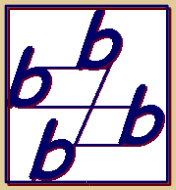


Mail Service Quality Support:
CSV and BATV

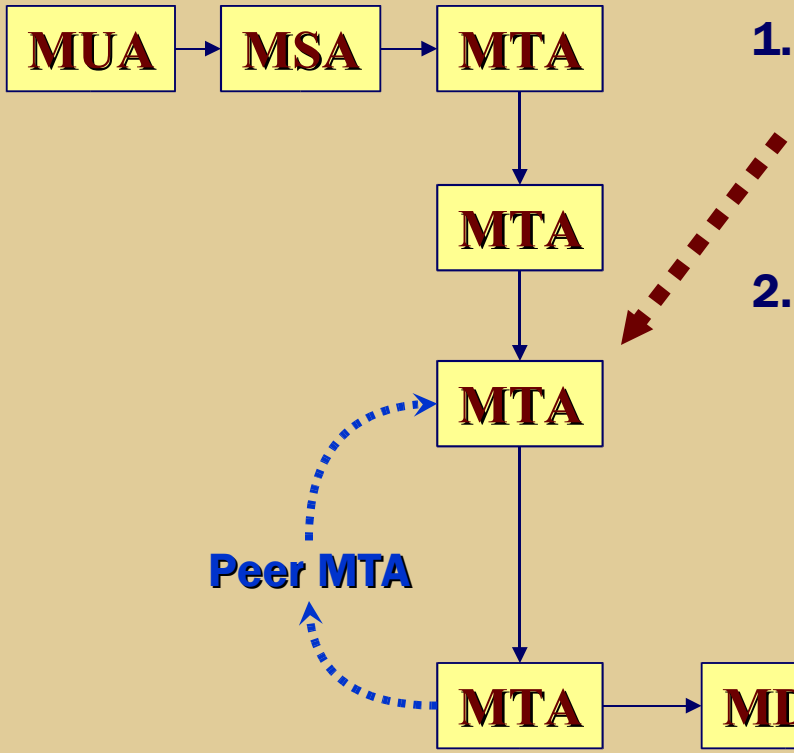
APCAUCE/APRICOT – Kyoto 2005

Dave Crocker

Brandenburg InternetWorking

bbiw.net

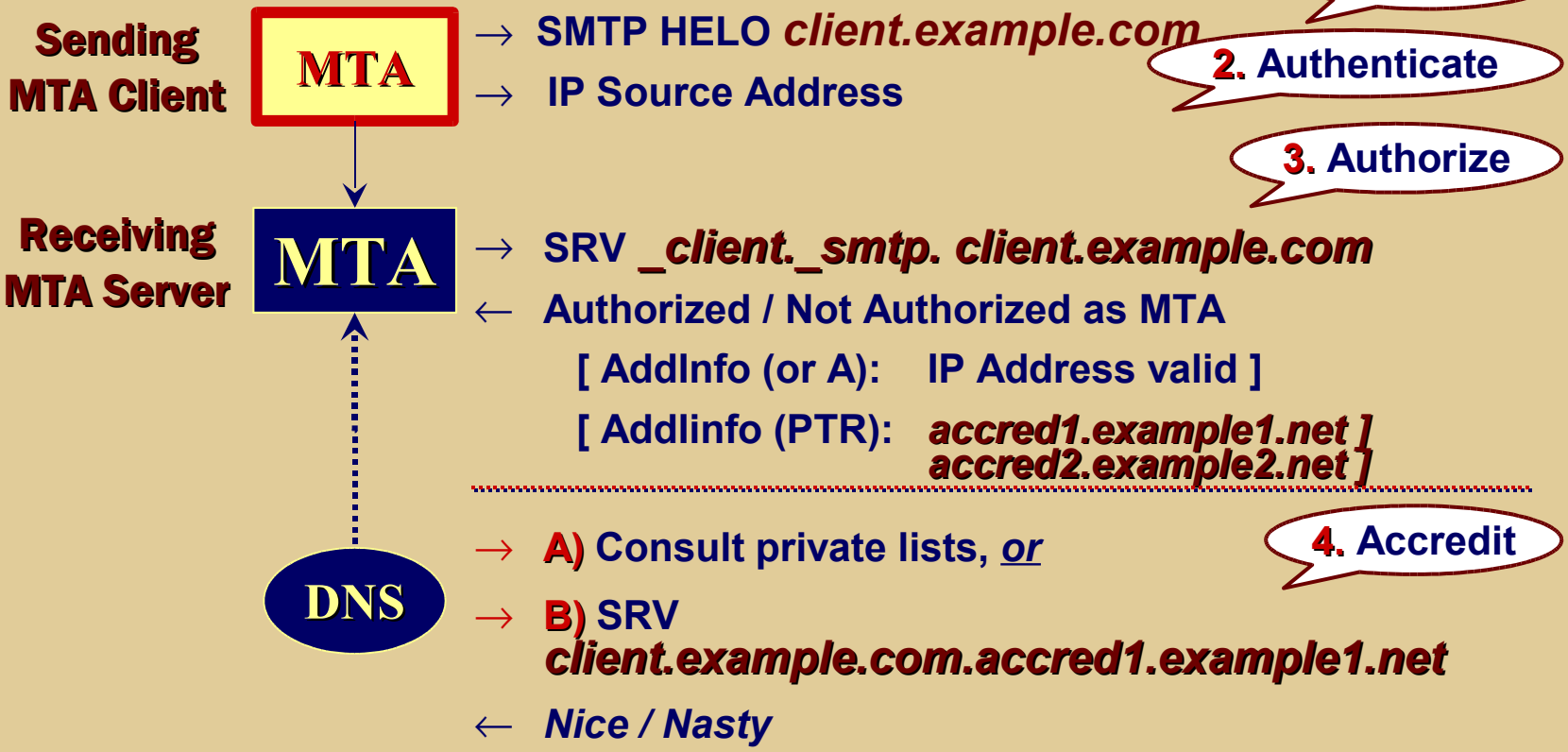
Certified Server Validation (CSV):
Assess Peer MTA Operation



