MAIL DIVIDE FRAMEWORK

Takehito Akagiri

Kaoru Maeda

Tatsuya Hayashi

Internet-Draft

- draft-akagiri-mail-divide-00
  - Submit; Jul 5th
  - Authors;
    - Takehito Akagiri@ Rakuten, Inc.
    - Kaoru Maeda@Lepidum Co. Ltd.
    - Kouji Okada@Lepidum Co. Ltd.
    - Tatsuya Hayashi@Lepidum Co. Ltd.
    - Masaki Kase@NIFTY Corporation

What is MAIL DIVIDE FRAMEWORK

The meaning of "divide"

Legitimate message

Unread message

Email separates like water at "divide"

Source of the photo:
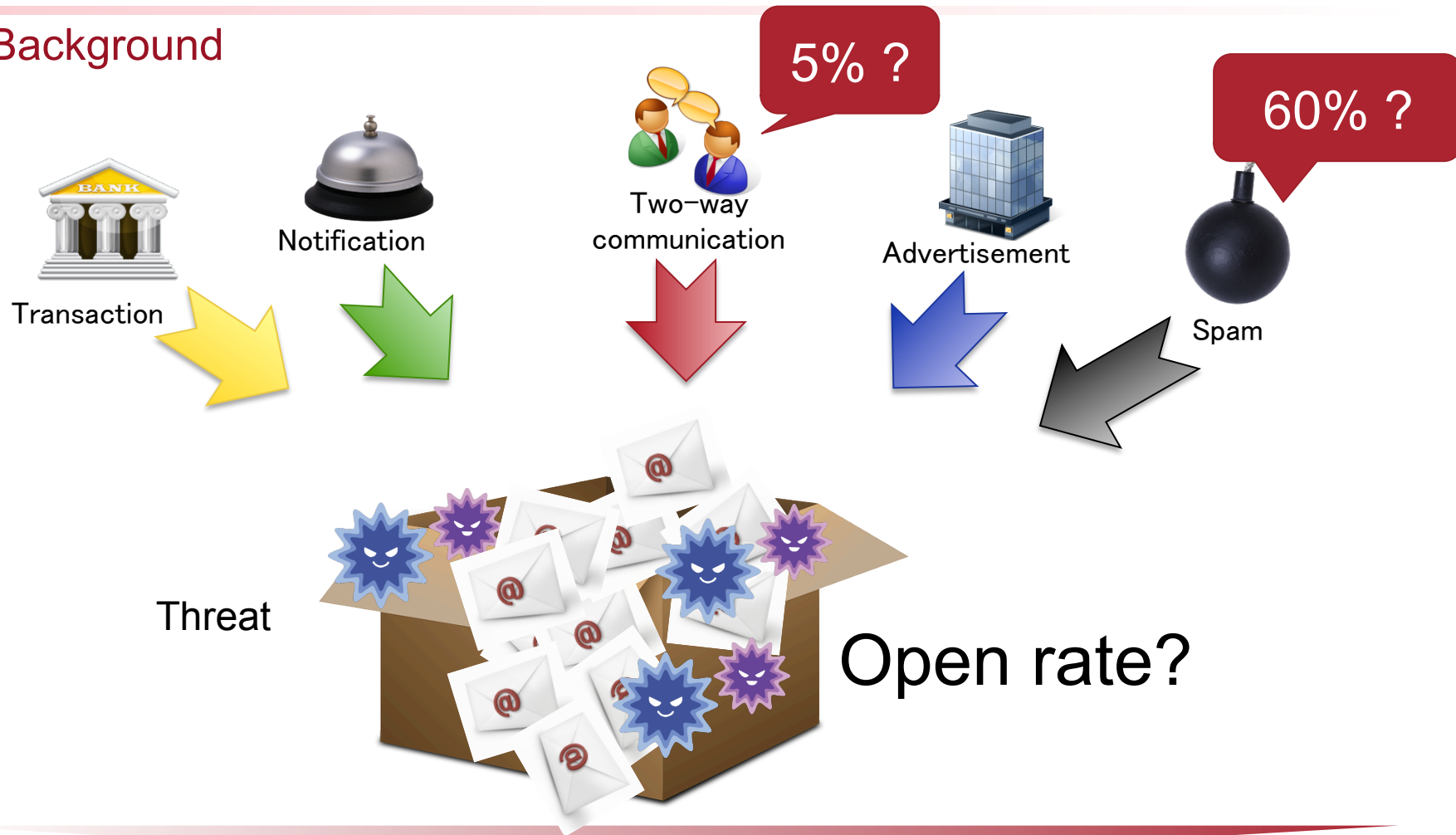https://ja.wikipedia.org/wiki/%E4%B9%97%E9%9E%8D%E5%B2%B3

