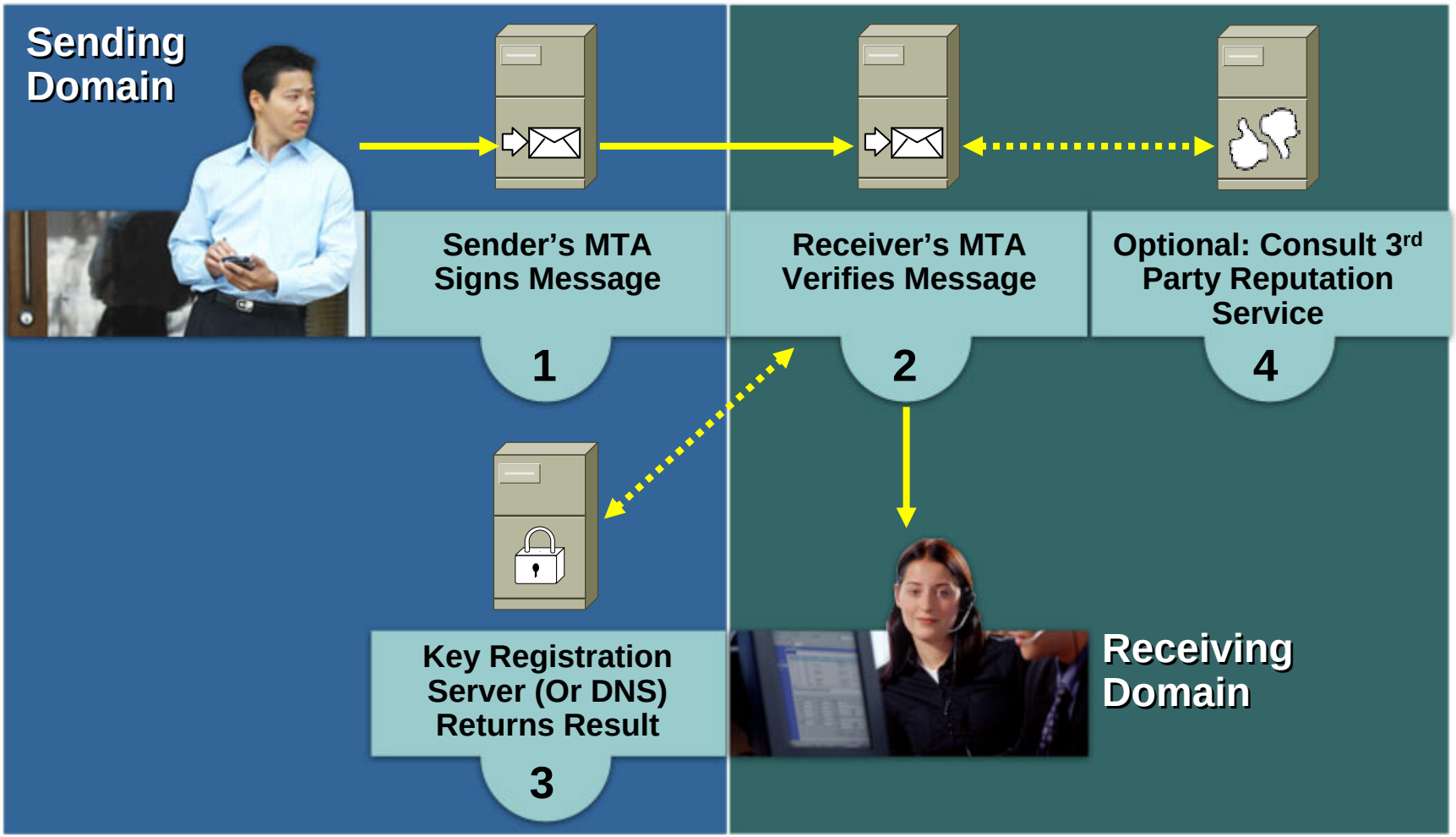
IDENTIFIED INTERNET MAIL AND DOMAINKEYS

JIM FENTON <fenton@cisco.com>

Introduction

- **Identified Internet Mail (IIM) and DomainKeys (DK) are signature-based methods of authenticating messages**
- **Published as Internet Drafts in 2004**
- **Implementations exist for both and some deployment experience has been obtained**

Identified Internet Mail Explained



DK/IIM Similarities

- **Signature appears as an additional message header**
  - **Generally ignored by non-signature-aware elements**
- **Signing and verification typically take place at MTAs, but may occur at MUA**
- **PGP signature over selected headers and body**
  - **Canonicalization may be used to allow “safe” modifications like spacing changes**

DK/IIM Differences

	Identified Internet Mail	DomainKeys
Key Distribution	Key sent in message	Key retrieved from DNS
Header Signing	Signed copy of selected headers	Signed headers determined by position
Signature Timestamps	Signing time, signature time-to-live	None

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)

Deploying Message Signing

- **Deploy a signature-capable MTA**
  - **Major MTA appliance vendors are adding signature support**
  - **“Milter” API software available for sendmail**
  - **DomainKeys toolkit for other MTAs (e.g., qmail)**
- **Generate and publish message signing keys**
  - **Published in DNS records in a separate subdomain**
  - **May delegate key subdomain to mail administrators**
  - **Optional: Publish a message signing policy**
- **Tell users how to handle message verification results**

Current Status

- DomainKeys is currently deployed by Yahoo!, GMail, several hosted domains, and some smaller domains
- IIM currently deployed in portions of Cisco and several smaller domains
- Focused effort on unifying the two proposals
  - Expect a single signature in the future
- Efforts on protocols for accreditation and reputation are just beginning