FTC Spam Forum

Technological Solutions to Spam / Structural Changes to Email

Trusted Email Open Standard

A Comprehensive Policy and Technology Proposal for Email Reform

Written by:

Vincent Schiavone

David Brussin

James Koenig

Stephen Cobb

Ray Everett-Church

Presented by:

Vincent Schiavone
President & CEO
ePrivacy Group

phone: 610.407.7083
email: vs@eprivacygroup.com

Why? Email is Too Important Not To Fix

Mission critical for:

businesses, consumers, governments, and non-profits

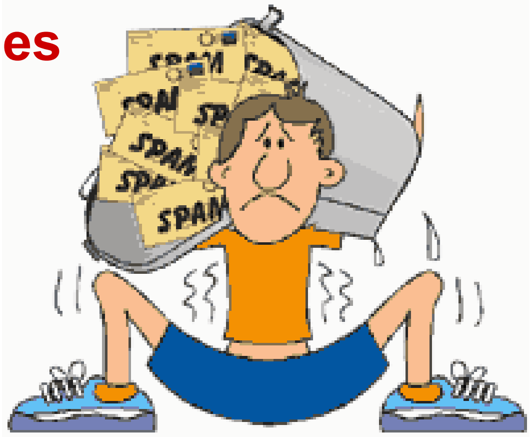
- Customer service (shipping, statements, receipts…)
- Business 2 Business Communications
- Personal communications (friends and family)
- Subscriptions/news (paid, time-sensitive)
- Want ads and offers (CRM)
- Official government communications
- Non-profits, advocates, charities

But 50% of all email is spam

- UCE (ADV)
- Bulk Email

Much of it very bad stuff

- **Porn (ADLT)**
- **Identity Theft**
- **Brand Theft**
- **Fraud**
- **Crimes**



Spam is getting worse… fast

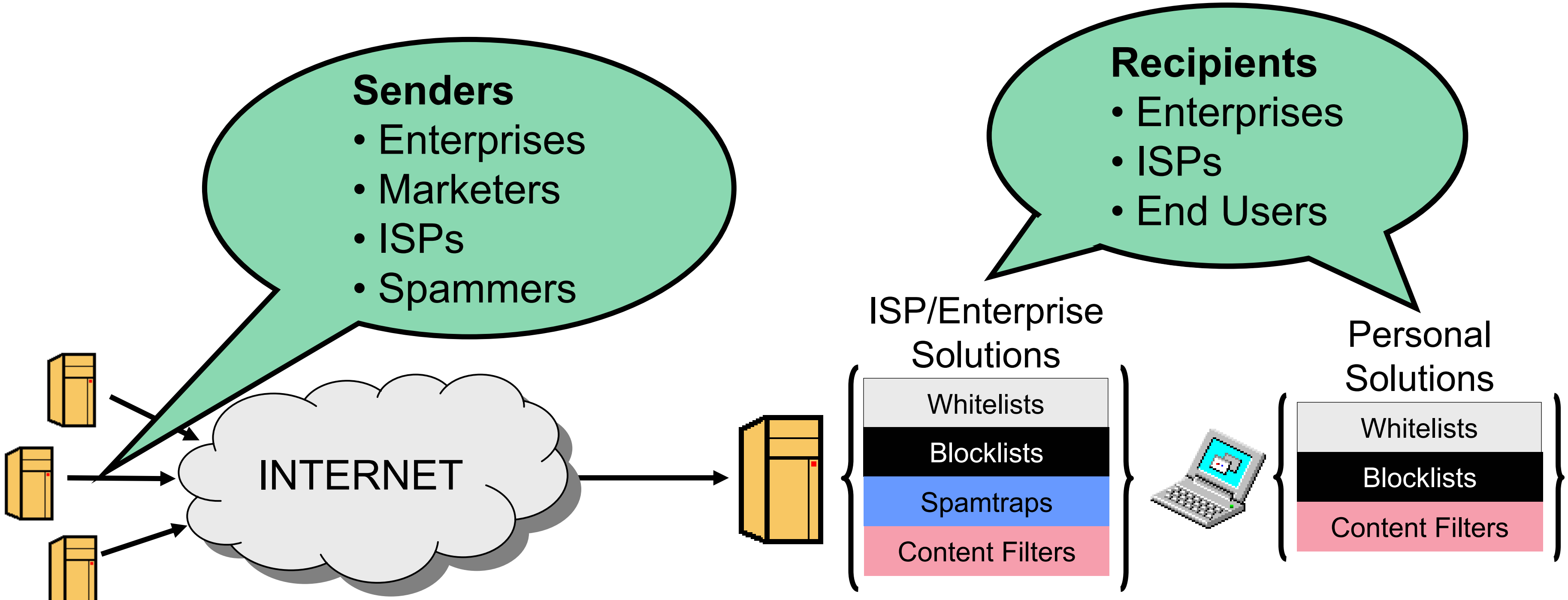
How *Not To* “Fix” Email – What Does Not Work

- Technology-only solutions
  - Evidence shows they’re not working
  - Technology can enforce trust, but cannot create it
  - Email technology today remains largely spoofable, insecure
- Policy-only solutions
  - Policy without technology to implement and enforce is weak
  - Industry self-regulation has not yet addressed the problem
- Solutions without major ISP and mail client support
  - Namely AOL, Earthlink, Microsoft, Yahoo
- Solutions not aligned with existing laws
  - Solution lacking truthful identity and subject labeling
  - Incomplete solutions that do not go from sender to recipient
  - Not supportive of Federal, State and International

How *To* "Fix" Email – What Will Work

- Technology that can enforce policy
  - While remaining platform independent and open
  - Creates end-to-end Accountability, from Sender to Recipients
- Policy that is aligned with technology
  - Without excluding any of the interested parties
    - legitimate senders, ISPs and Recipients
- ISPs adopting standards, creating incentives
  - A critical mass of participation will set *de facto* standards
  - A few large ISPs will drive rapid adoption (absence is not adoption)
  - Consideration of positive features by ISP and filters will help
- Laws
  - Create "Safe Harbors" to encourage adoption of standards
  - Recognize role of Technology & Policy to aid in enforcement

How Email Works Today



Senders
- Enterprises
- Marketers
- ISPs
- Spammers

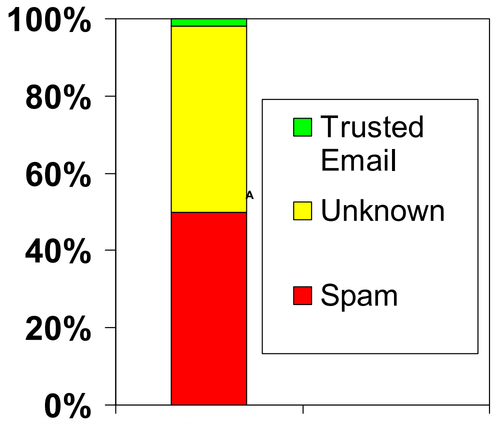
INTERNET

Recipients
- Enterprises
- ISPs
- End Users

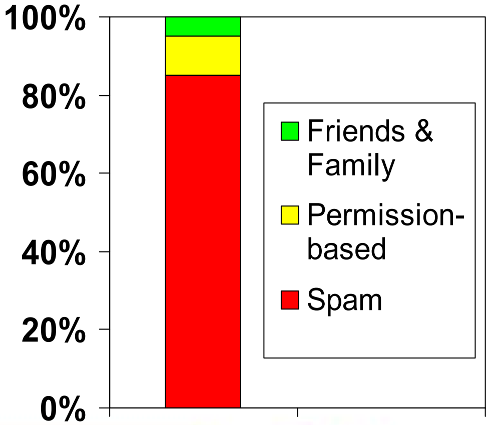
ISP/Enterprise Solutions
- Whitelists
- Blocklists
- Spamtraps
- Content Filters

Personal Solutions
- Whitelists
- Blocklists
- Content Filters

ISP/Enterprise View



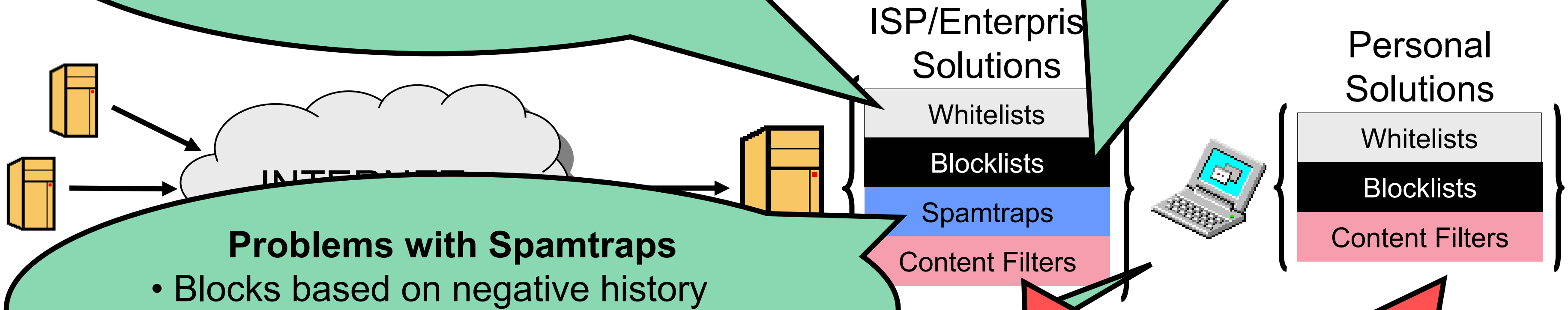
Consumer View



How Spam Fighting Works Today – Poorly !

