# IDENTIFIED INTERNET MAIL

JIM FENTON

DISTINGUISHED ENGINEER

CISCO SYSTEMS, INC.

# Goals of Identified Internet Mail

- Provide tools to identify and block spoofed email
- Preserve the positive aspects of email
  - Anyone can send to anyone, without introduction
  - Senders can be anonymous to the extent they are now
  - Ability to send mail independent of location
- Messages should not fail verification in case of inconsequential modifications
  - Accommodate common mailing-list behavior
- Use existing trust hierarchies
  - Inclusive of large and small domains
  - Easier to deploy rapidly—processes are already defined
- Support mechanisms that evaluate reliability of message senders

# Authentication/Authorization Model

## Messages must pass two tests before they are authenticated

### AUTHENTICATE THE MESSAGE

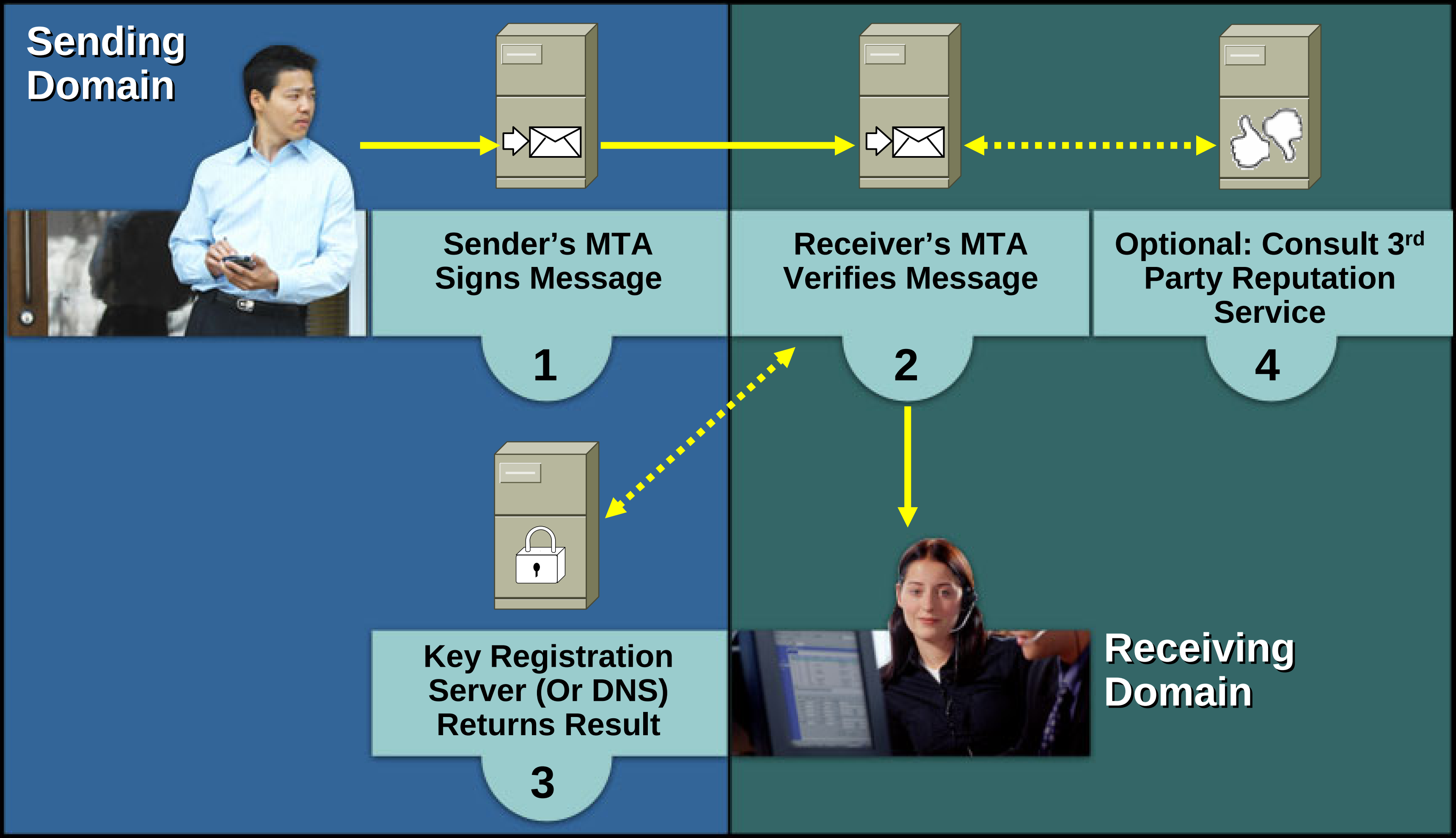
Receiving domain authenticates the message—i.e. Verifies that the message was not altered in any consequential manner prior to reaching the receiving domain