What is MAIL DIVIDE FRAMEWORK

The purpose of MAIL DIVIDE FRAMEWORK

- Purpose
  - Making a TRUSTED NETWORK in the current email network
  - Receiver policy declaration
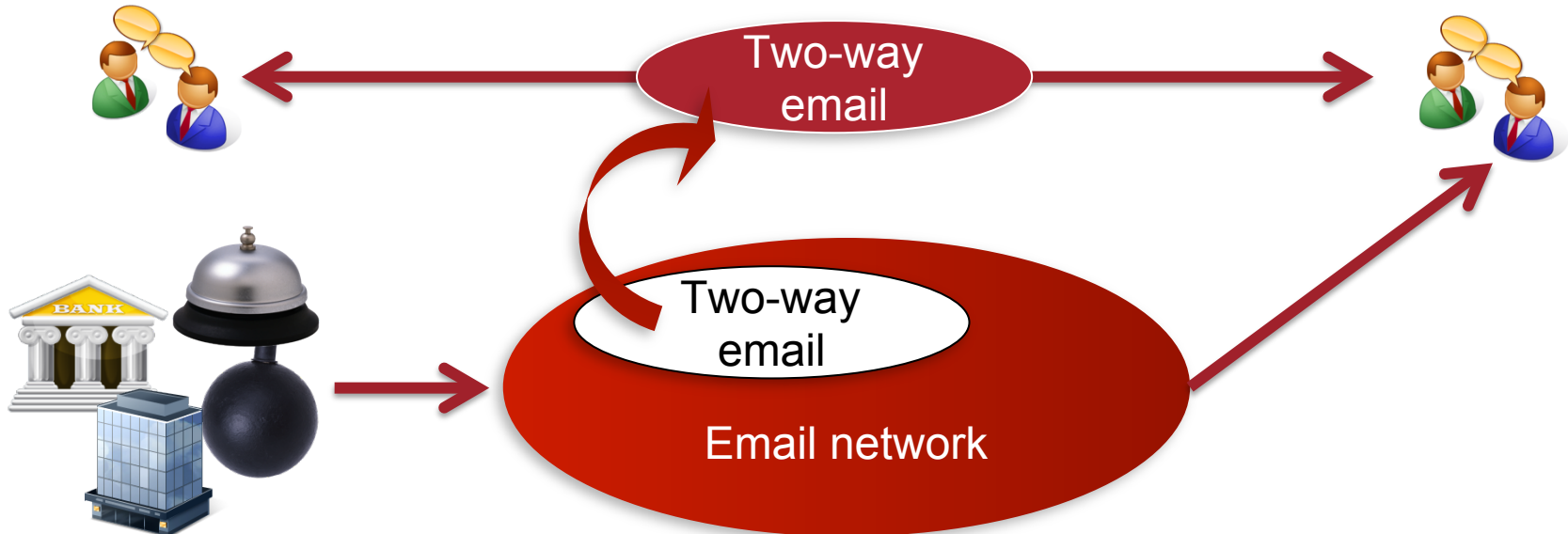
- Shortened form
  - DIVIDE

