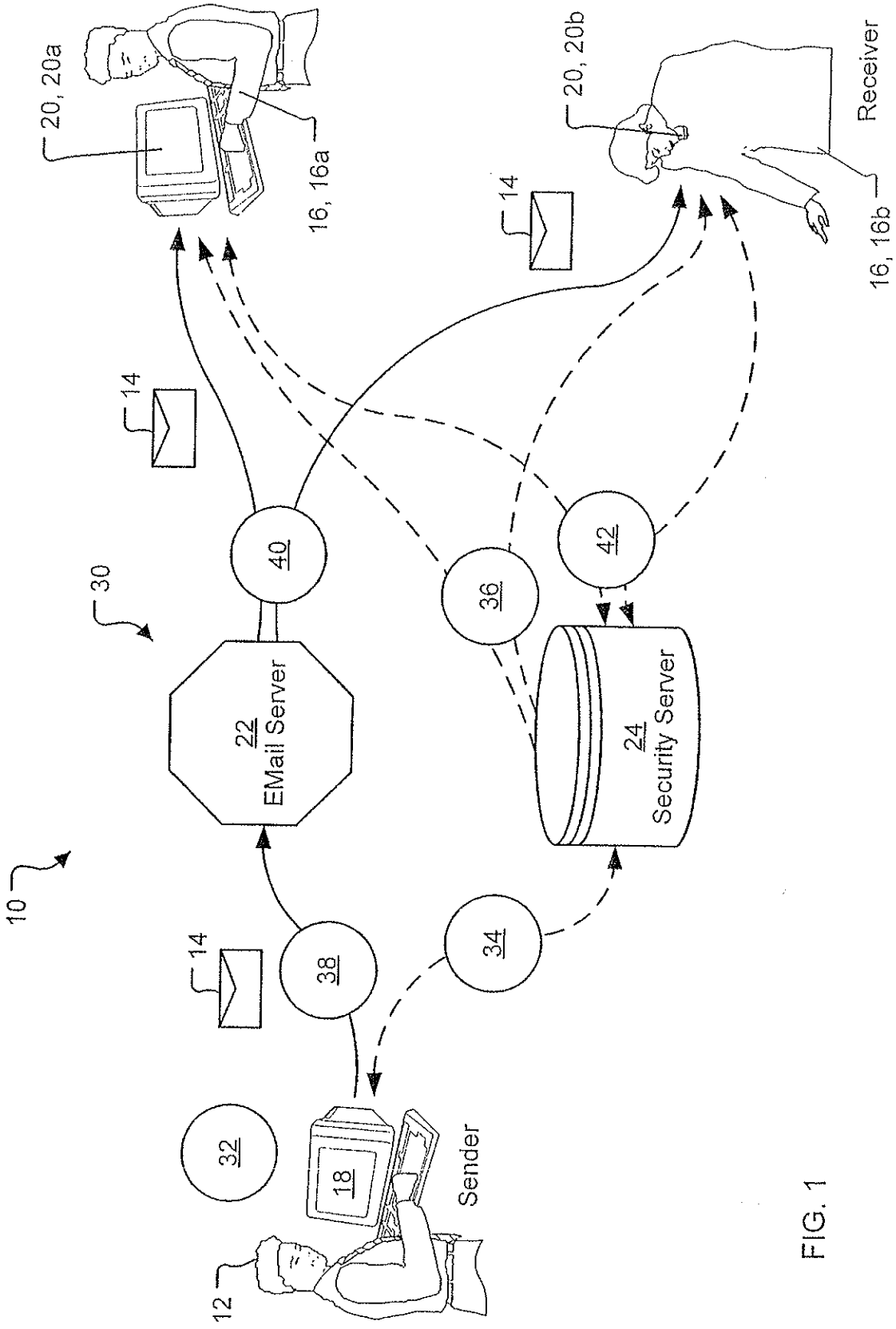

10
12
Sender
18
32
34
36
38
40
42
14
14
14
22
EMail Server
24
Security Server
30
20, 20a
16, 16a
20, 20b
16, 16b
Receiver