Problems with Whitelists
- Requires 1-on-1 Negotiation
- Not secure - Source IP is spoofable
- Bad feedback causes de-listing
- No consistent standards

Problems with Blocklists
- Reliability Issues
- Source IP is spoofable
- Lack of granularity
- No consistent standards



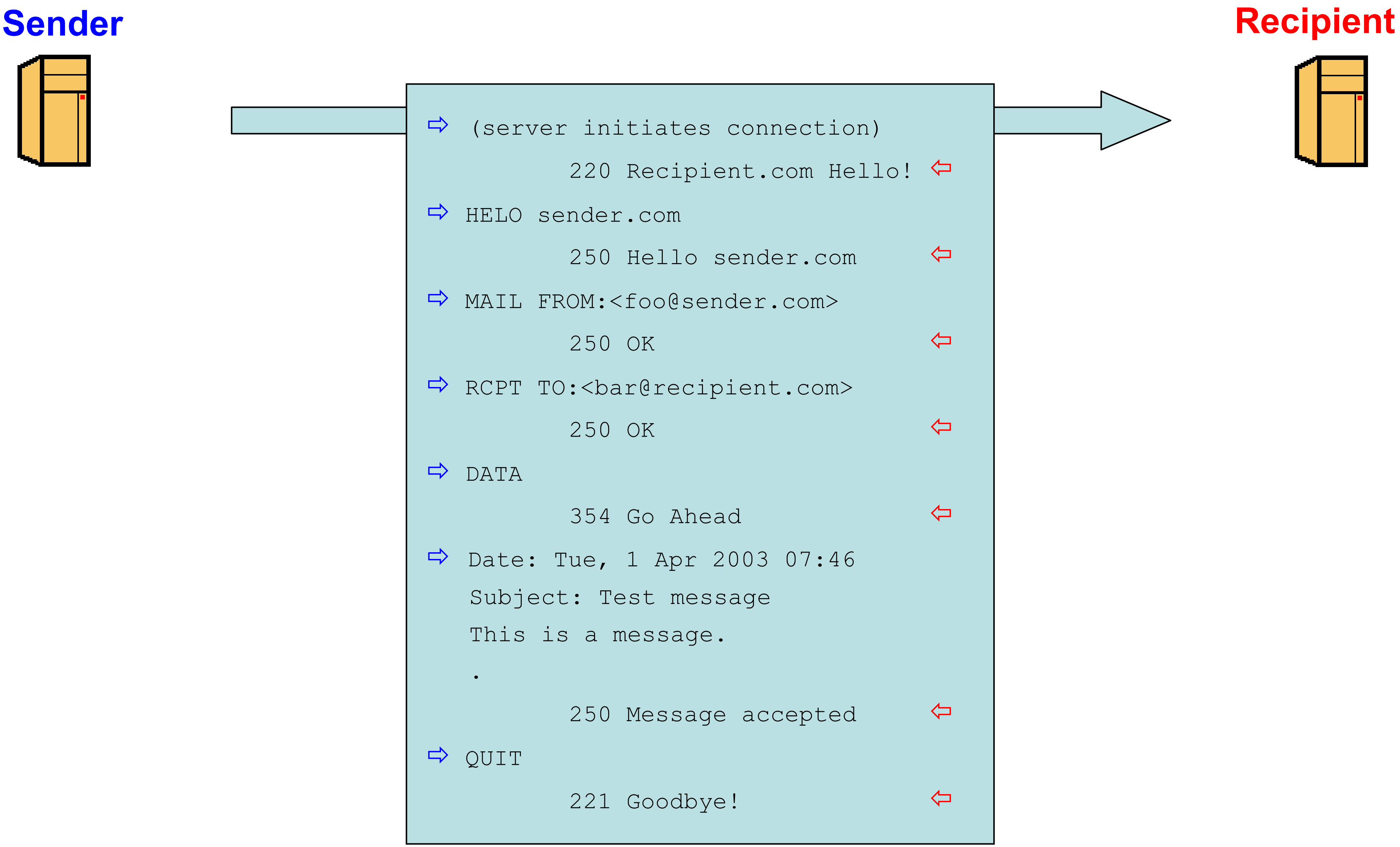
Problems with Spamtraps
- Blocks based on negative history
- Passes-through if no known history
- Complex to maintain large network

Problems with DNS-Based Approach
- DNS is insecure, spoofable
- DNS stops at the ISP; no useful information to end user

Top 3 Problems with Filtering

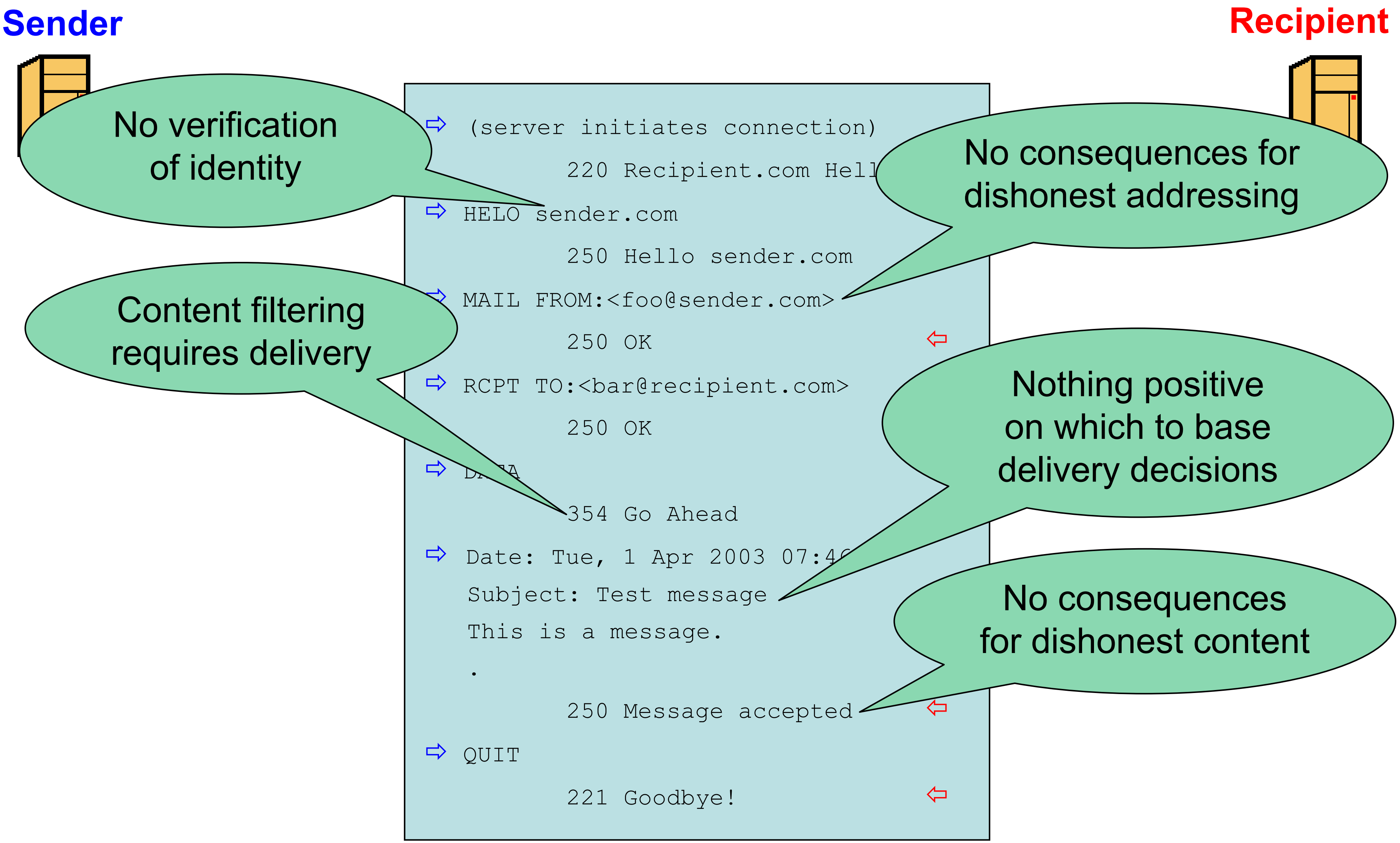
1. Doesn’t STOP enough spam
2. Doesn’t STOP enough spam
3. False positives

Simple Mail Transport Protocol (SMTP)



```
⇨ (server initiates connection)
                220 Recipient.com Hello!   ⇦
⇨ HELO sender.com
                250 Hello sender.com       ⇦
⇨ MAIL FROM:<foo@sender.com>
                250 OK                     ⇦
⇨ RCPT TO:<bar@recipient.com>
                250 OK                     ⇦
⇨ DATA
                354 Go Ahead               ⇦
⇨ Date: Tue, 1 Apr 2003 07:46
  Subject: Test message
  This is a message.
  .
                250 Message accepted       ⇦
⇨ QUIT
                221 Goodbye!               ⇦
```

Problems Inherent in SMTP



```
⇨  (server initiates connection)
         220 Recipient.com Hell
⇨  HELO sender.com
         250 Hello sender.com
⇨  MAIL FROM:<foo@sender.com>
         250 OK                         ⇦
⇨  RCPT TO:<bar@recipient.com>
         250 OK
⇨  D  A
         354 Go Ahead
⇨  Date: Tue, 1 Apr 2003 07:4
   Subject: Test message
   This is a message.
   .
         250 Message accepted           ⇦
⇨  QUIT
         221 Goodbye!                   ⇦
```

No verification of identity

No consequences for dishonest addressing

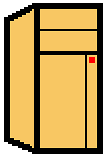
Content filtering requires delivery

Nothing positive on which to base delivery decisions

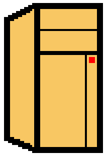
No consequences for dishonest content

No Useful Standards for Stating / Verifying Identity

Sender



Recipient



What if a sender ***could*** state its identity in email in a verifiable way?

For example:

1. Reliable DNS

2. Secure ID in Headers

No Standards for Content Assertions

Sender

Recipient

Assertions

What if a sender ***could*** say more about the content of the email?

For example:

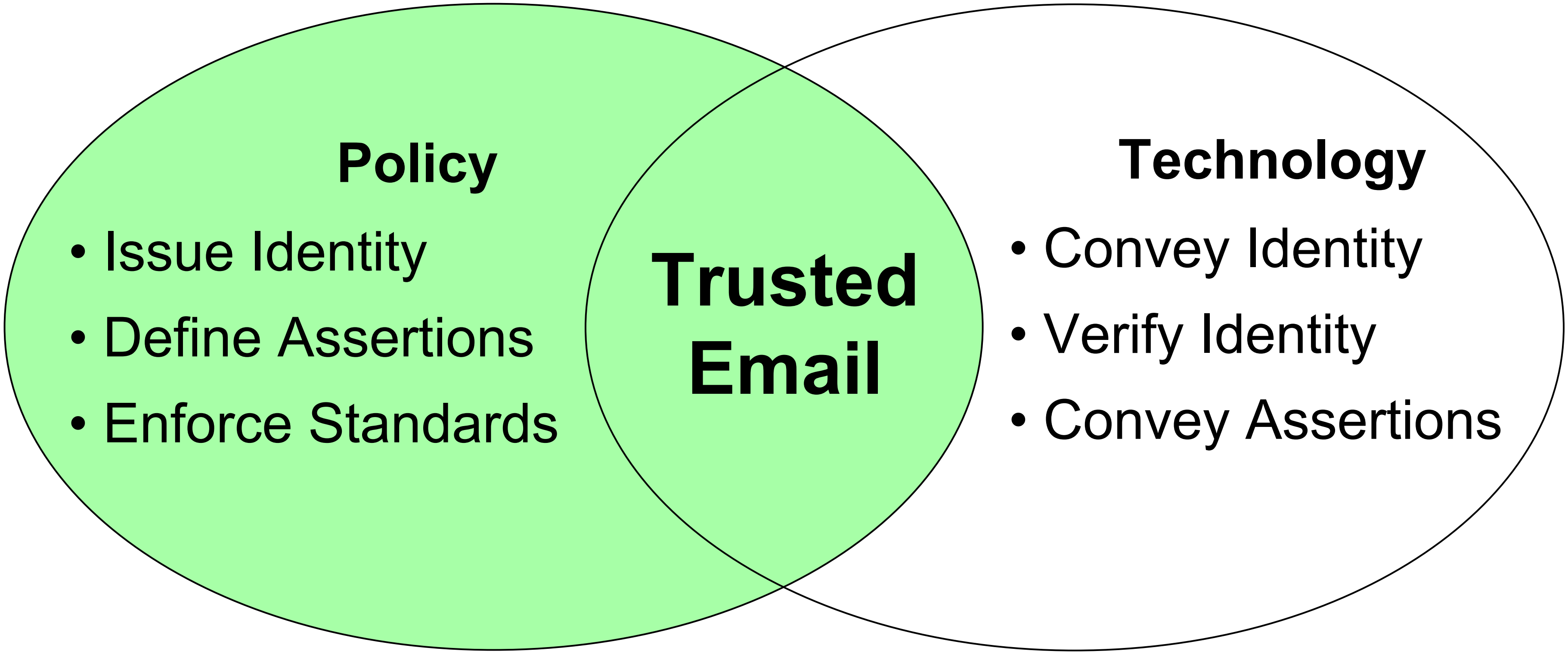
1. **Unsolicited advertisements** (ADV)
2. **Adult** (ADT)
3. **Permission-based ads, offers** (CRM)
4. **Customer Service (shipping, receipts)** (CSC)
5. **Subscriptions** (SUB)
6. **Official government email** (GOV)
7. **Business to business or employee** (BIZ)
8. **Personal, friends and family** (FAF)
9. **Non-profit, charitable** (NPE)

Trust and Accountability

through

Trusted Email Open Standard

Trusted Email – Integration of Policy & Technology



Policy

- Issue Identity
- Define Assertions
- Enforce Standards

Trusted Email

Technology

- Convey Identity
- Verify Identity
- Convey Assertions

No Integration = No Solution

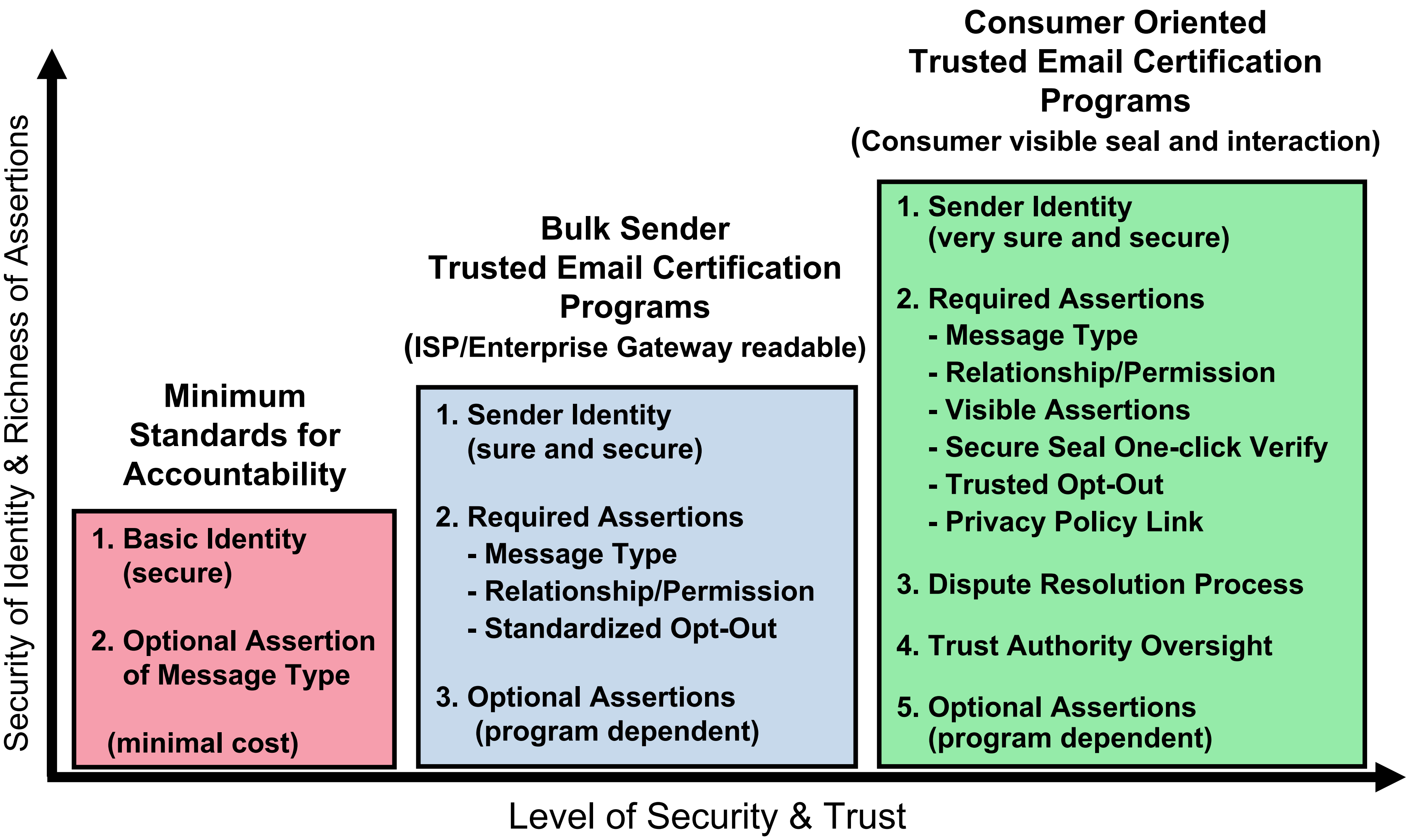
Trusted Email Open Standard

<u>Goal</u>: Communicating Trusted Identity and Trusted Assertions, throughout the email delivery chain with the same level of trust, and enforceability, without risk of spoofing, forgery or fraud

1. A framework to provide **Trusted Identity** for email senders
   - Secure, fast, lightweight signatures in headers
   - Optimized with DNS-based systems for flexibility and ease of implementation
2. A framework for making **Trusted Assertions** about
   - Sender
   - Content of each individual message
   - Relationship / Permission with respect to individual recipient
3. A framework for creating a **Federation of Trusted Email Programs**
   - Independent trust authorities
   - Industry self-regulation groups
   - Self-certifying organizations
4. A framework of **Open Standards** and Platform Independent Technology

Not Intended to Eliminate Anonymous and Individual Email

Trusted Email – Send and Receive Choices



Security of Identity & Richness of Assertions

Level of Security & Trust

Minimum Standards for Accountability

1. Basic Identity (secure)
2. Optional Assertion of Message Type

(minimal cost)

Bulk Sender Trusted Email Certification Programs

(ISP/Enterprise Gateway readable)

1. Sender Identity (sure and secure)
2. Required Assertions
   - Message Type
   - Relationship/Permission
   - Standardized Opt-Out
3. Optional Assertions (program dependent)

Consumer Oriented Trusted Email Certification Programs

(Consumer visible seal and interaction)

1. Sender Identity (very sure and secure)
2. Required Assertions
   - Message Type
   - Relationship/Permission
   - Visible Assertions
   - Secure Seal One-click Verify
   - Trusted Opt-Out
   - Privacy Policy Link
3. Dispute Resolution Process
4. Trust Authority Oversight
5. Optional Assertions (program dependent)

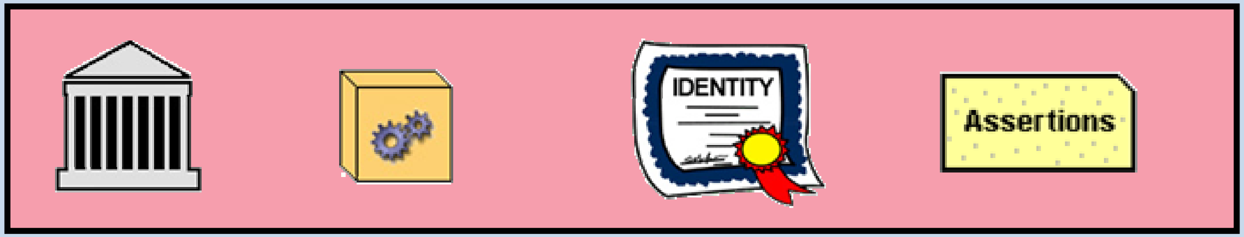
Minimum Standards – Technical Elements

- Basic Identity (secure Near $0 cost)
  - Certificate Authorities and Domain Registries
- Trusted Email Send/Receive Engine
  - Open Standards, Open Source, Royalty Free
  - Performs DNS Checks and Secure ID Verifications
- Standard Language for Stating Identity
- Standard Language for Stating Assertions (optional)
  - Optional Assertions About Individual Email Messages

1. **Unsolicited advertisements** (ADV)
2. **Adult** (ADT)
3. **Permission-based ads, offers** (CRM)
4. **Customer Service (shipping, receipts)** (CSC)
5. **Subscriptions** (SUB)
6. **Official government email** (GOV)
7. **Business to business or employee** (BIZ)
8. **Personal, friends and family** (FAF)
9. **Non-profit, charitable** (NPE)

Bulk Sender Trusted Email – Program Elements

In addition to Level 1:



- Sender Identity (sure and secure)
  - Certificate Authorities – Level 2 ID Cert

Rich Assertions

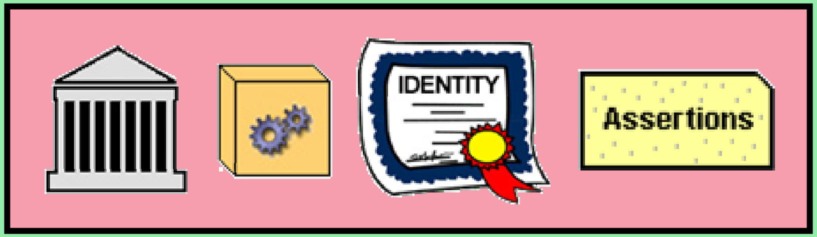
- Standard Language for Stating Assertions
  - Required assertions About Individual Email Messages
    - Message Type, Relationship/Permission

