Figures 1-3
Existing Protocols
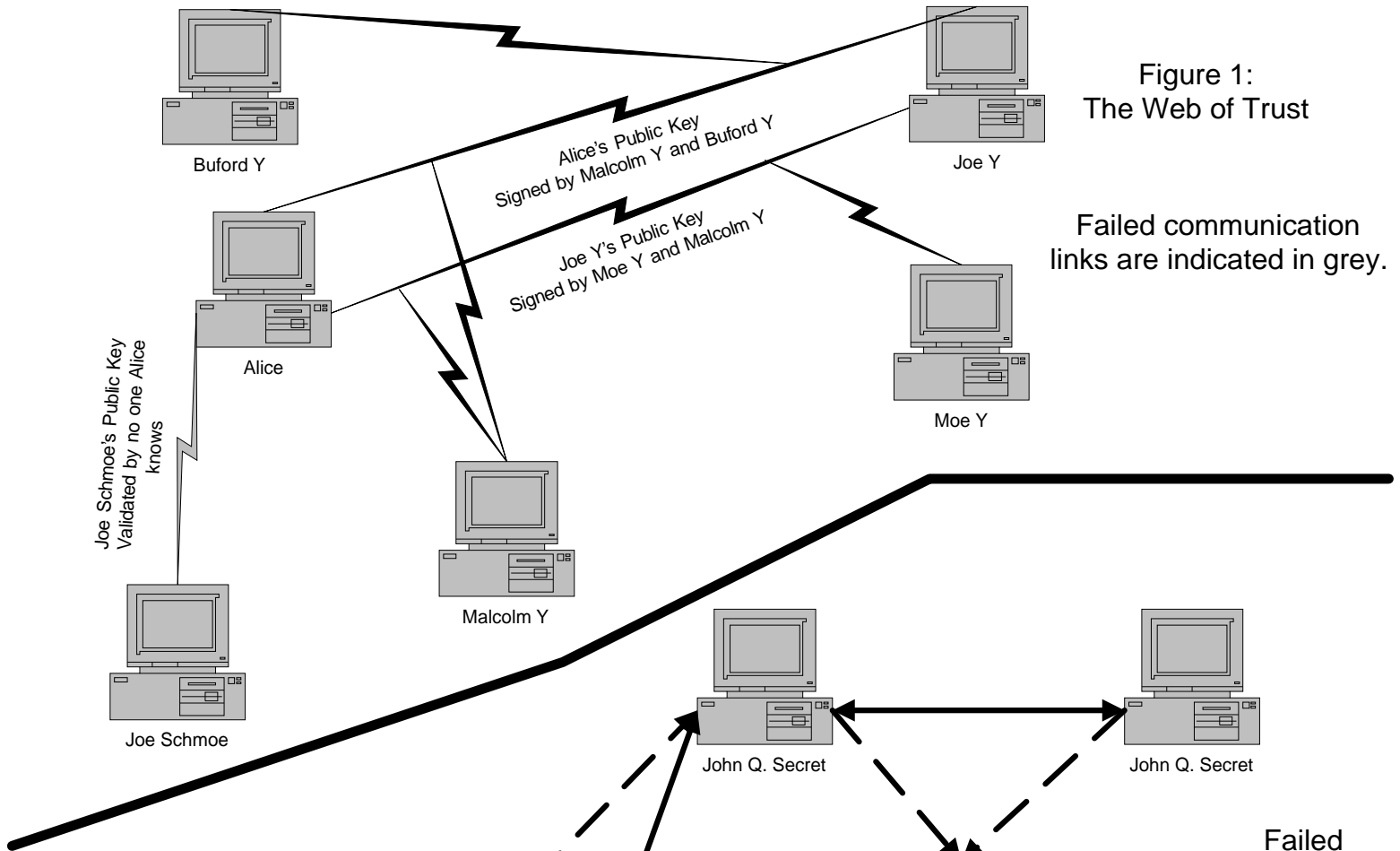
Figure 1:
The Web of Trust

Failed communication
links are indicated in grey.