Why DIVIDE

Jumble mailbox make it hard to control abuse

Why DIVIDE

Email dies unless two-way communication is given priority

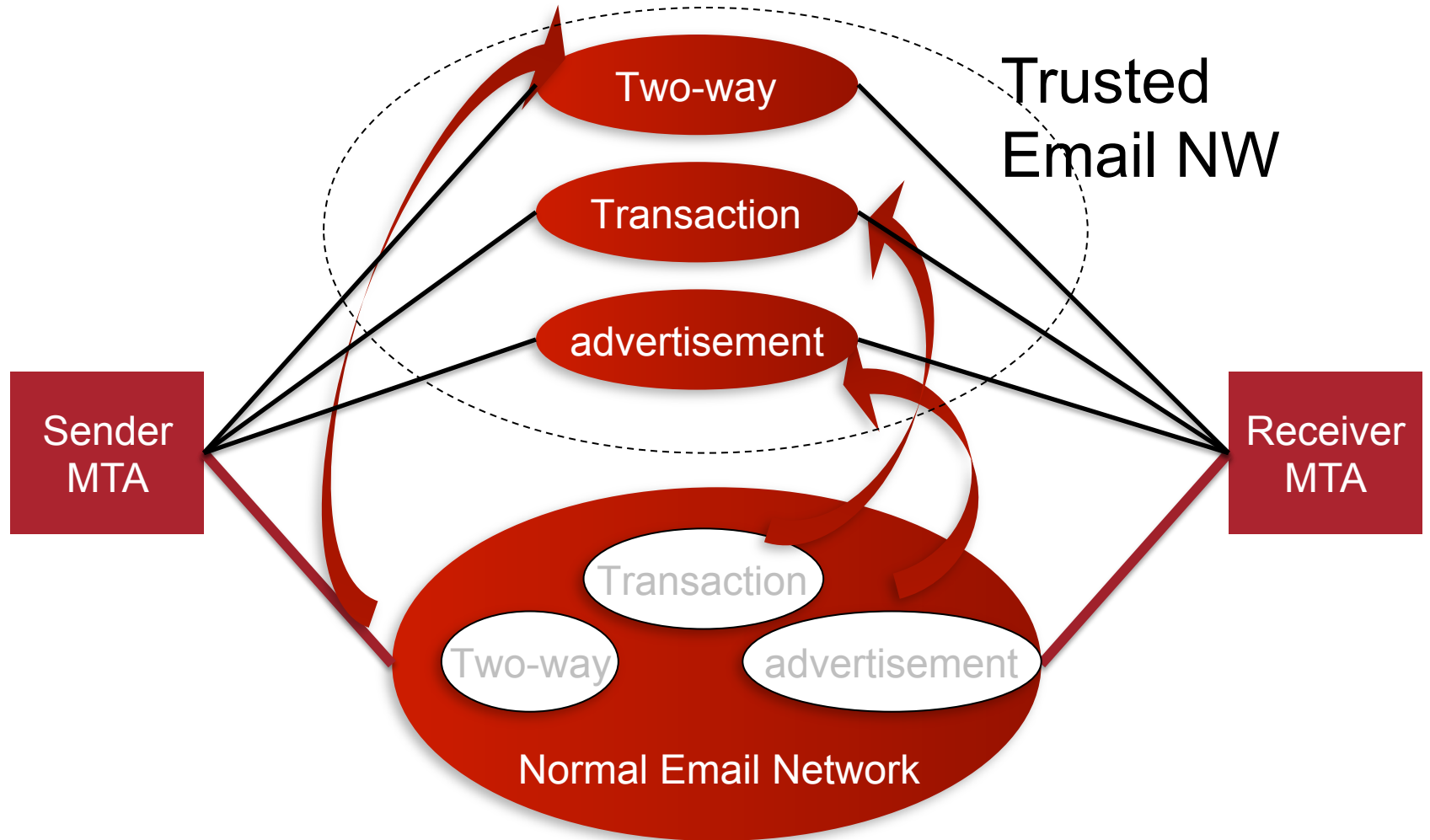Two-way communication : One way email

➡ 5 : 95

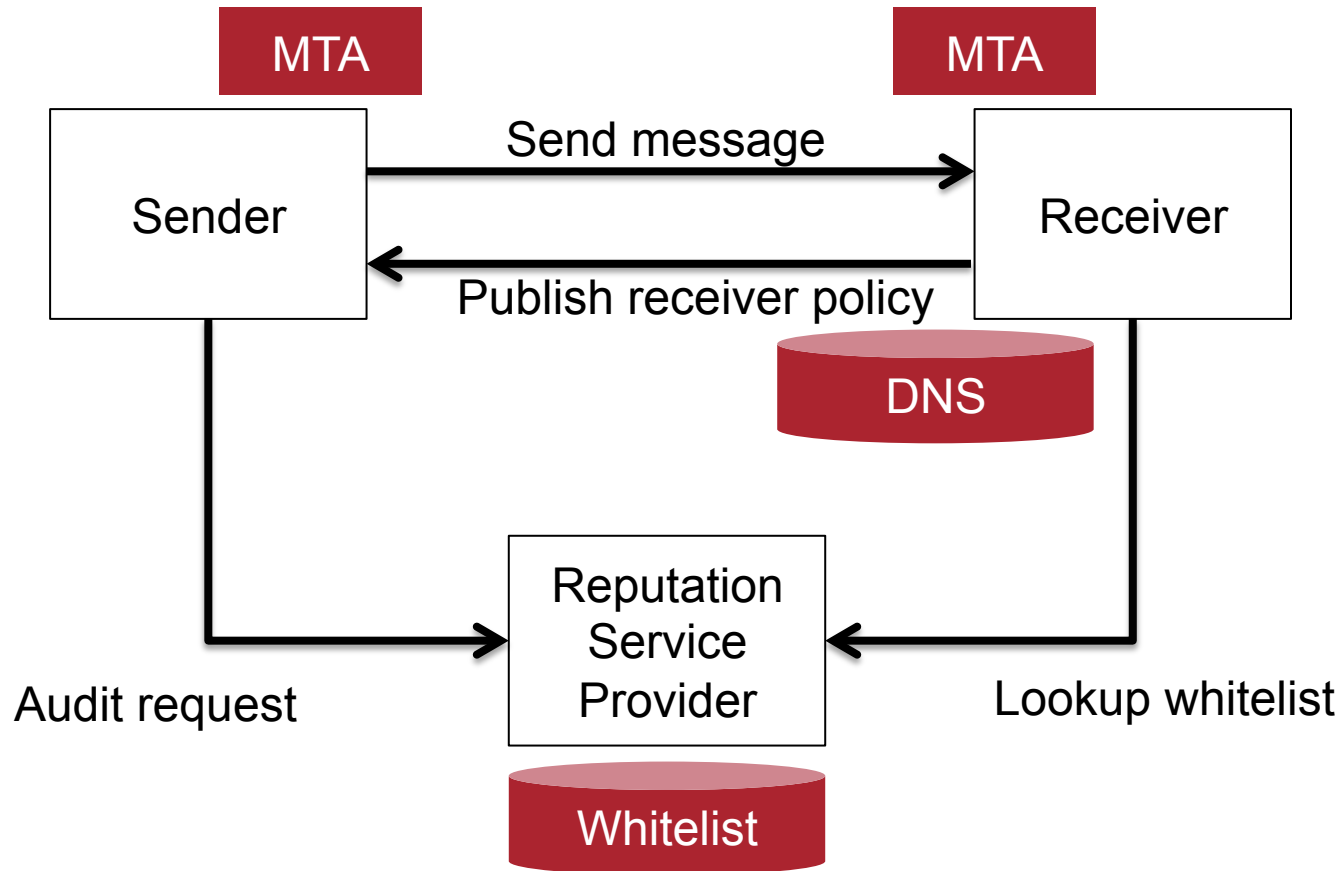Two-way email

Two-way email

Email network

Why DIVIDE

Trusted Email NW

Two-way

Transaction

advertisement

Sender MTA

Receiver MTA

Normal Email Network

Transaction

Two-way

advertisement

Divide email network by categories

How DIVIDE

How DIVIDE

Normal mail routing

RCPT TO:
bob@beta.example.com

MSA/MTA

Trusted Sender
RCPT: **bob@beta.example.com**

Sender
RCPT TO: **bob@beta.example.com**

MX
(beta.example.com)