HTML/XML MUA read

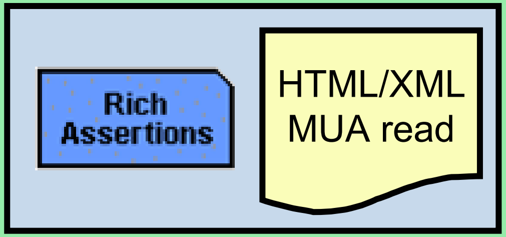
- Standardized Opt-out (verifiable link)

Consumer Trusted Email – Program Elements

In addition to Level 1:



and Level 2:

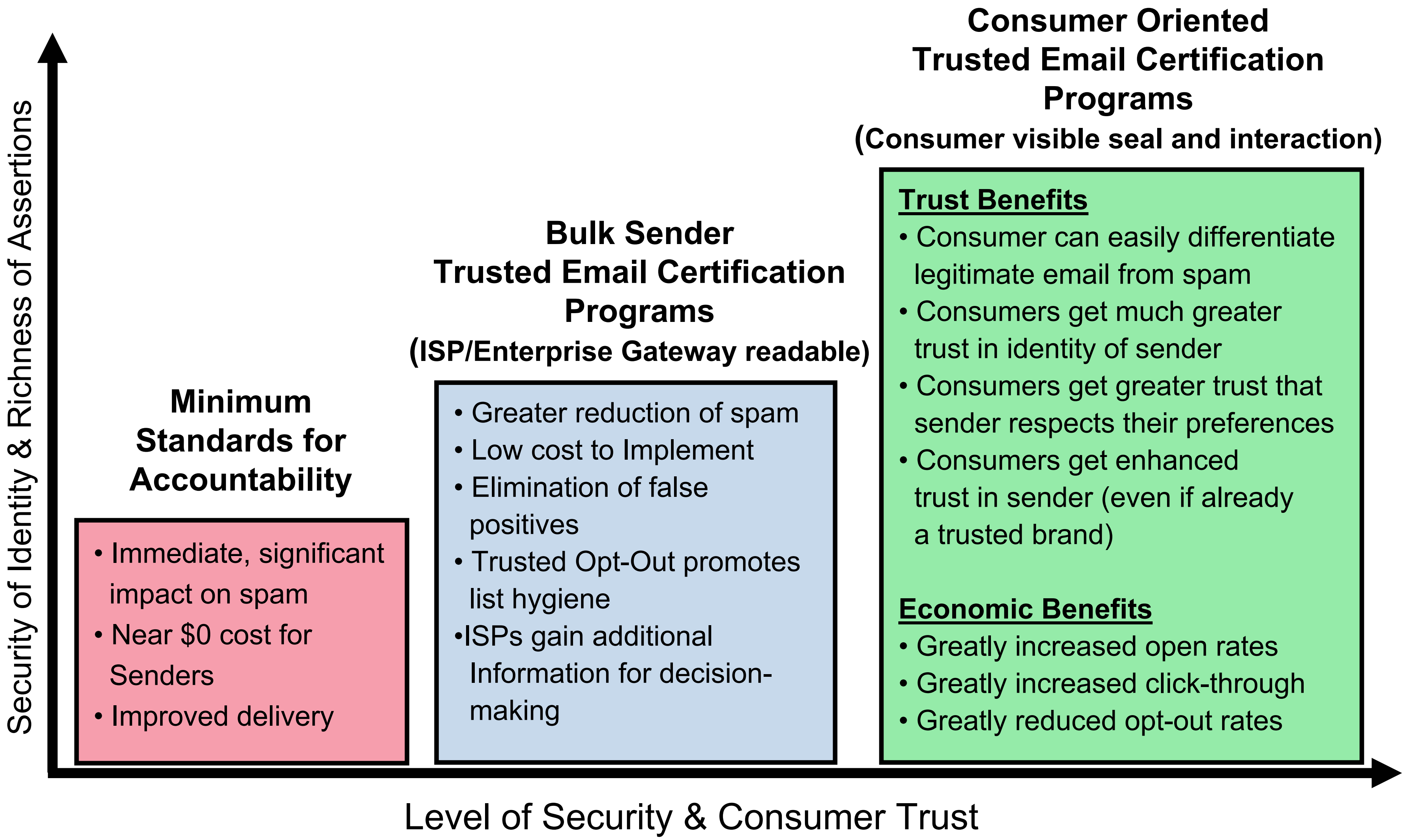


- Sender Identity (very sure and very secure)
  - Certificate Authorities – Level 3 ID Cert

- Visible Assertions
  - Secure “Seal” (one-click verification)
  - Trusted Opt Out (verifiable standard link)
  - Privacy Policy (verifiable link)

- Trust Authority Oversight
- Dispute Resolution Mechanism

Trusted Email – Benefits Senders and Recipients



Security of Identity & Richness of Assertions
Level of Security & Consumer Trust

Minimum Standards for Accountability

- Immediate, significant impact on spam
- Near $0 cost for Senders
- Improved delivery

Bulk Sender Trusted Email Certification Programs

(ISP/Enterprise Gateway readable)

- Greater reduction of spam
- Low cost to Implement
- Elimination of false positives
- Trusted Opt-Out promotes list hygiene
- ISPs gain additional Information for decision-making

Consumer Oriented Trusted Email Certification Programs

(Consumer visible seal and interaction)

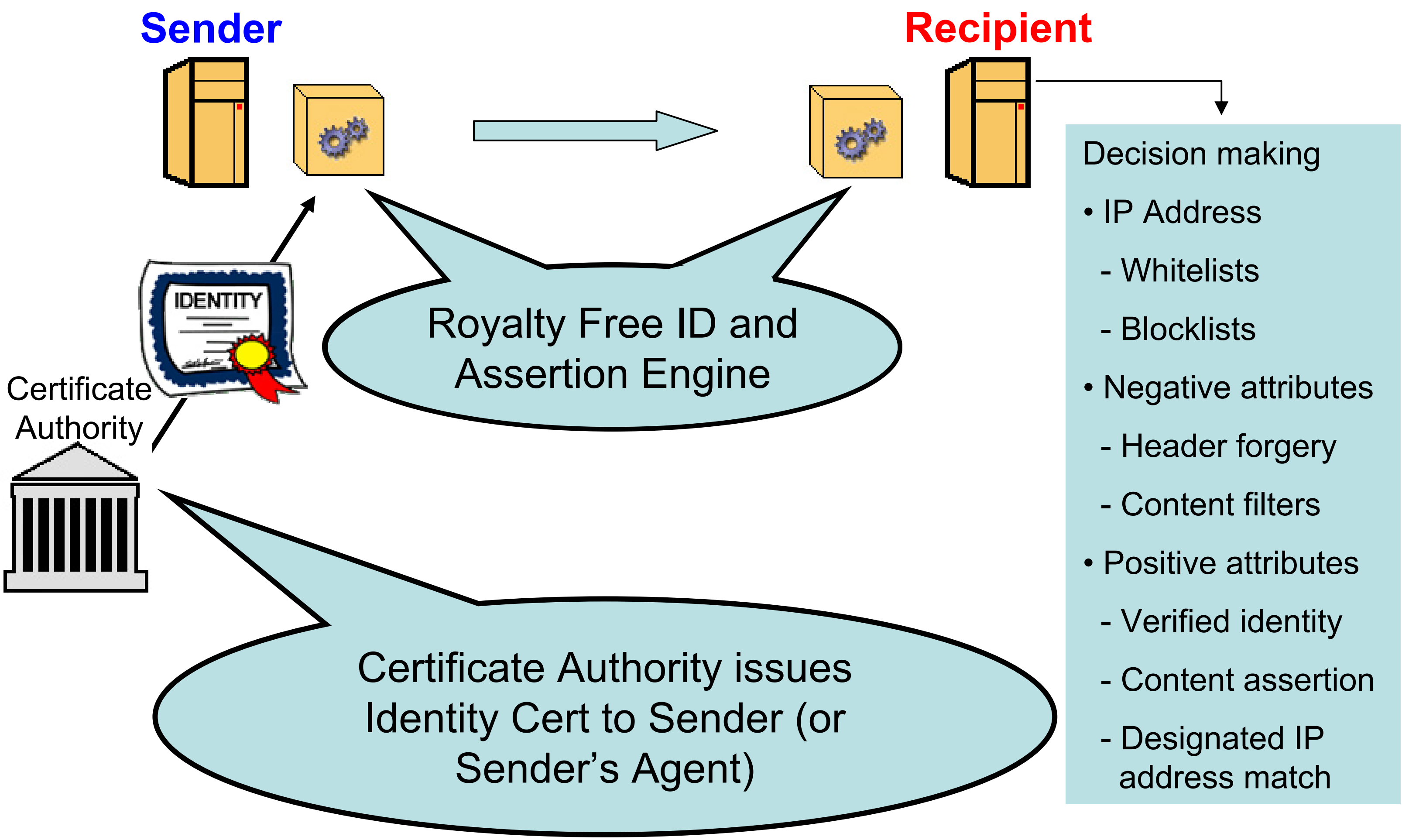
Trust Benefits

- Consumer can easily differentiate legitimate email from spam
- Consumers get much greater trust in identity of sender
- Consumers get greater trust that sender respects their preferences
- Consumers get enhanced trust in sender (even if already a trusted brand)

Economic Benefits

- Greatly increased open rates
- Greatly increased click-through
- Greatly reduced opt-out rates