Buford Y

Joe Y

Alice's Public Key
Signed by Malcolm Y and Buford Y

Joe Y's Public Key
Signed by Moe Y and Malcolm Y

Alice

Moe Y

Joe Schmoe's Public Key
Validated by no one Alice
knows

Malcolm Y

Joe Schmoe

Figure 2:
The Strict Hierarchy Model

John Q. Secret

John Q. Secret

John Q. Top Secret

John Q. Classified

Failed
communication
links are
indicated as
dashed lines
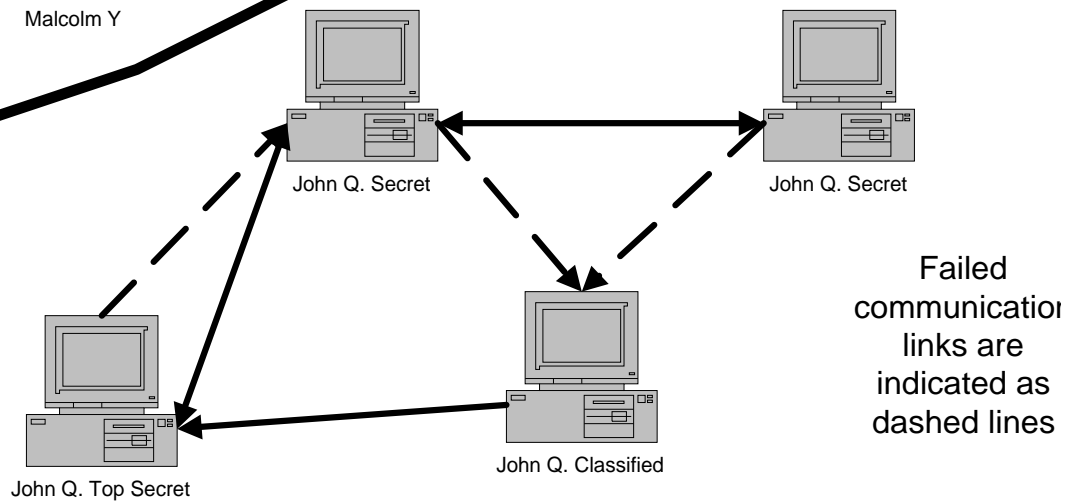
Figure 3:
The Escrowed Encryption
Standard

John Q. N. S. A.

John Q. Metzger

Jean-Paul Q. French

John Q. Regular

Failed
communication
links are
indicated as
dashed lines

John Q. Business Partner

Ioannis Q. Ioannidis
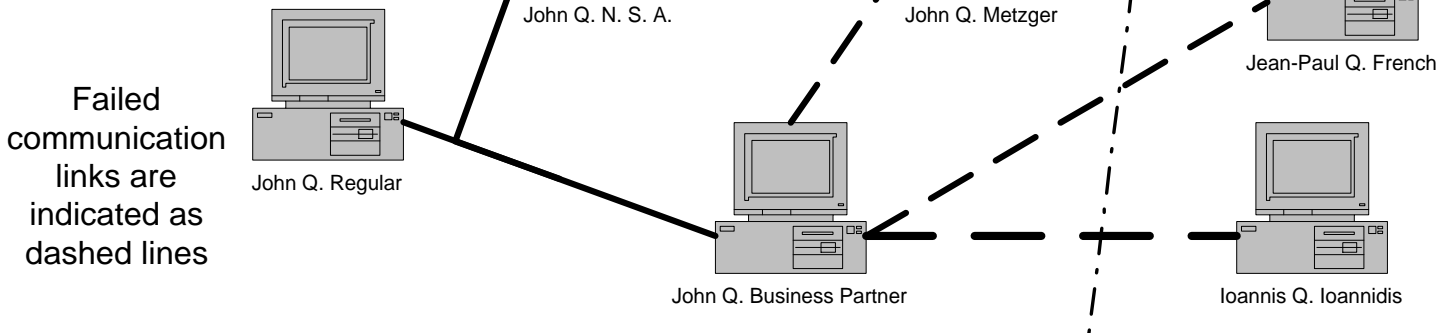
Figure 4
The Web of Hierarchies

8

Eventual Communication

Bob

Alice

1

Request for information regarding Alice

Private-key encrypted communications are indicated in grey; public-key communications in black.