FIG. 1

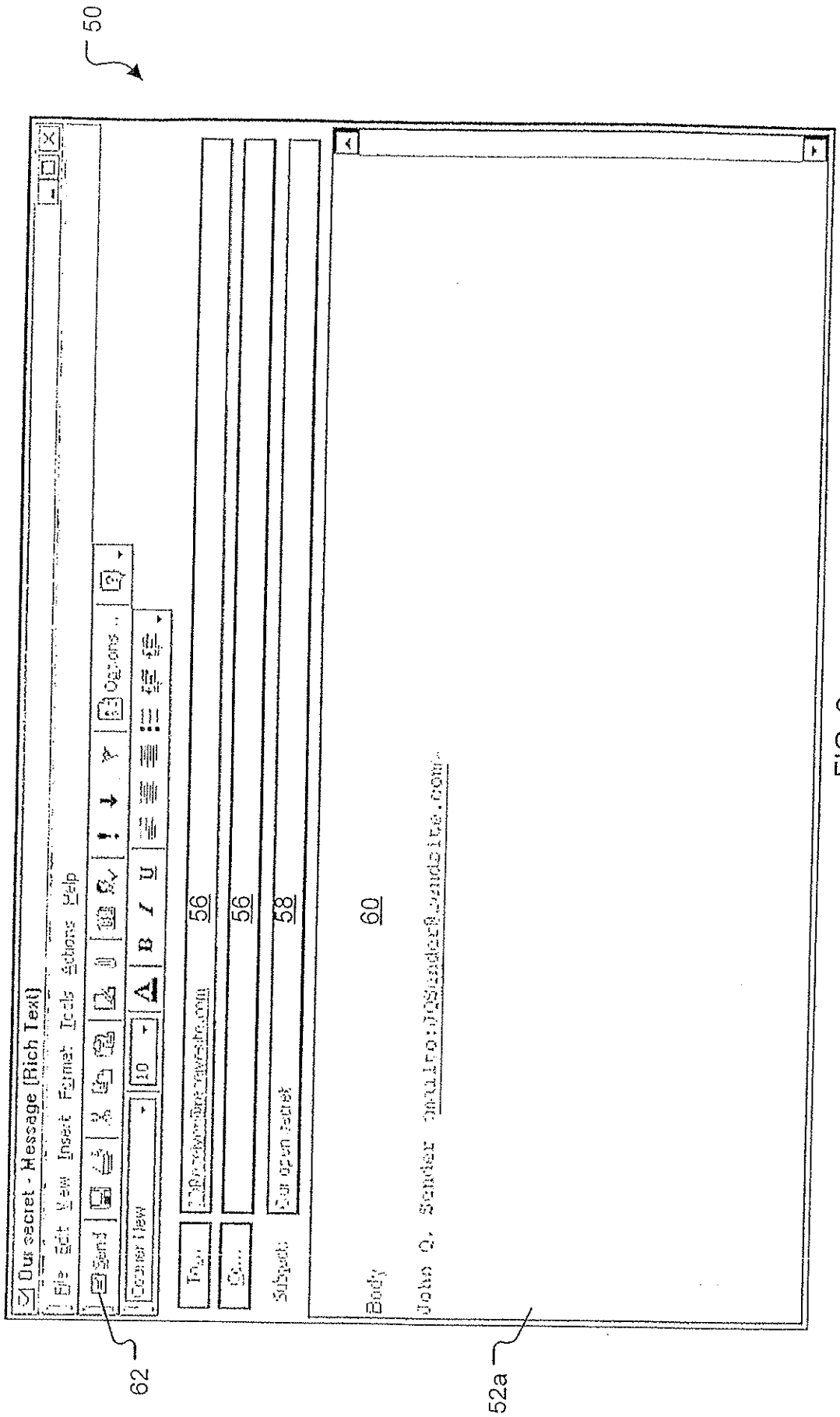

50
Our secret - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Send
Options...
To...
Cc...
Subject:
56
56
58
60
Body
62
52a