Trusted Email in Practice



Sender

Recipient

Certificate Authority

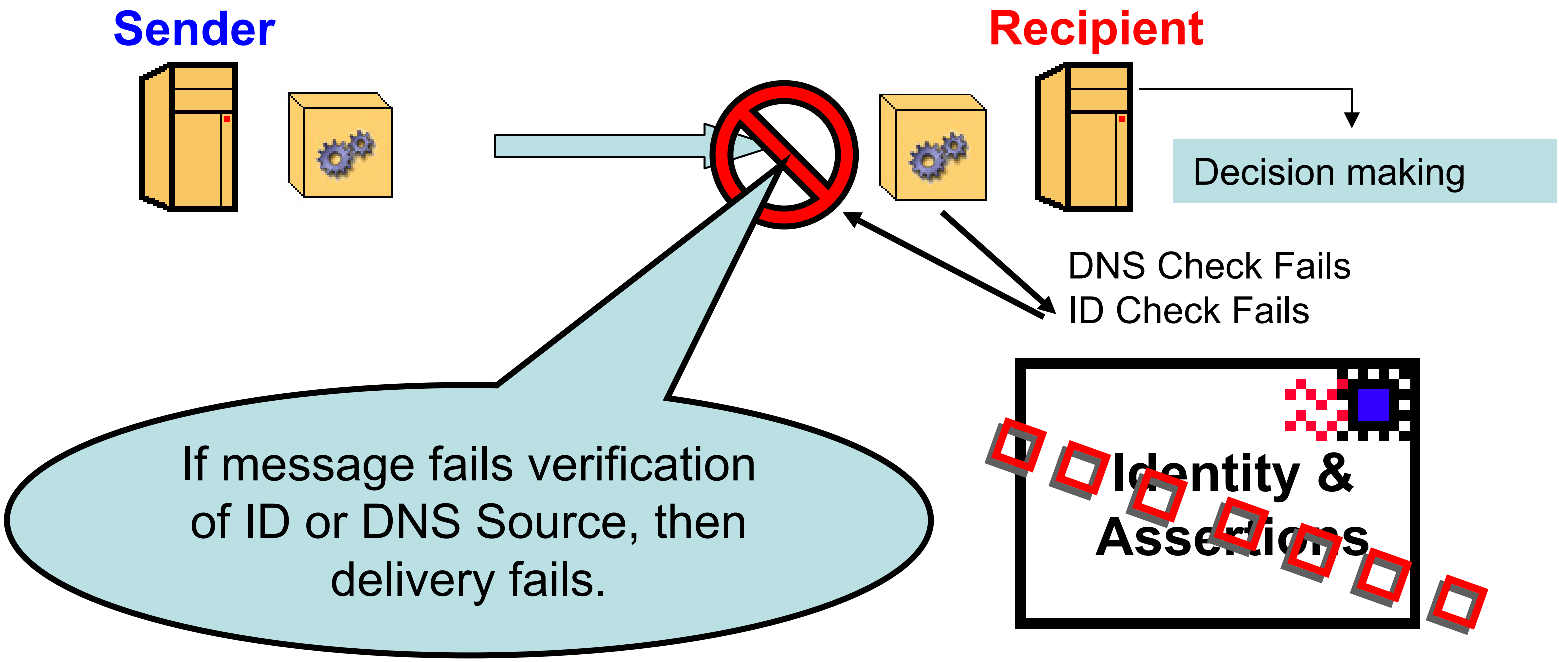
Royalty Free ID and Assertion Engine

Certificate Authority issues Identity Cert to Sender (or Sender's Agent)

Decision making

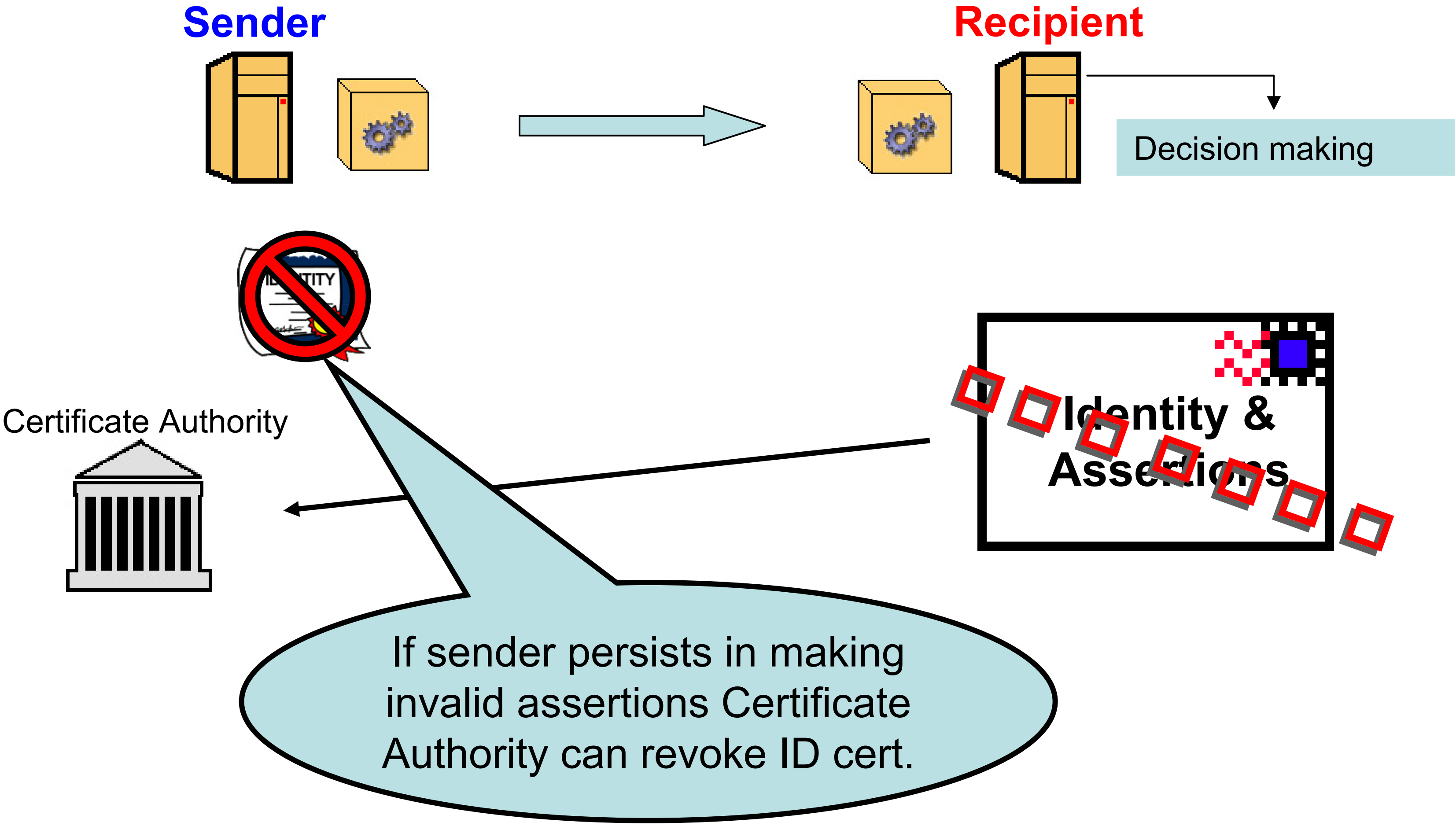
- IP Address
  - Whitelists
  - Blocklists
- Negative attributes
  - Header forgery
  - Content filters
- Positive attributes
  - Verified identity
  - Content assertion
  - Designated IP address match

Consequences for Spoofing



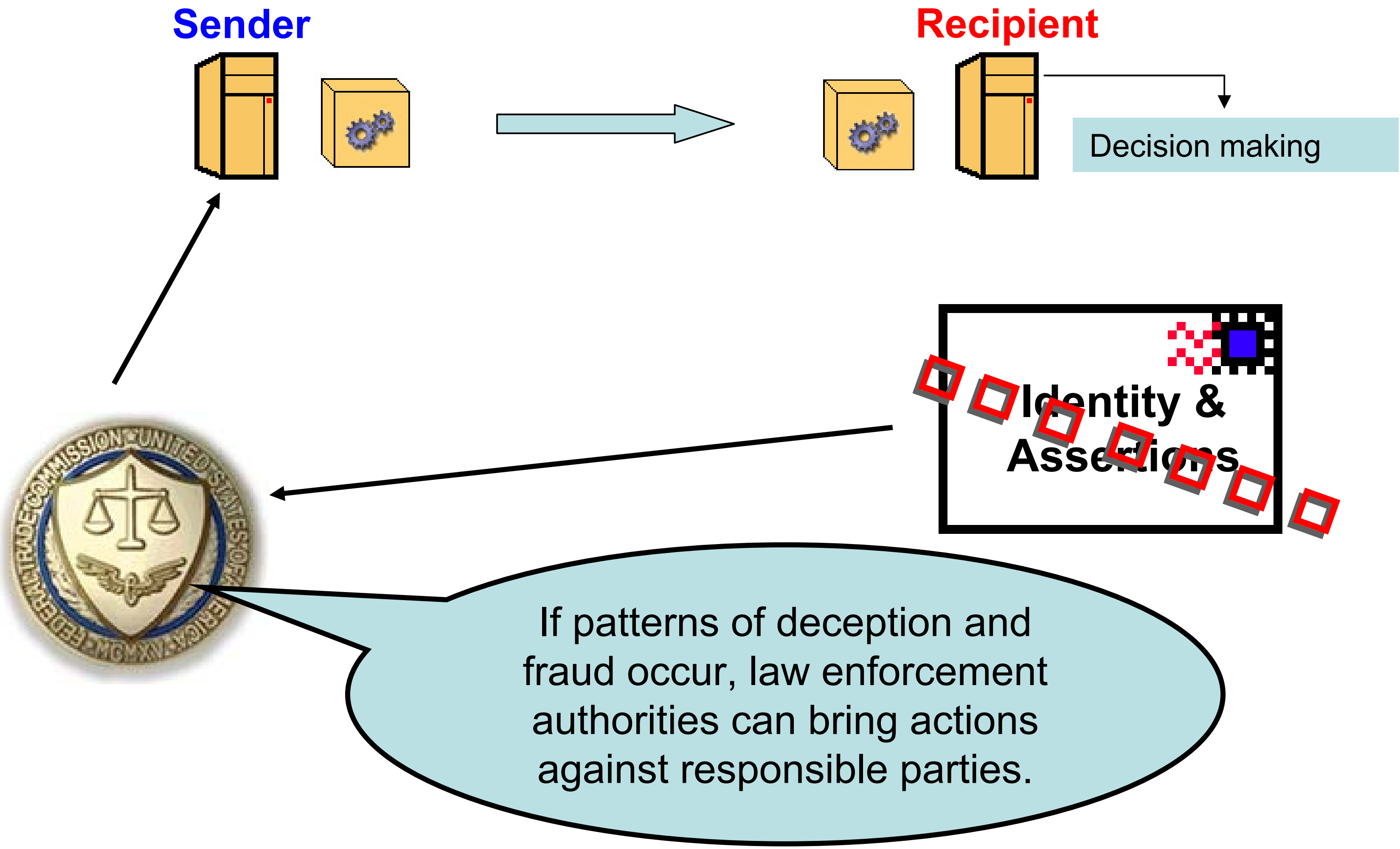
If message fails verification of ID or DNS Source, then delivery fails.