Bob
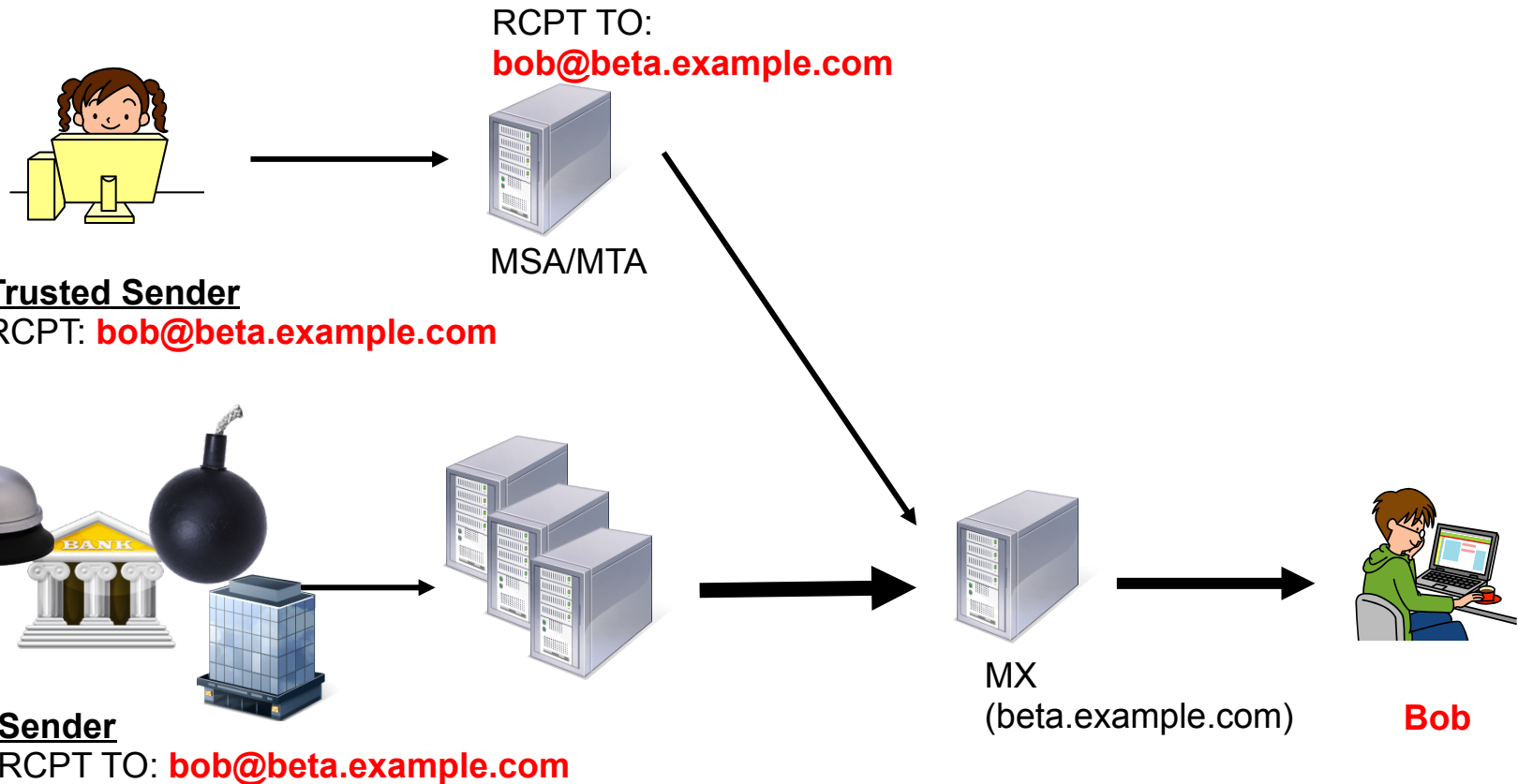
How DIVIDE

Divide mail routing
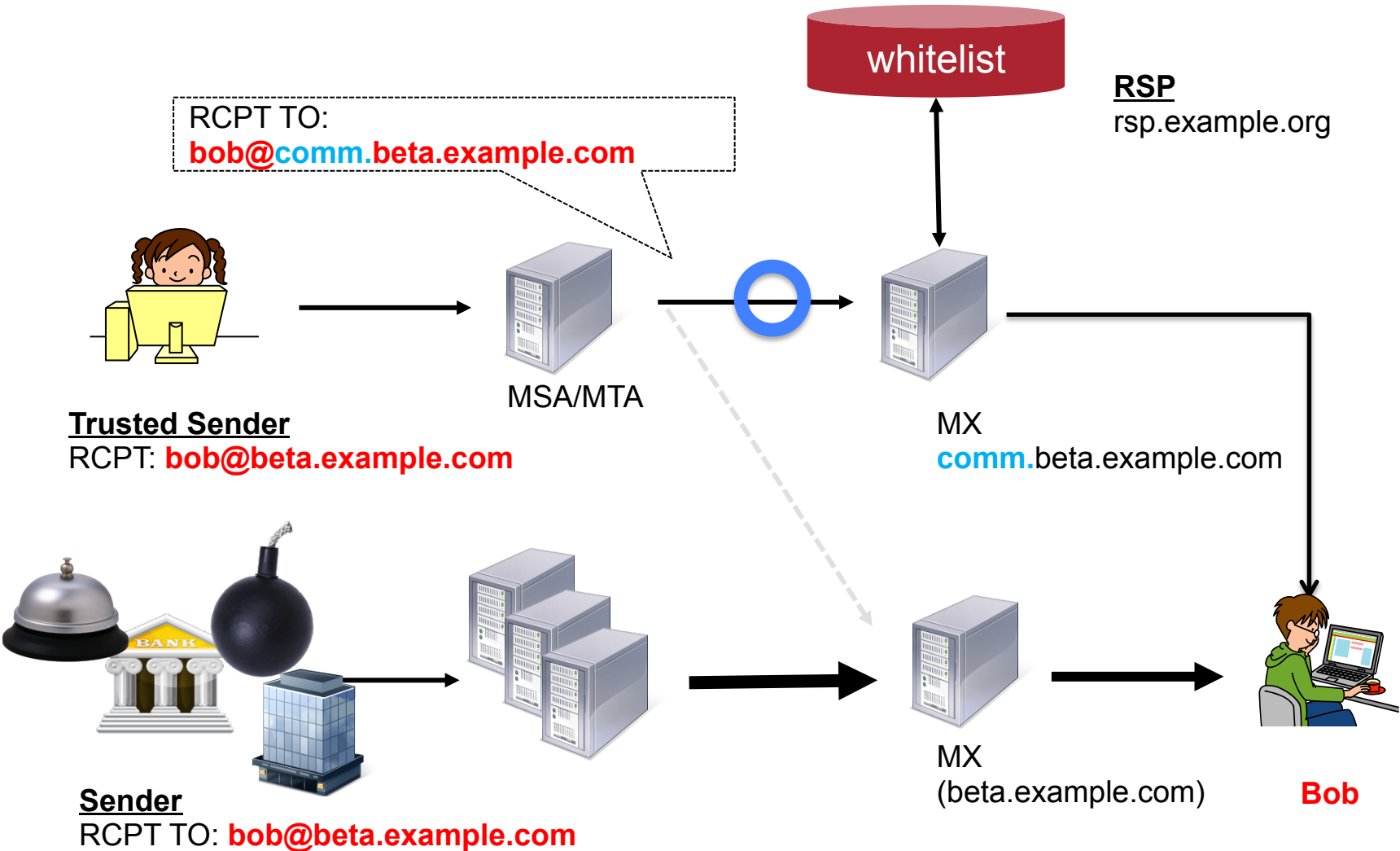
How DIVIDE

Whitelist basis trusted network

Whitelist

RSP
rsp.example.org

MSA/MTA

MX
comm.beta.example.com

Trusted Sender
RCPT: **bob@beta.example.com**

MX
(beta.example.com)

