Fighting Abuse with Trust: *Enhancing the paradigm*

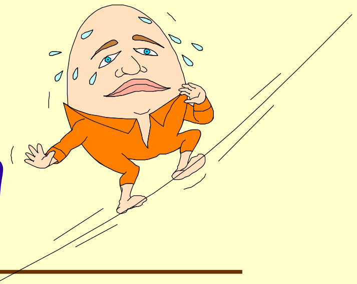
Dave Crocker
Trusted Domain Project (trusteddomain.org)
Brandenburg InternetWorking (bbiw.net)

FCC ~ 2 Feb 12

Internet Abuse

- **Advertising (spam)**
  - *Aggressive, legimitate companies*
  - *Deceptive, criminal-like organizations*
- **Fraud**
  - *Phishing*
  - *Illegal purchases*
- **Destruction (DDOS)**
  - *Extortion*
  - *Anger*
- **Well-organized**
  - *Extensive, hierarchical underground economy*
  - *Trans-national*
- **"The Net is too Open"**
  - *Or, "an error in Internet design is a failure to authenticate users"*
  - *Just like the real world...*
- **Abuse is a social problem**
  - *Social problems are not amenable to technical solutions*

It's Persistent and Spreading



20 years of:

Look for bad actors, using IP Address of neighbor

Looking for bad content

Progress?

Excellent filtering engines protect receivers

No significant change across open Internet

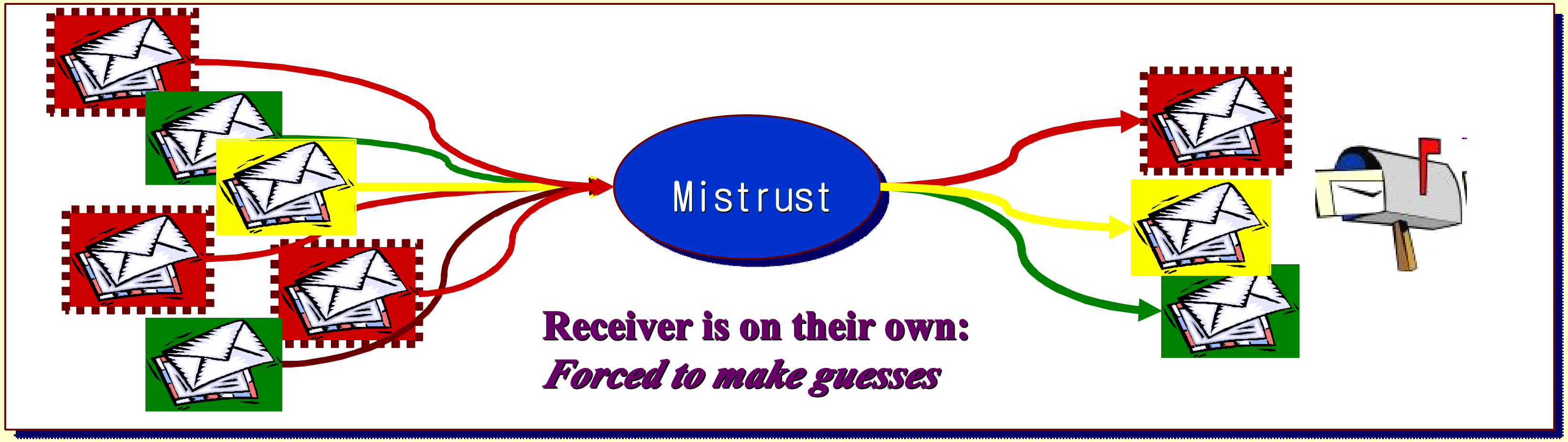
Victories are ephemeral

This is an arms race and the enemy is well-funded, bright and aggressive

Abuse will end on the Internet when it ends on the streets...