Consequences for Invalid Assertions



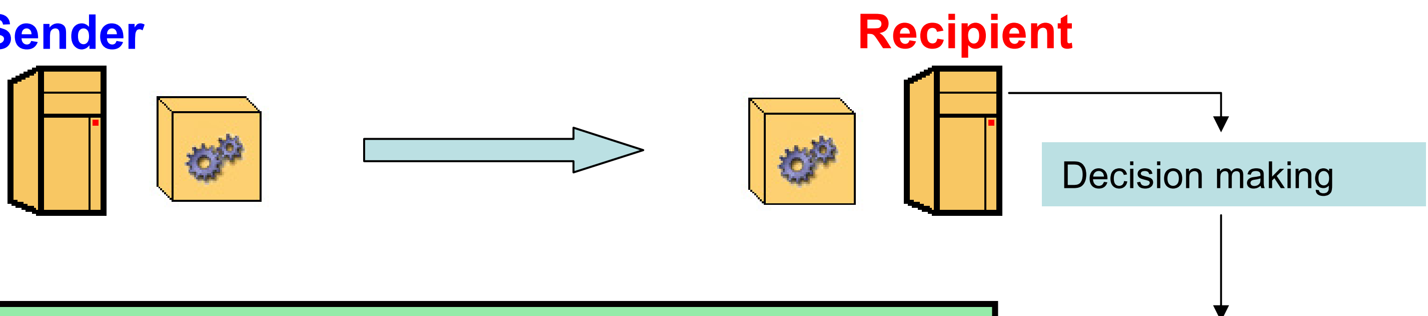
If sender persists in making invalid assertions Certificate Authority can revoke ID cert.

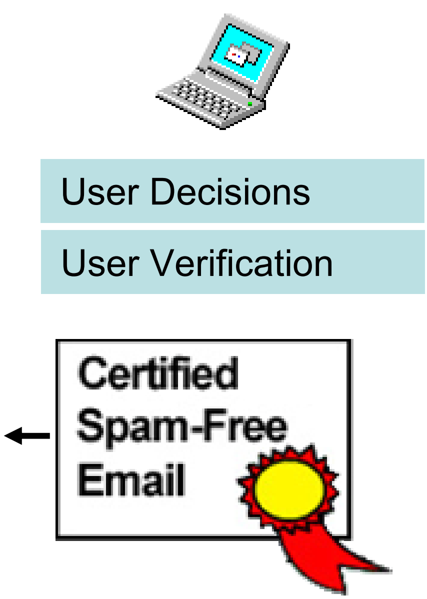
Consequences for Fraudulent Behavior

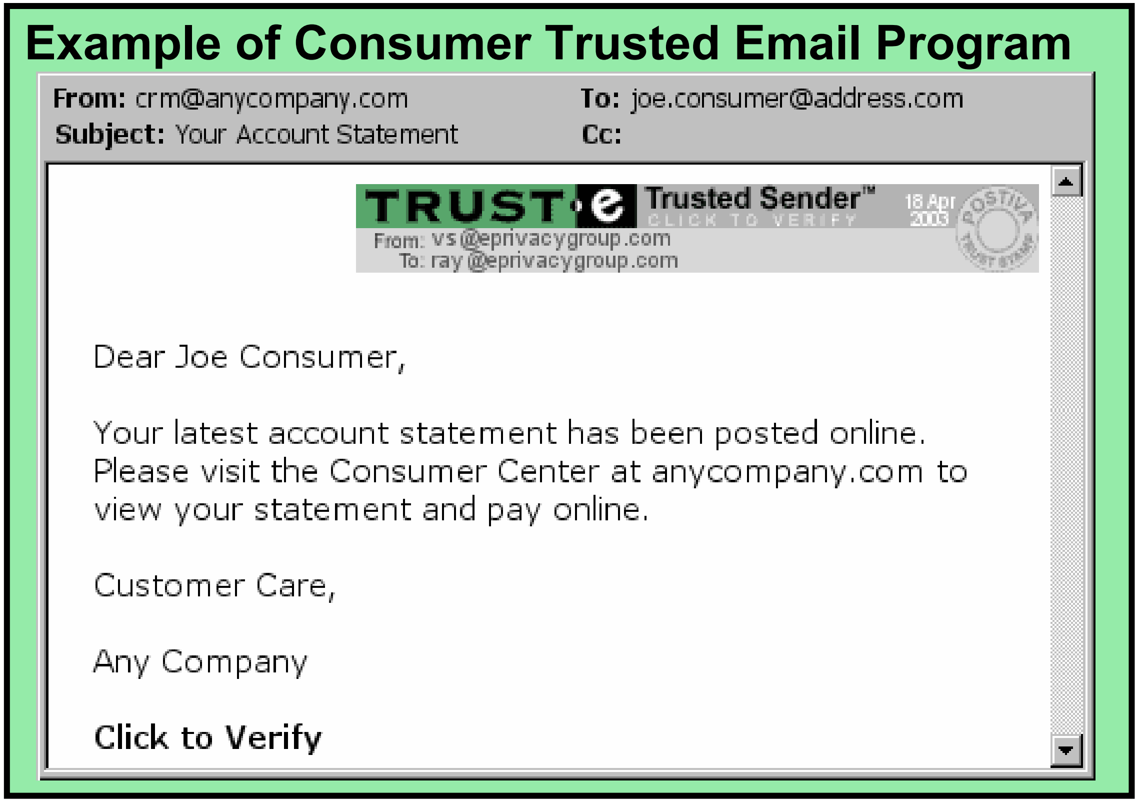


If patterns of deception and fraud occur, law enforcement authorities can bring actions against responsible parties.

Consumer Trust Program – One Example







Example of Consumer Trusted Email Program

From: crm@anycompany.com **To:** joe.consumer@address.com
Subject: Your Account Statement **Cc:**

From: vs@eprivacygroup.com
To: ray@eprivacygroup.com

Dear Joe Consumer,

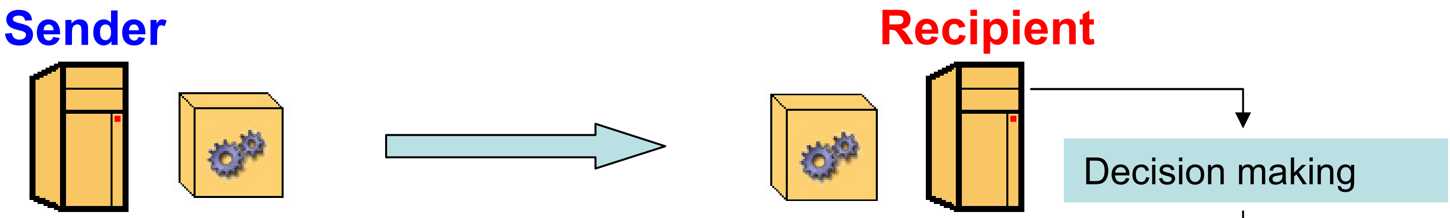
Your latest account statement has been posted online. Please visit the Consumer Center at anycompany.com to view your statement and pay online.

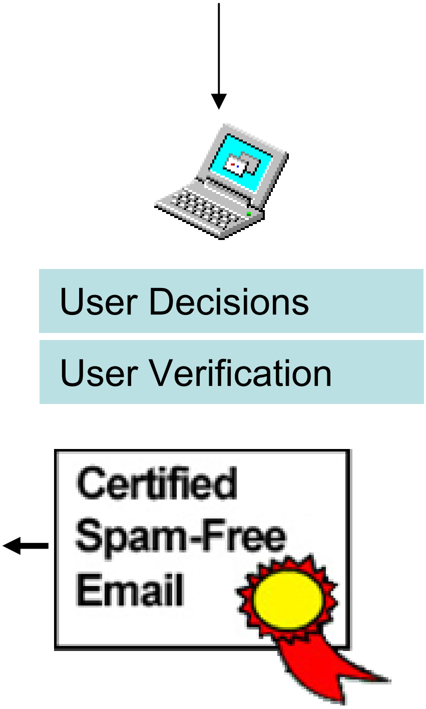
Customer Care,

Any Company

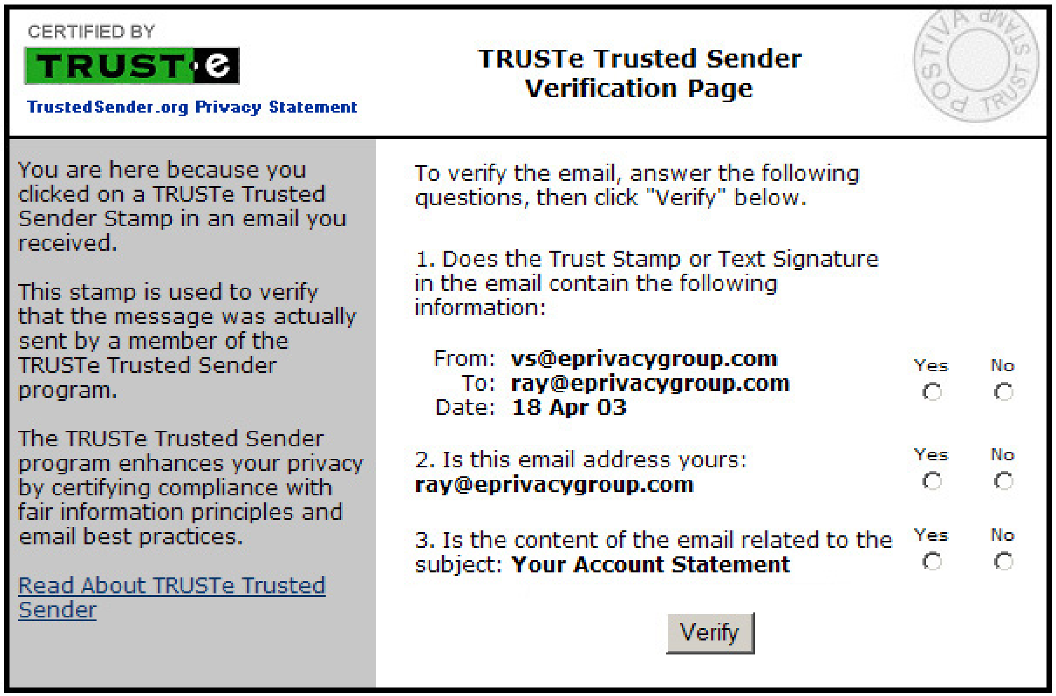
Click to Verify

Consumer Trust Program – Verification





Example of Consumer Trusted Email Program



CERTIFIED BY TRUSTe

TrustedSender.org Privacy Statement

TRUSTe Trusted Sender Verification Page

You are here because you clicked on a TRUSTe Trusted Sender Stamp in an email you received.

This stamp is used to verify that the message was actually sent by a member of the TRUSTe Trusted Sender program.

The TRUSTe Trusted Sender program enhances your privacy by certifying compliance with fair information principles and email best practices.

Read About TRUSTe Trusted Sender

To verify the email, answer the following questions, then click "Verify" below.