Sender
RCPT TO: **bob@beta.example.com**

Bob
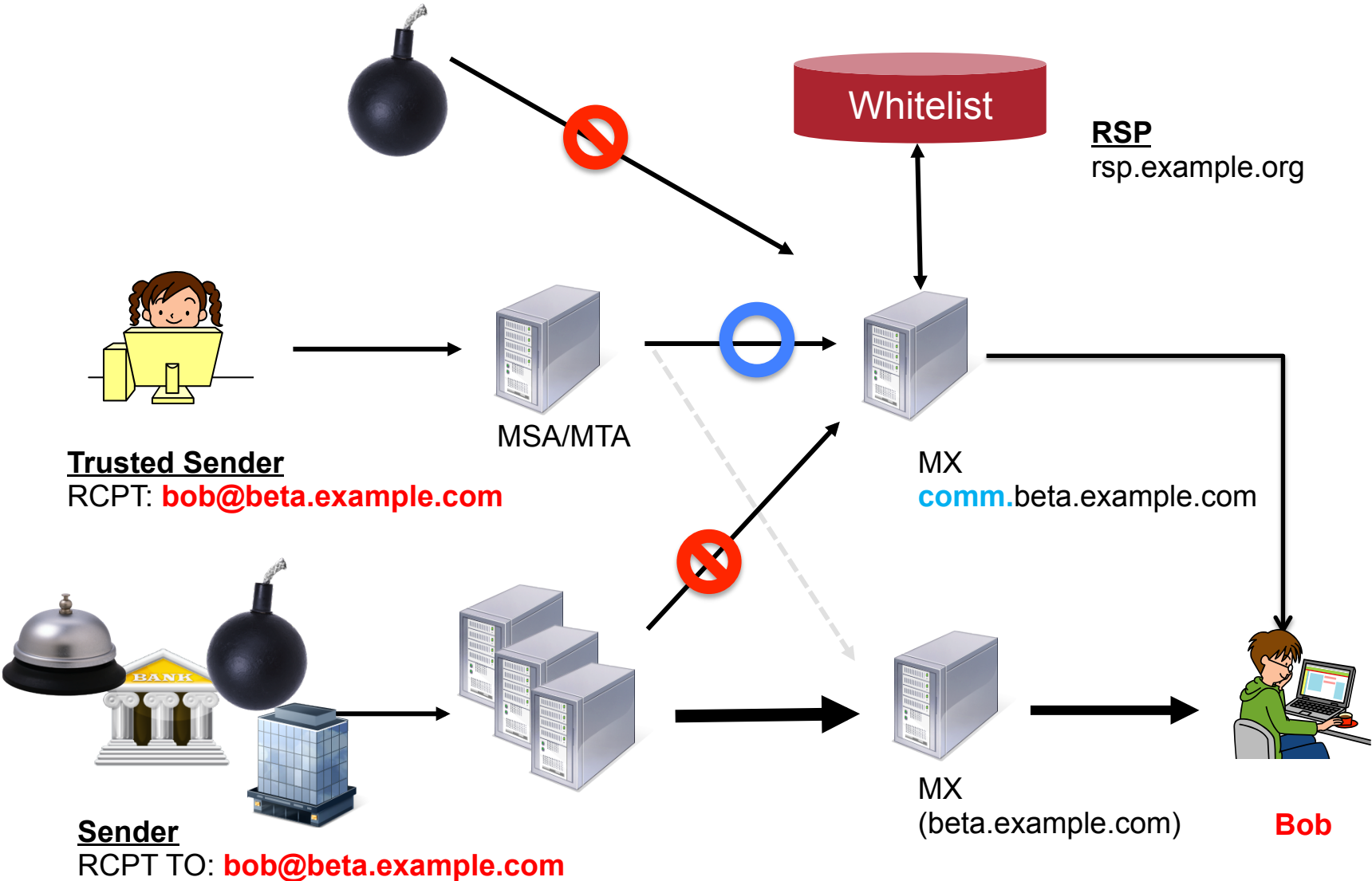
Why now

- Components have been standardized well
  - Sender Authentication Mechanism
    - DMARC, SPF, DKIM …
  - Reputation
    - repute, marf …
- Closed communication NW can work well
  - OTT Messaging, SNS messenger

Missing part is "Receiver Policy"

Why now

_divide.beta.example.com IN TXT

v=DIVIDE1\; a=DMARC p=comm:c rsp=rsp.example.org;

a=DMARC p=notif:n rsp=reputation.example.com

| Tag name	Description	Value
v	Version info	1
a	Sender Authentication Mechanism verifying by receiver's MTA	SPF, DKIM, DMARC …etc
p	Specify the set of category and subdomain which should be added by sender	Refer to next slide
rsp	Reputation service provider specified by receiver	FQDN * Discovery method follows by RFC707X

What's next

- Update I-D to ver.01
  - Find authors from outside of Japan
  - Discuss through ML
- Implementation
  - Prototype has already prepared
- Trial or beta service Project
  - Among some ISPs for two-way
  - Experimental adoption

Appendix.