Email → Web → IM → Blogs → VOIP → mobile…

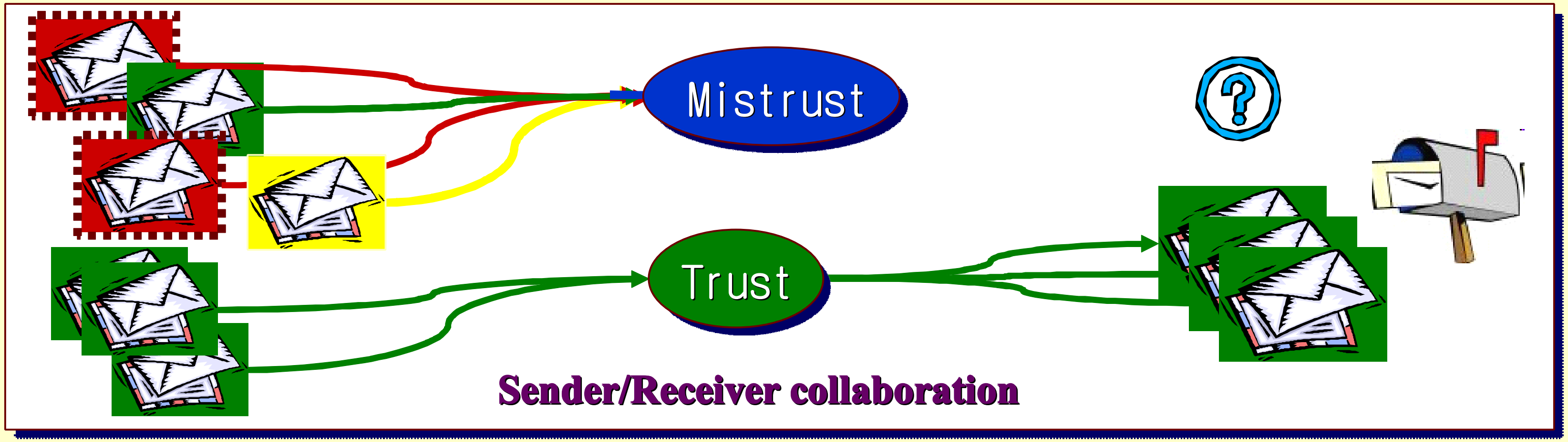
Mistrust vs. Trust



Mistrust

Receiver is on their own:

Forced to make guesses



Mistrust

Trust

Sender/Receiver collaboration

Different and Complementary

Mistrust

Sender actively trying to trick receiver

Content is usually spoofed

Heuristics (Bayes, Blacklists, etc.) to distinguish valid from spoofed

… Look for content to reject

Trust

Sender is collaborating, at least for identifier

With valid identifier can be an assessment (reputation) not confused by “noise” of bad actors

DKIM, SPF, DMARC, Whitelists, DNSSec, DANE, Repute, OpenDKIM

… Look for content to accept

Trust is Becoming Fashionable

This week's announcement of DMARC:

> *“Google, Microsoft, PayPal, Facebook and other big names have announced a new anti-spam and phishing project, [that] will use 'a feedback loop between legitimate email senders and receivers to make impersonation more difficult'”*
>
> *-- Slashgear 30jan12*

Forthcoming Book:

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, Bruce Schneier

Roles & Responsibilities, Tussles & Trust

Actors

People, organizations and processes that are responsible for sets of actions

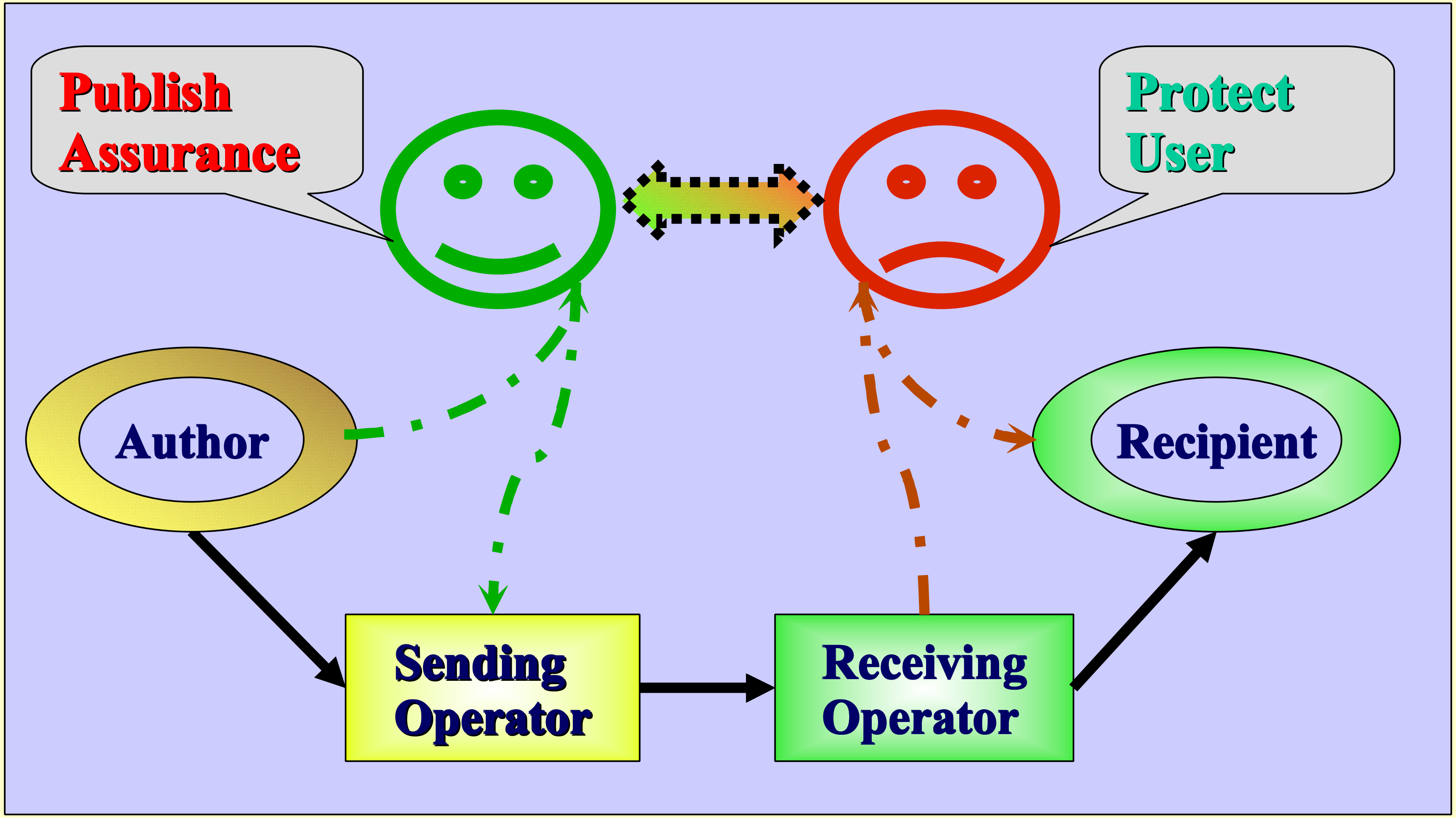
Examples: Author, Recipient, Mailing list, Operator

Administrative [Management] Domains (ADMD)

Components organized under an integrated span of control, with common, internal trust

Example: Within organization, versus between

A Negotiation View of Send/Receive or Pub/Sub



Publish Assurance

Protect User

Author

Recipient

Sending Operator

Receiving Operator

Trust Begins with Authenticated Names

Domain Name

- ***Organizational boundary****, not network topology*
- *More stable and reliable than IP Address*
- *Easier to manage than personal identifiers*
- *Sub-domain names permit added flexibility*

Personal name

- *Necessary only when the trust is independent of a larger organization*

Identifying Content Streams

Multiple “types” of content

Corporate

Transactions (purchase order, order confirmation...)

Proposals

Marketing mass mailings

Customer Support

Label them with subdomains

sales.bbiw.net

newsletter.bbiw.net

personal.bbiw.net

Allow different reputations to develop

Warning: Naming is Confusing

(Even Email From: Field is Complex)

Dave Crocker <dcrocker@bbiw.net>

- ***"Display Name"*** *— never validated!*
- ***Mailbox*** *— controlled by ADMD*
- ***System*** *or Organization (ADMD)*

Users only see the Display Name...

- ***Trust mechanisms are (mostly) for operators, not users!***
- ***Human factors issues make end-users poor enforcers of security***
- ***Saying that better security requires better user training is dereliction of duty...***

Naming and Other Applications

- **Some are like email**
  - IM, VOIP
- **Some have no visible naming (Web)**
  - *But the structure of data permits adding attributes*
  - *So add one with a name*
- **Popular Web security**
  - ***TLS** (http**s**)*
  - *Protects **channel**, not "**object**"*
  - *Really only privacy and a bit of server*

- **Active IETF efforts**
  - ***SPF, DKIM** for mail*
  - ***DANE** for better channel (TLS) certification*
  - ***Websec** for better Web content (object) certification*
  - ***OAuth** for Web authorization (login)*
  - ***Repute** to query reputation information*
  - ***draft-dispatch-ono:** Referencing and Validating User Attributes*

