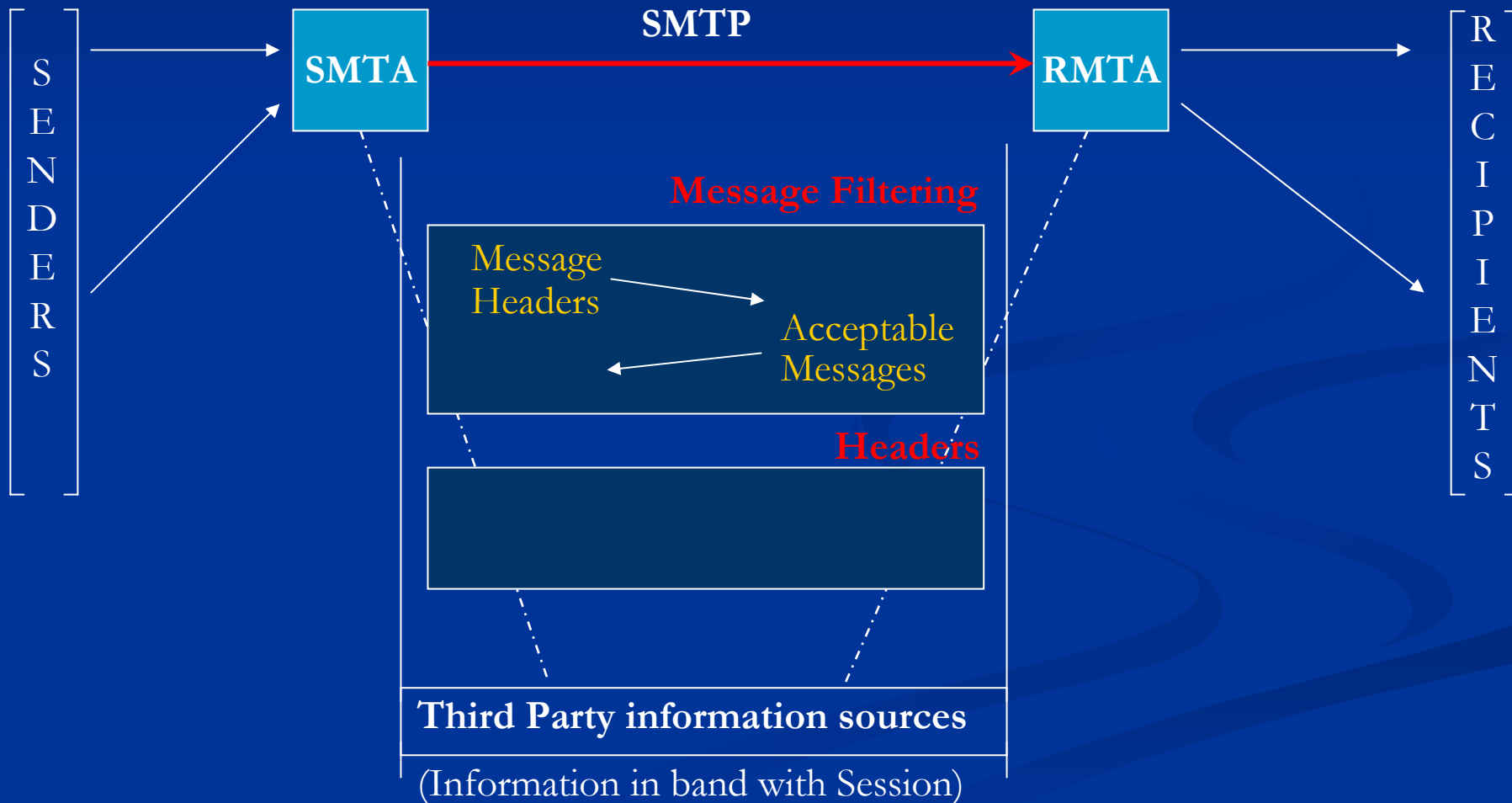
e.g.: Consider a message (m) with characteristics:

[password authentication of sender, personal message]

MSP for a session with trusted SMTA can rule:

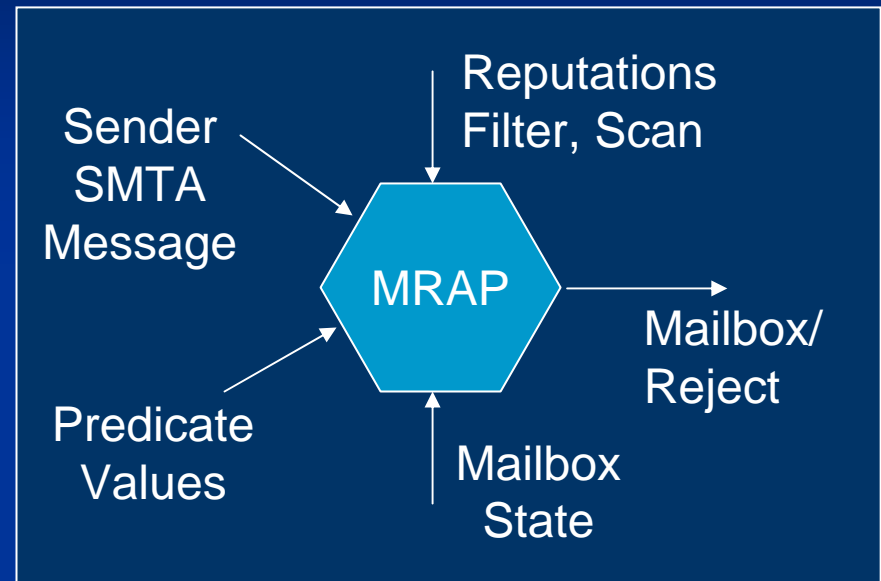
<i>(load=heavy & password auth)</i>	<i>Only official</i>	<i>Delay</i>
<i>(load=light & password auth)</i>	<i>Official and personal</i>	<i>Accept</i>

MSP Extension to SMTP



Mailbox Resource Allocation Policy (MRAP)

- Each Recipients' reception preferences
- Out of band application
- Session information available with each message



Input: **Message, Reputations, Scan** etc.

Output: **Destination Folder / Rejection**

Example MRAP Policy

- MRAP defines individual ‘tunable’ preferences for each recipient for accepting messages

e.g.: Alice subscribes to newsletters for cooking recipes

Bob does not subscribe to any newsletter

Alice: if (mailbox < 50%) accept cooking ads/news

Bob: No ads/newsletters

Filters/Attention bonds/Turing tests may drop messages for Alice which she considers valuable.

Conclusion: The Umbrella

- A framework to implement current solutions
 - Non prescriptive, policy based-flexible
 - Support for most of the technical and economic solutions
- Framework for identity/attribute based decision making with reputation based feedback and information sharing about email behavior.
- Support for greater control for recipients
- Customizable email delivery and reception preferences for each component in the email pipe

Questions?