1. Does the Trust Stamp or Text Signature in the email contain the following information:

From: **vs@eprivacygroup.com**
To: **ray@eprivacygroup.com**
Date: **18 Apr 03**

Yes ○ No ○

2. Is this email address yours: **ray@eprivacygroup.com**

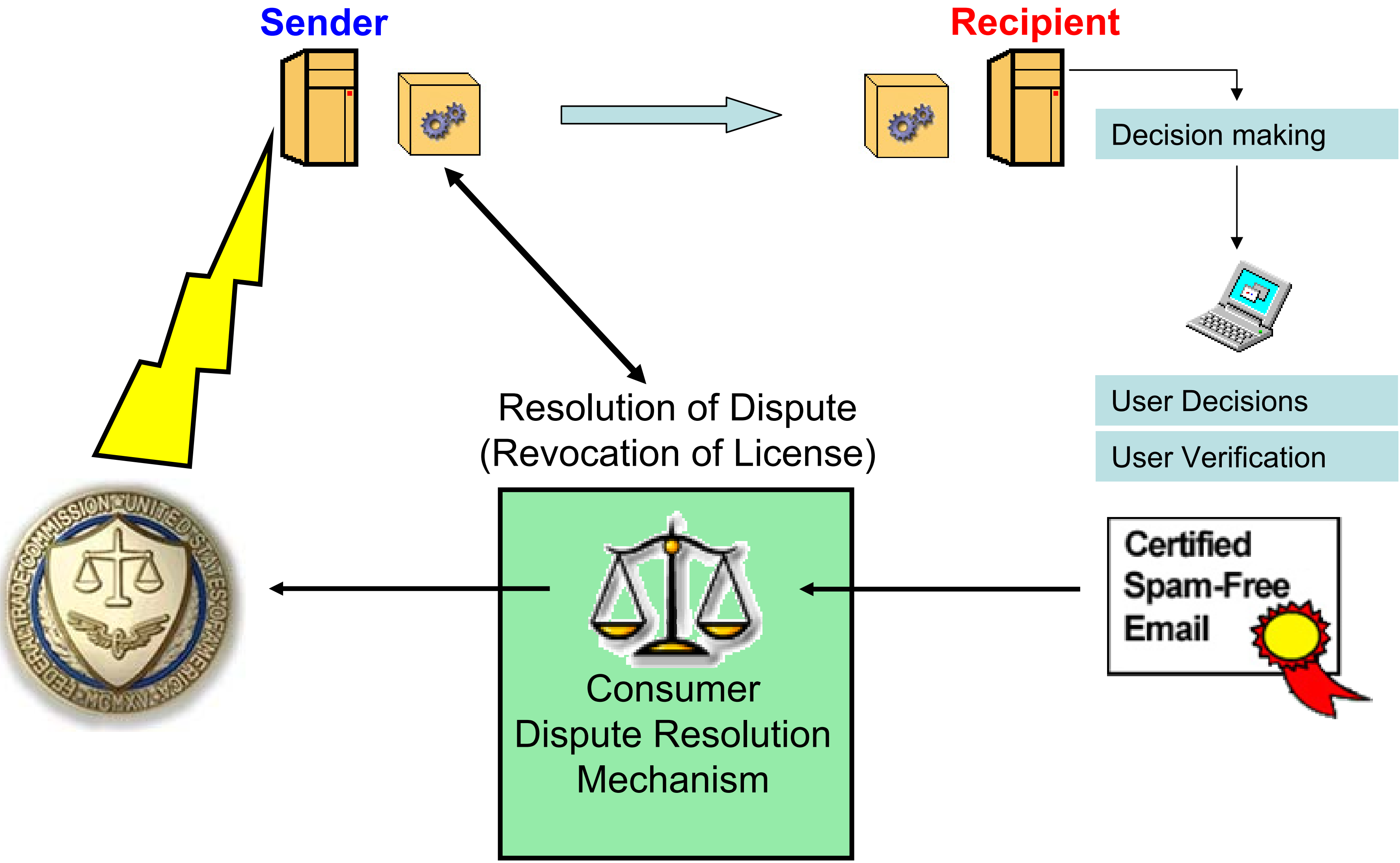
Yes ○ No ○

3. Is the content of the email related to the subject: **Your Account Statement**

Yes ○ No ○

Verify

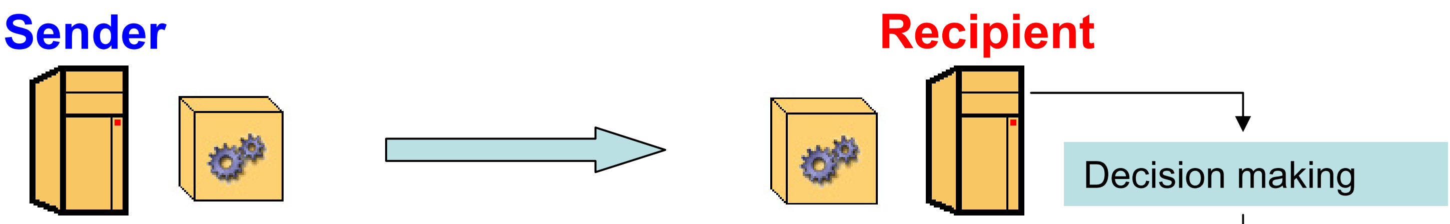
Consumer Trust Program - Dispute Resolution


Sender
Recipient
Decision making
User Decisions
User Verification
Certified Spam-Free Email
FEDERAL TRADE COMMISSION UNITED STATES OF AMERICA MCMXIV

Resolution of Dispute
(Revocation of License)

Consumer
Dispute Resolution
Mechanism

Consumer Trust Programs Increase Trust & Results !



Decision making

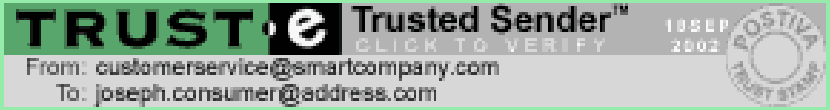
User Decisions

User Verification

User Empowerment

- Certified Opt-Out
- Permission Management
- Dispute Resolution
- Predictability + Accountability = TRUST

Economic ROI


TRUST·e Trusted Sender™ CLICK TO VERIFY 10 SEP 2002 POSITIVA TRUST STAMP

From: customerservice@smartcompany.com
To: joseph.consumer@address.com

- **23%** higher open rate
- **52%** higher click-through rate per delivered email
- **61%** lower opt-out rate per delivered email

Trust ROI

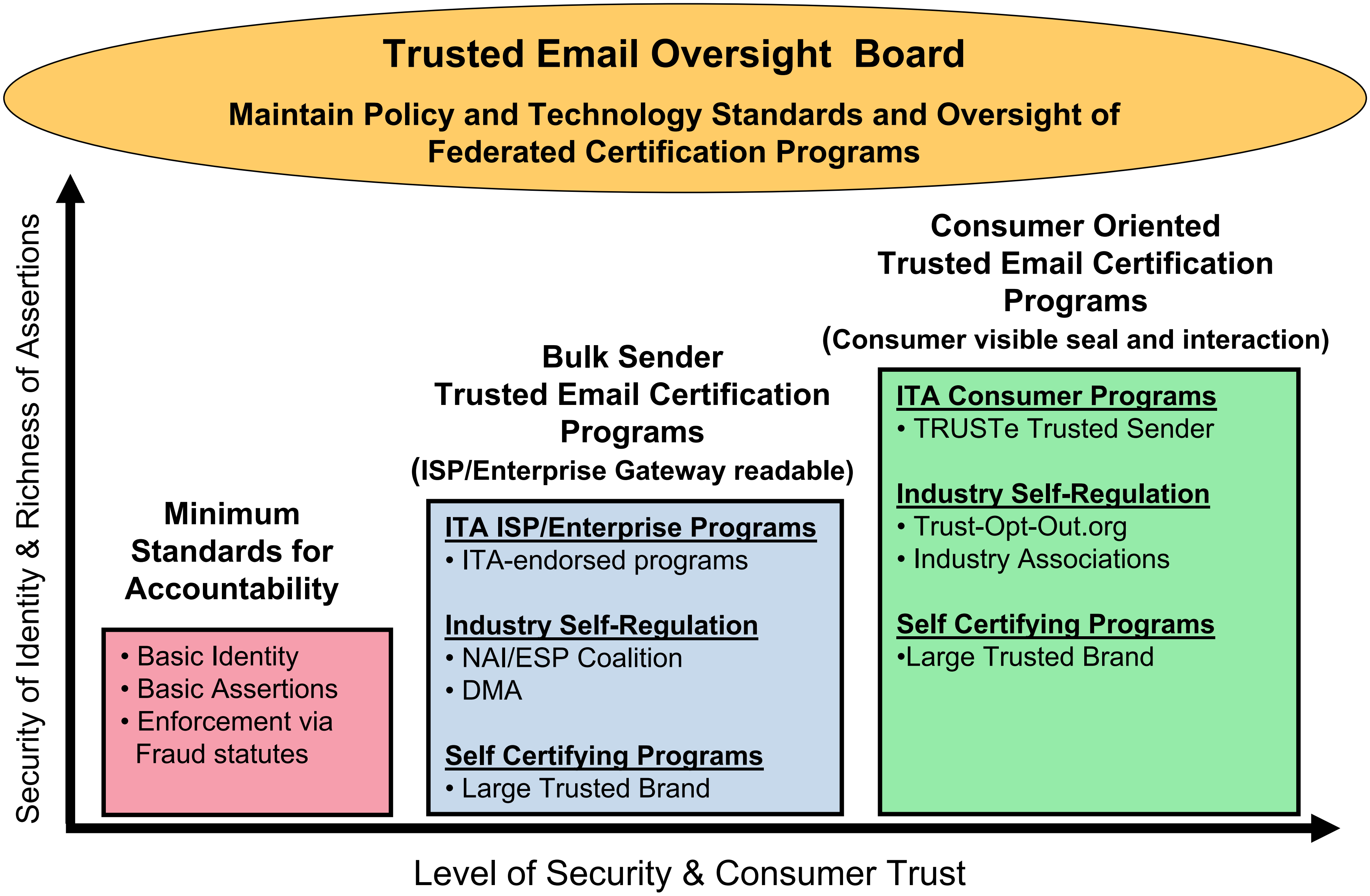
- **81%** report seal increases ability to differentiate legitimate email from spam
- **79%** report seal greatly increases comfort-level in identity of sender
- **76%** report seal increases level of trust that company respects communication preference

Based on consumer company 2003 study of 20,000 customers and 20,000 control group

ePrivacy Group Will Contribute IP to Standards

We are open to contributing elements of our proprietary technology to the common good, for a Trusted Email Open Standard that has:

- The 3 necessary elements:
  - **Policy**: Multiple levels/multiple programs
  - **Enabling technology**: Must include trusted email identity and a common language of trusted declarative statements
  - **Trusted Email Oversight Board**: See next slide
- The strong support and participation of at least 2 large ISP/email client companies
  - AOL, Microsoft, Yahoo, Earthlink