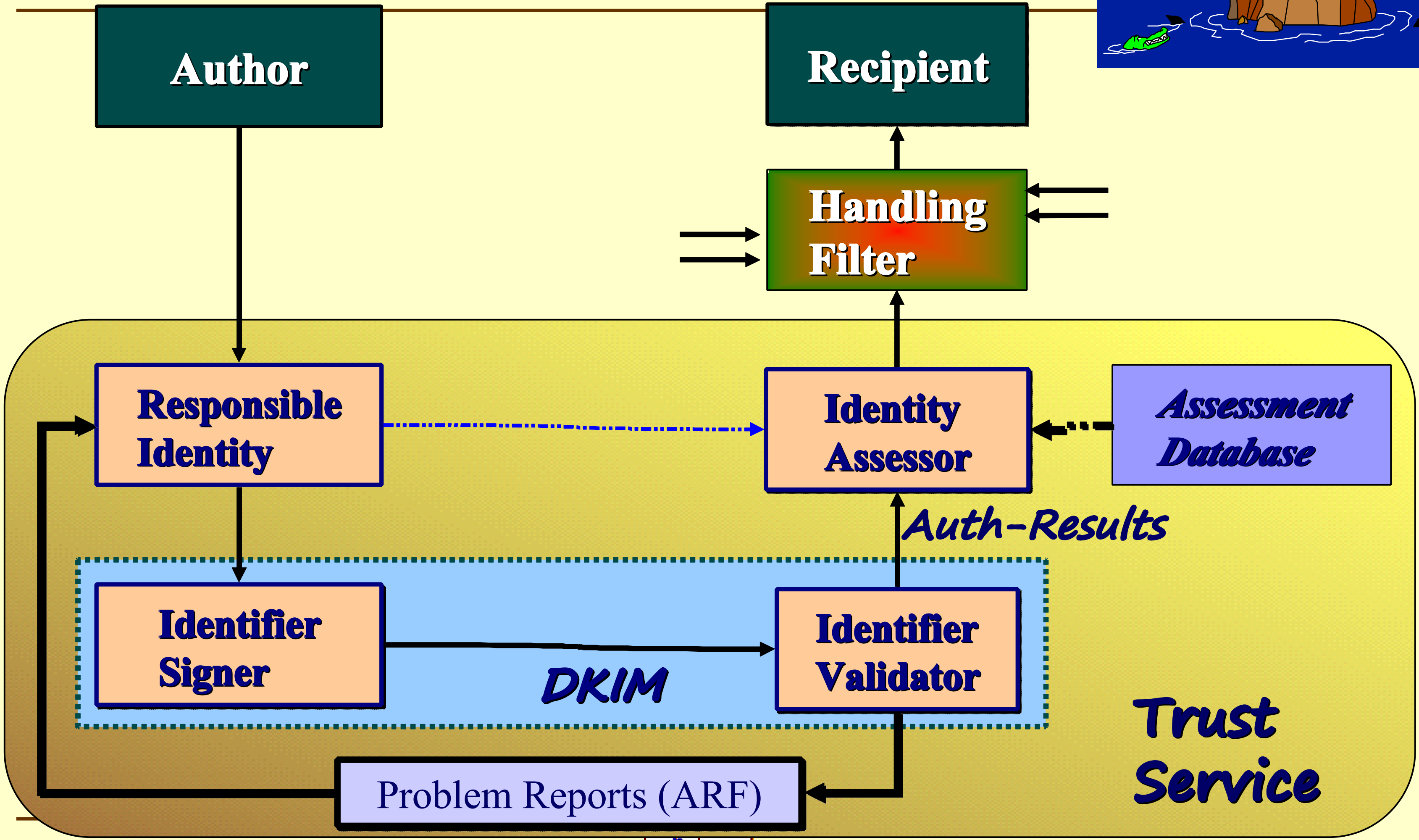
An Amateur's View of Security

- **Ambiguous uses of terminology**
  - “Security”, “authentication”, “validation”, “certification”, “privacy”
- **Very high barriers to entry**
  - Administration, operations, end-user usability
  - For example: certificates...