+

### AUTHORIZE THE SENDER

Receiving domain asks sending domain to confirm that whoever signed the message was authorized to do so (without having to identify the sender)

# Identified Internet Mail Explained



Sending Domain

Sender's MTA Signs Message
1

Receiver's MTA Verifies Message
2

Optional: Consult 3rd Party Reputation Service
4

Key Registration Server (Or DNS) Returns Result
3

Receiving Domain

# User-level Keys and Privacy

- Signing normally occurs at domain level
- Some users will need to sign their own messages
  - Users sending messages from outside their home domain
  - Roving users, mobile phones, PDAs
  - “Affinity addresses” (e.g., ieee.org)
- Outsourced services sending email sign client addresses
  - Email marketers
- User-level keys need not specify identity of signer
  - Only that signer was authorized by the sending domain
- A few domains will need large numbers of authorized keys
  - Key authorization must scale adequately

# IIM Support for Wide Range of Use Cases

| | IIM Support |
|---|---|
| Authorize signing by third-party partner companies | ✓ |
| Scale to support dispersed work force | ✓ |
| Support for common behavior of mailing lists | ✓ |
| Flexible use of affinity email addresses | ✓ |
| Single user with multiple devices | ✓ |
| Third party message transmission | ✓ |
| Authorize users to sign messages for multiple email accounts | ✓ |

# Example of Signed Message

```
Subject: Sample message
From: John Doe <jdoe@example.com>
To: Mary Smith <msmith@example.net>
Content-Type: text/plain
Message-Id: <1098727240.13184.0.camel@lucid.example.com>
Mime-Version: 1.0
X-Mailer: Ximian Evolution 1.4.6 (1.4.6-2)
Date: Mon, 25 Oct 2004 11:00:40 -0700
Content-Transfer-Encoding: 7bit
IIM-SIG: v:"1"; h:“lucid.example.com"; d:“example.com"; z:"home"; m:"krs";
   t:"1098727241.26722"; x:"432000"; a:"rsa-sha1"; b:"nofws:31";
   e:"Iw=="; n:"1hl/HhbD4yHBqFXxH3+ERpvWgnWfwczz5NhfB7tmP/PfdBa6OUZi+LHQvxOUF"
   "MHOw2H5M0/E84eJ/HyNmzszCXfoqGNvqmR1kyceOmW4auQ9CBz868jzUpe/Nw"
   "/B82DxH+ikRGeoUsMHSJ2POdwjOuKXxbSWWRu9Yzft5ASbOpc=";
   s:"J2LbKMHfW2XkZJwP05Cm+IadAJaED1dZ8lSZo7asq7KUZGJwBOuI6W9DRrcvA"
   "LGgb3z3ozxCEL2gjref8dwtofuwHAmTEXiXpaChBIKM7zPIctpCM8G7onDiX9"
   "2ao+/YPO86xww+MIkFoG2jtEZTJtoli2AH+LLvJXOR3+USJEg=";
   c:"Subject: Sample message";
   c:"From: John Doe <jdoe@example.com>";
   c:"Date: Mon, 25 Oct 2004 11:00:40 -0700"
IIM-VERIFY: s:"y"; v:"y"; r:"60"; h:“incoming.example.net";
   c:"message from lucid.example.com verified; "
```

Public Key

Signature

Copied Headers

CISCO SYSTEMS®