1. Does a Domain Name Manager *authorize* this client MTA to be sending email?

2. Does an independent *accreditation* service consider domain manager's practices to be adequate, for controlling email abuse?

CSV Process


Sending MTA Client
MTA
Receiving MTA Server
MTA
DNS
→ SMTP HELO client.example.com
→ IP Source Address
1. Identify
2. Authenticate
3. Authorize
→ SRV _client._smtp. client.example.com
← Authorized / Not Authorized as MTA
[AddInfo (or A): IP Address valid]
[Addlinfo (PTR): accred1.example1.net]
accred2.example2.net]
4. Accredit
→ A) Consult private lists, or
→ B) SRV client.example.com.accred1.example1.net
← Nice / Nasty

CSV Usage

- **Sending MTA Network Operator**
  - **Register** authorized MTAs in CSV SRV DNS
  - [**Register** "explicit" record, for default *"not authorized"*]
- **Sending MTA Client**
  - **Use** EHLO authorized domain name
- **Receiving MTA Server**
  - **Query** CSA SRV for Client domain name
  - [**Query** CSA SRV for Client domain name 'explicit' record]
  - **Query** private table or public DNA PTR record

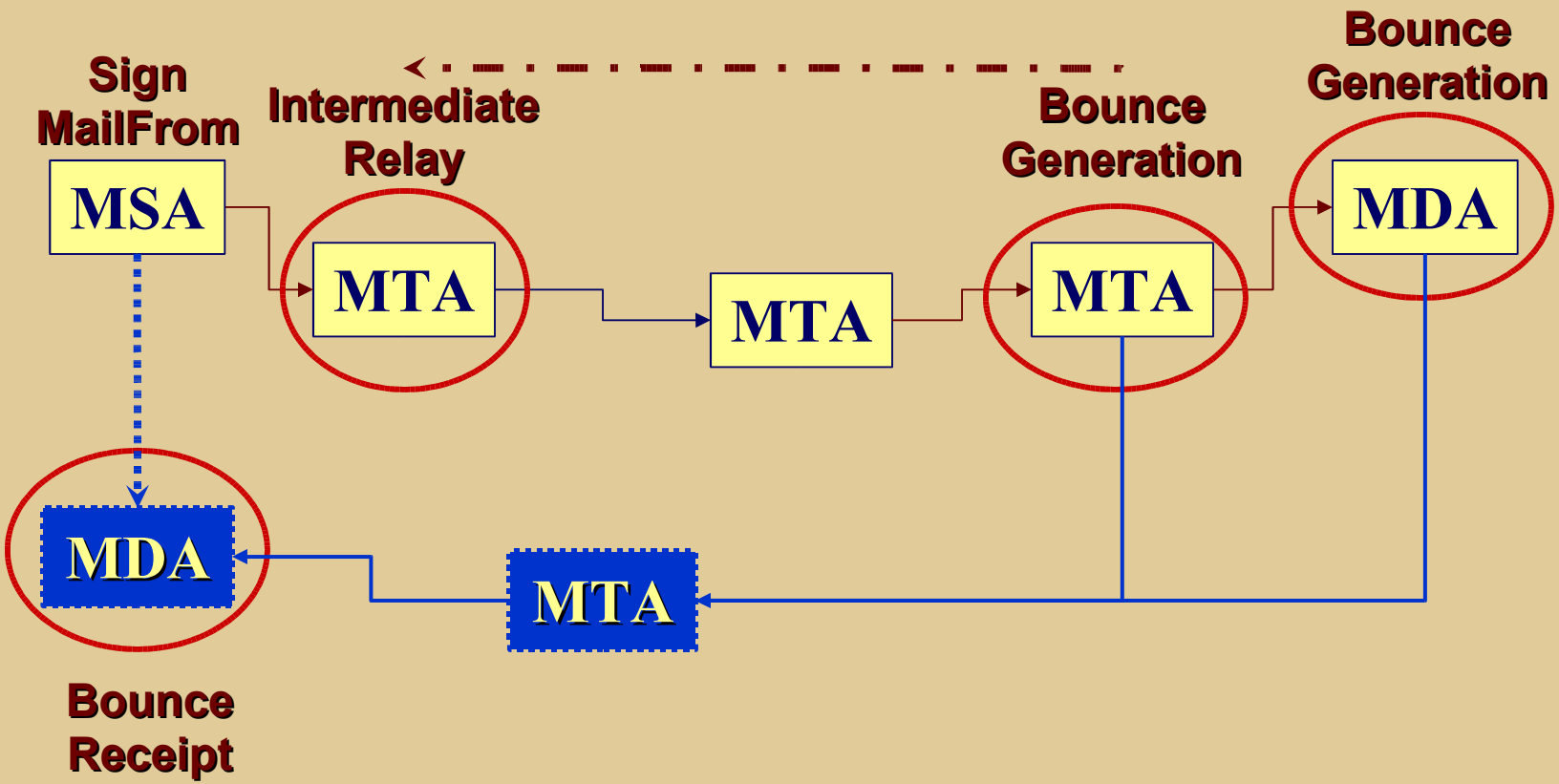
Bounce Address Tag Validation (BATV):

Detecting Forged 2821.MailFrom

- **Digital signature** of bounce address
  - Key is based on domain portion of address
- **Multiple schemes** permitted
  - First one is simple and private to the originating system
- **Meta-syntax** on LHS (local-part) for parameters