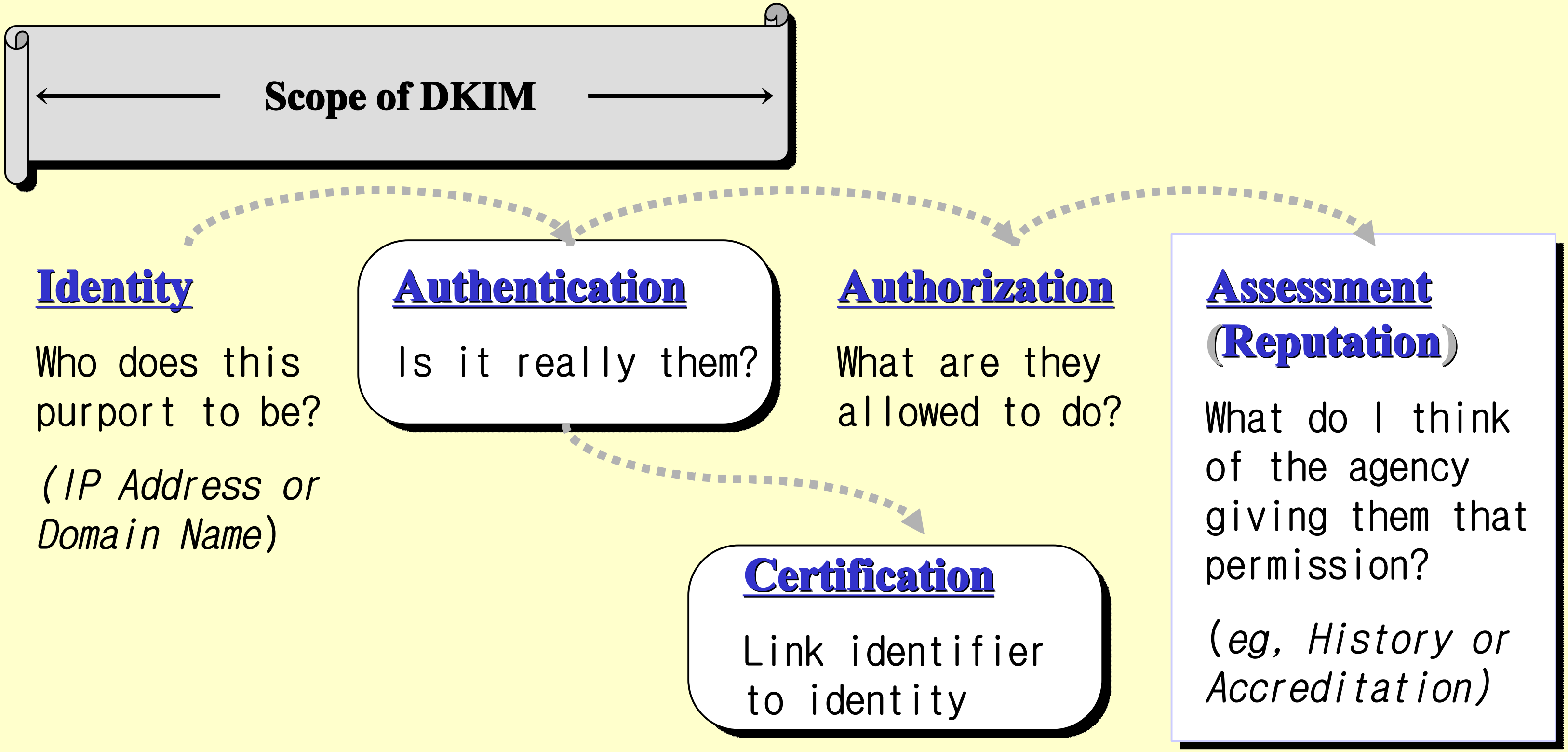
- **Authentication/Validation of...**
  - ***Actor*** *– author vs. recipient vs. handler*
  - ***Content validity*** *– content is truthful vs. accurate vs. ...?*

- **Compare precision and implications:**
  - “XML Signatures provide integrity, message authentication, and/or signer authentication”
  - “DKIM... permit[s] verification of the source and message contents”
  - “DKIM permits a person, role, or organization to claim some responsibility for a message”

Trust Service Architecture



Authentication as a Part of…



Scope of DKIM

Identity

Who does this purport to be?

(IP Address or Domain Name)

Authentication

Is it really them?

Authorization

What are they allowed to do?

Assessment (Reputation)

What do I think of the agency giving them that permission?

(eg, History or Accreditation)

Certification

Link identifier to identity

Assessment

History *(statistical reputation)*

Past performance ***is*** *indicator of future behavior*

But what if there is no history (eg, new name)?

Affiliation *(objective information)*

Membership in recognized group is a good sign

*eg, fcc.**gov**, "member FDIC", 501(3)(c)*

Vouching/Reputation service *(opinion)*

Trust those who you trust say are trustworthy...

Challenges

Complexity and usability

Additional layer of service and operations

Requires excellent quality control

Subjet to social engineering

Funding

Standalone reputation services have failed

Reduced functionality

Every packet is patted down when crossing administrative domain boundary?

Functional fixedness

*Trust mechanisms primarily being considered for finding **bad** actors!*

Thank you...