Request for Alice's public key

7

trustmaster@dept.bob.com

2

Request for information regarding Alice

3

Request for the public key of trustmaster@alice.com

NIC

4

Request for the public key of trustmaster@alice.com

Request for information regarding Alice

6

trustmaster@dept.alice.com

5

Request for information regarding Alice

trustmaster@bob.com

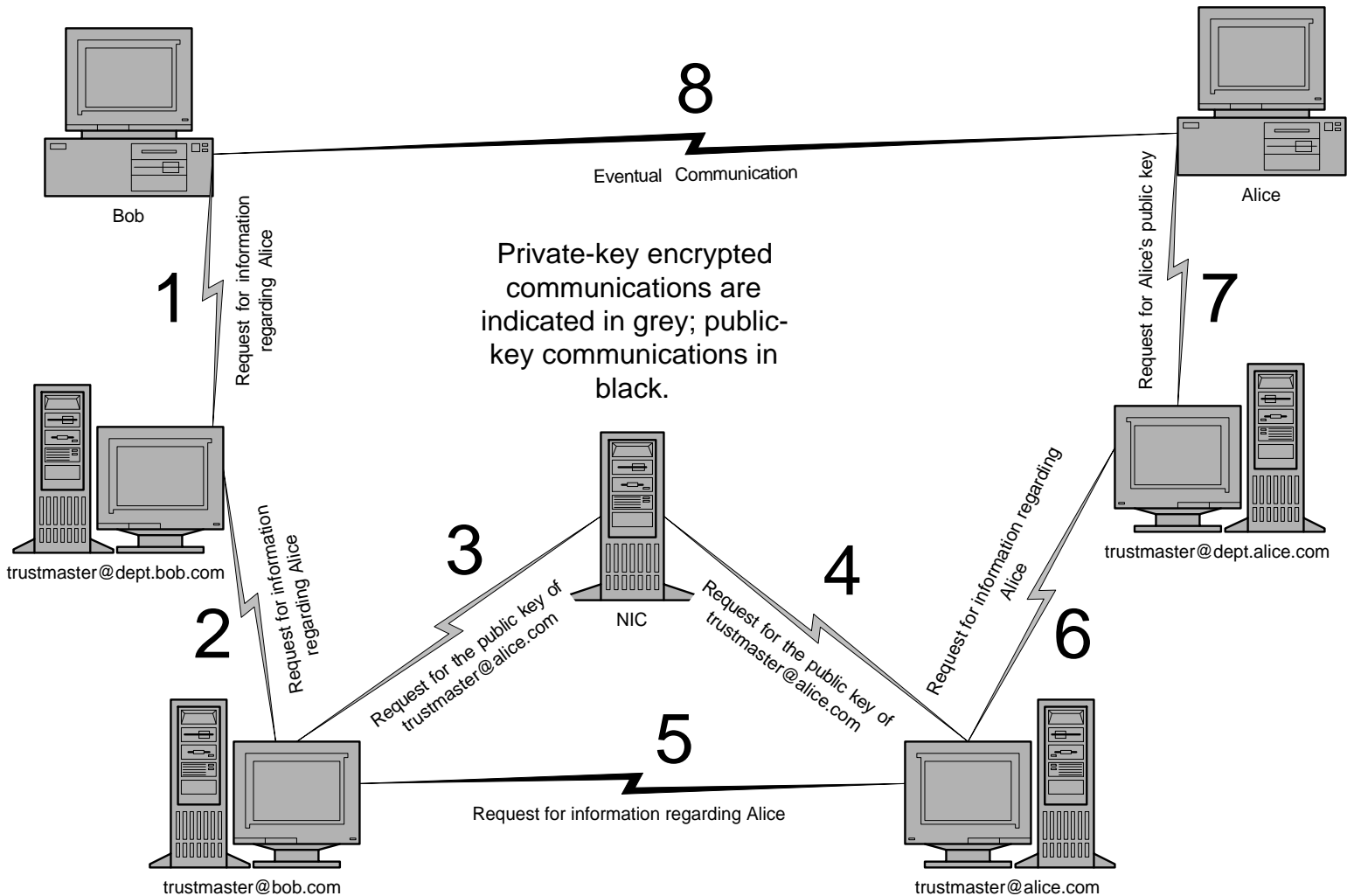trustmaster@alice.com

Order of operations:
1. Bob mails trustmaster@dept.bob.com for info about Alice.
2. trustmaster@dept.bob.com mails trustmaster@bob.com for info about Alice.
3. trustmaster@bob.com checks to see if it has the up-to-date public key for trustmaster@alice.com. If so, skip to step 5. If not, mails the NIC database for the public key.
4. NIC checks to see if it has an up-to-date public key for trustmaster@alice.com. If so, it returns it to trustmaster@bob.com. If not, it returns an error to trustmaster@bob.com.
5. If trustmaster@bob.com can get a valid public key. it mails trustmaster@alice.com for information about Alice.
6. trustmaster@alice.com mails trustmaster@dept.alice.com for information about Alice, including her public key. If trustmaster@dept.alice.com has her public key, it sends it back, with a report of her status. Skip to step 8.
7. If not, it requests Alice's public key.
8. Bob, now armed with Alice's public key and a report on her trusted status, can now either mail Alice a message with her public key or abort.