  - Permits finding mailbox without understanding signature, but entire string (with meta-syntax) must be used as bounce
  - Hard limit of 64 bytes for total of local-part

mailbox@example.com → **batv=mailbox/scheme/parameters@example.com**

Bounce Address Evaluation Venues



First Scheme: *PSB0*

- **Private Signed Bounce, version zero**
  - Detect invalid received bounces
  - Interpreted *only* by issuer
  - Limited replay protection

sig-val = key-id,
encrypt (bounce address,
timestamp,
random-string)

Approach for "Public Key" Schemes

- **Allows interpretation by Relays earlier in the sequence**
  - Requires PK infrastructure
  - Will be based on a content-signing standard, *when available*
  - Link to content permits strong replay protection
- **Tune computation to MailFrom's limitations**
  - E.g., hash the signature into a short string.

To Follow Up…

- **CSV and BATV**
  - Mailing list and specifications: **mipassoc.org/clear**
  - Certified Server Validation (CSV): draft-ietf-marid-csv-intro-02
    - Client SMTP Authorization (CSA): draft-ietf-marid-csv-csa-02
    - Domain Name Accreditation (DNA): draft-ietf-marid-csv-dna-02
  - Bounce Address Tag Validation (BATV): draft-levine-mass-batv-00
- **Email architecture**
  - **bbiw.net/specifications/draft-crocker-email-arch-03.html**
  - Internet Mail Architecture: draft-crocker-email-arch-03