Trusted Email Oversight Board

Maintain Policy and Technology Standards and Oversight of Federated Certification Programs

Minimum Standards for Accountability

- Basic Identity
- Basic Assertions
- Enforcement via Fraud statutes

Bulk Sender Trusted Email Certification Programs

(ISP/Enterprise Gateway readable)

ITA ISP/Enterprise Programs
- ITA-endorsed programs

Industry Self-Regulation
- NAI/ESP Coalition
- DMA

Self Certifying Programs
- Large Trusted Brand

Consumer Oriented Trusted Email Certification Programs

(Consumer visible seal and interaction)

ITA Consumer Programs
- TRUSTe Trusted Sender

Industry Self-Regulation
- Trust-Opt-Out.org
- Industry Associations

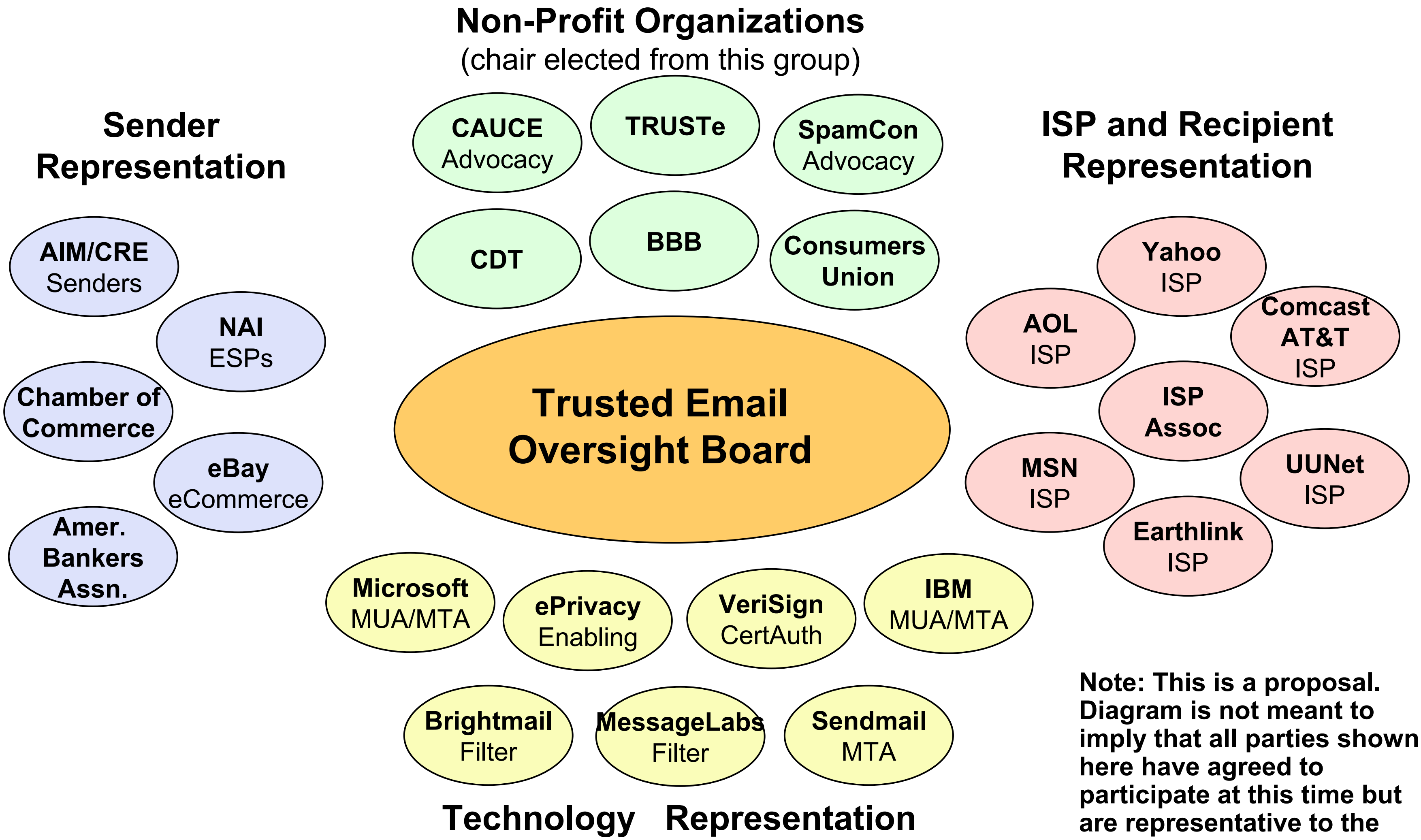
Self Certifying Programs

•Large Trusted Brand

Security of Identity & Richness of Assertions
Level of Security & Consumer Trust

Trusted Email Oversight Board

Design Goals: Credibility and balance of interests



Non-Profit Organizations
(chair elected from this group)

CAUCE Advocacy

TRUSTe

SpamCon Advocacy

CDT

BBB

Consumers Union

Sender Representation

AIM/CRE Senders

NAI ESPs

Chamber of Commerce

eBay eCommerce

Amer. Bankers Assn.

Trusted Email Oversight Board

ISP and Recipient Representation

Yahoo ISP

AOL ISP

Comcast AT&T ISP

ISP Assoc

MSN ISP

UUNet ISP

Earthlink ISP

Microsoft MUA/MTA

ePrivacy Enabling

VeriSign CertAuth

IBM MUA/MTA

Brightmail Filter

MessageLabs Filter

Sendmail MTA

Technology Representation

Note: This is a proposal. Diagram is not meant to imply that all parties shown here have agreed to participate at this time but are representative to the interests to be represented.

Trusted Email Programs Structure Follows Law

ISP/Enterprise Gateway Trust Program
Program: ABC Bond Program
Trust Authority:
Operator:
Participants:

Component:		Description/Comments:
Notice:		
Identity Type		
Choice:		
Access:		
Security:		
Dispute:		
Notes:		

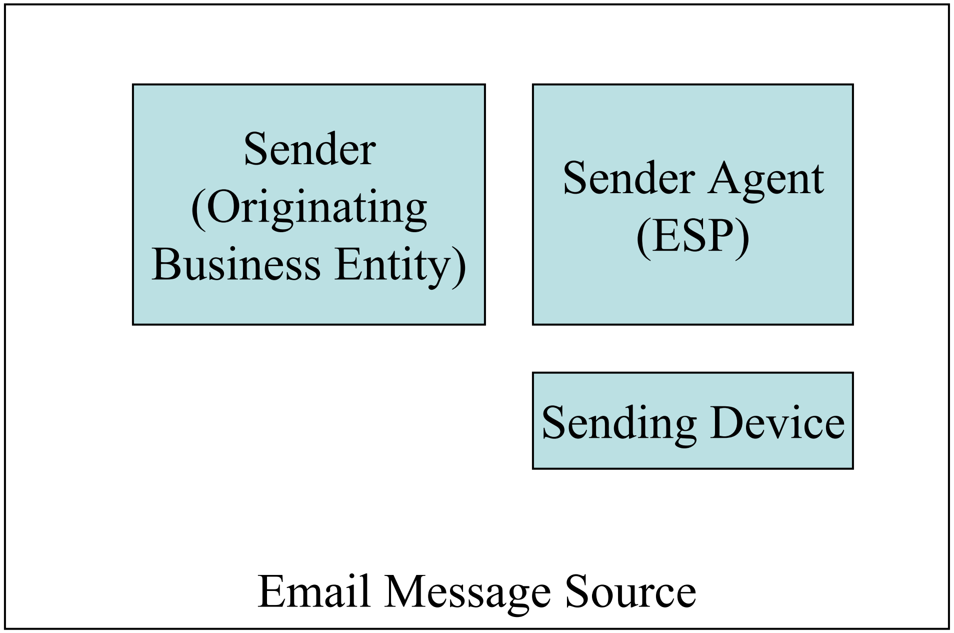
Consumer Email Trust Program
Program: TRUSTe Trusted Sender
Trust Authority: TRUSTe
Operator: ePrivacy Group
Participants:

Component:		Description/Comments:
Notice:		
Identity Type		
Choice:		
Access:		
Security:		
Dispute:		
Notes:		

Technical Elements

Secure Identity

- Real identity resolved to cryptographic keys
  - Each 'email message source' has a unique public/private key pair
- Identity issuers and Trusted Email Programs sign public keys



Conveying Secure Identity

- Data added to x-headers of email message
  - Public key of message source
    - Identity issuer
    - (optionally) Trusted Email Program(s) keys/signatures
  - Signed message specific data
    - SMTP envelope sender & recipient
    - SMTP envelope recipient
    - Message-specific data (data/time, id, etc)
    - Assertions
- All data 'clear-text signed' to permit optimization of processing
  - Cryptographic operations optional, can be path-optimized or performed on exception basis
  - DNS is an important optimization, and path optimization ensures that cryptographic verification is at the option of the receiver

Secure Assertions

- Flexible, extensible language and framework for communication of Trusted Declarative Statements (Assertions)
- Must allow 1st party statements about sender, recipient and content
  - ‘Message Type’ a key required assertion
- Must allow trusted 3rd party statements about sender, recipient and content
  - ‘Program Membership’ asserts sender membership in 3rd party principle-based trust program
- Per-Message Assertions
  - Must provide for assertions about each individual message. General information about a sender is valuable but insufficient for the required decision processing

Implementing Identity & Assertions

- Standards compliant, header-based, lightweight (several hundred bytes), cryptographically signed data
  - Forgoes the weight and computational expense of S/MIME and typical PKI implementations
  - Persistent and secure, empowering all email processing components, including the MUA, to verify authenticity as appropriate
  - Utilizes RSA asymmetric cryptography, SHA1 hashes. X509v3 compatibility leverages existing CA infrastructure
- Bytecode/Operator structure for communication of Assertions
  - Expandable to XML for human processing using existing tools
  - Computationally inexpensive to process in real time

Conclusions:

- **Trusted Email Open Standard** can happen now
  - Time is right
  - Pain level is right
  - Cooperation level right
- **Trusted Email Open Standard** benefits senders
  - Low cost to implement
  - Elimination of false positives
  - Trusted Opt-Out promotes list hygiene
  - Extremely positive consumer response is “Win-Win-Win”
- **Trusted Email Open Standard** benefits recipients
  - Reduces spam
  - increases recipients ability to differentiate good email from bad

Trusted Email is proven to work well

for Senders, ISPs and recipients.

Thank You

Vincent Schiavone

President & CEO

ePrivacy Group

phone: 610.407.7083

email: vs@eprivacygroup.com