How DIVIDE
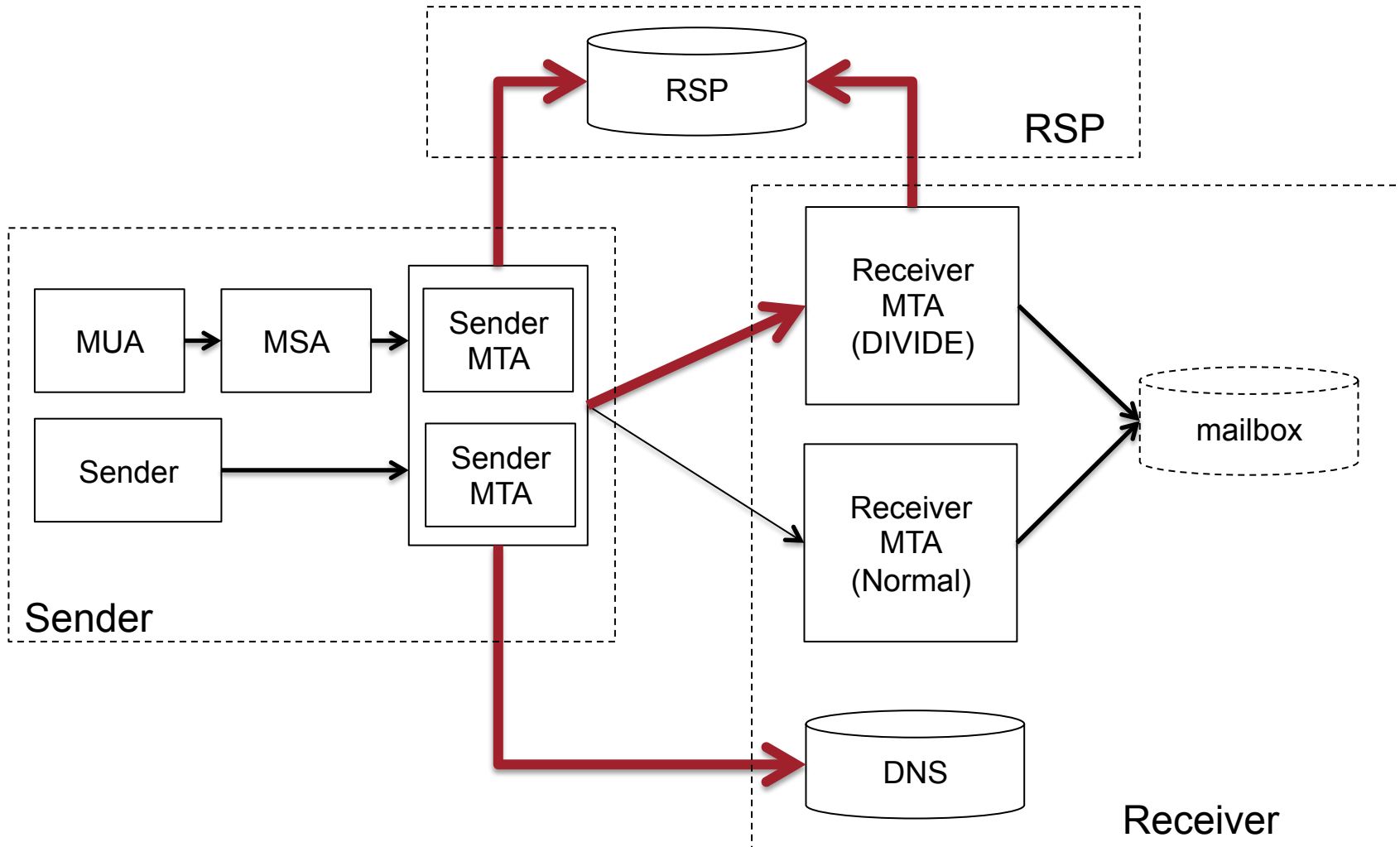
How DIVIDE

- Sender Authentication
  - Which kind of sender authentication mechanism receiver can verify
- Category
  - Category and subdomain which should be added
- RSP (Reputation Service Provider)
  - Which RSP receiver using

How DIVIDE

- P=[Category]:[subdomain]
  - XXX ➔ Defined category
  - YYY ➔ Subdomain which added by trust sender
- Category
  - comm ➔ Two-way communication
  - trans ➔ Transaction
  - notif ➔ Notification
  - promo ➔ Promotion
  - mL ➔ Mailing-list
  - mh ➔ Forward email
  - default ➔ default
- Subdomain
  - Specified by receiver

How DIVIDE

- ## Register
  - Request audit to RSP
    - In case of acceptance, sender's info add into trust list

- ## Subdomaining
  - DNSlookup _divide record
  - Add subdomain to the "Envelope To" address based on category
    - Never change "Header To" address

How DIVIDE

- Provide whitelist for receiver
  - Receiver itself can act as RSP
  - Whitelist basis reputation
- Audit sender
  - Should be add to trust list