FIG. 2a

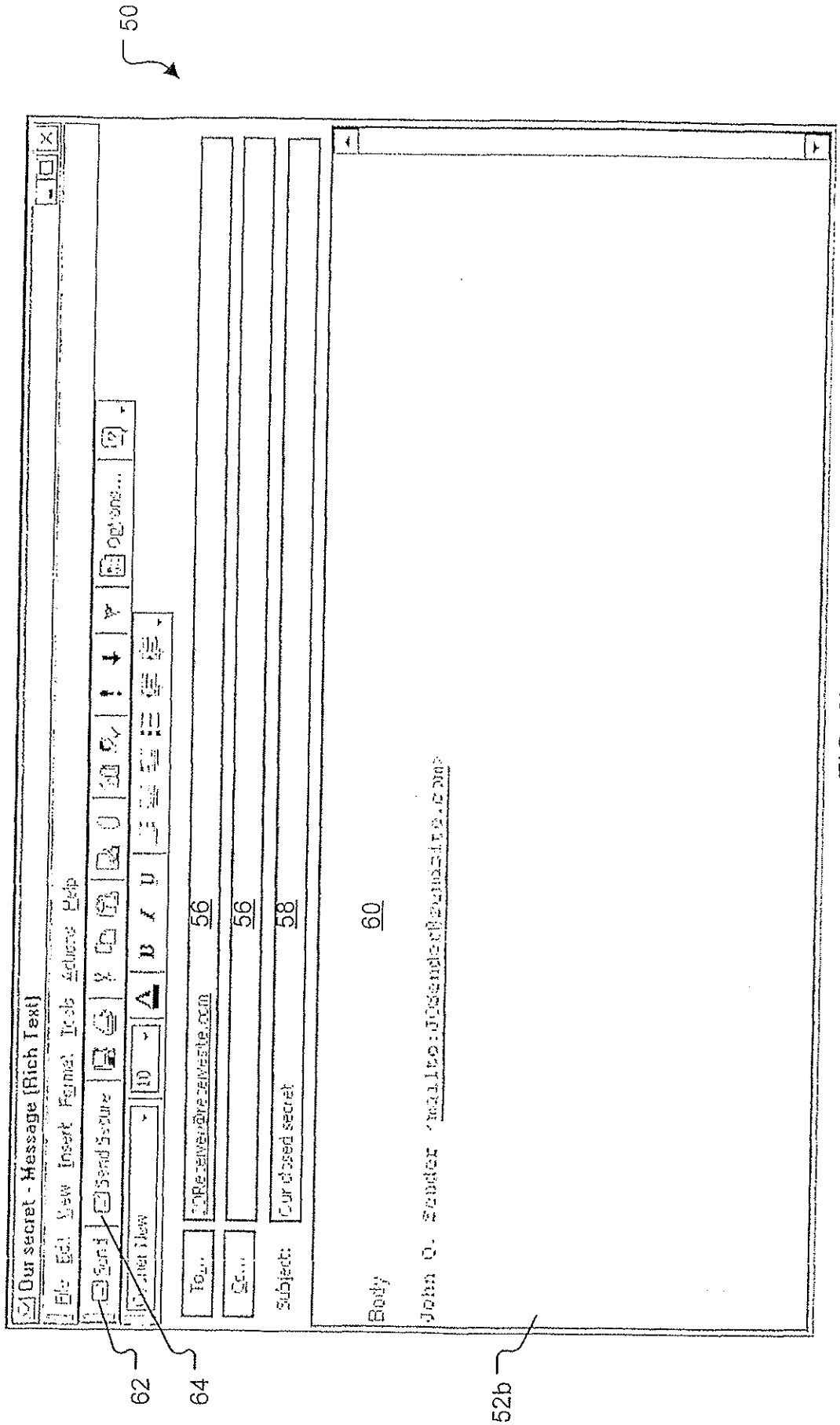

50
Our secret - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Send
Send Secure
Options...
To...
Cc...
Subject:
Our closed secret
56
56
58
60
Body
John D. Sender
62
64
52b

FIG. 2b

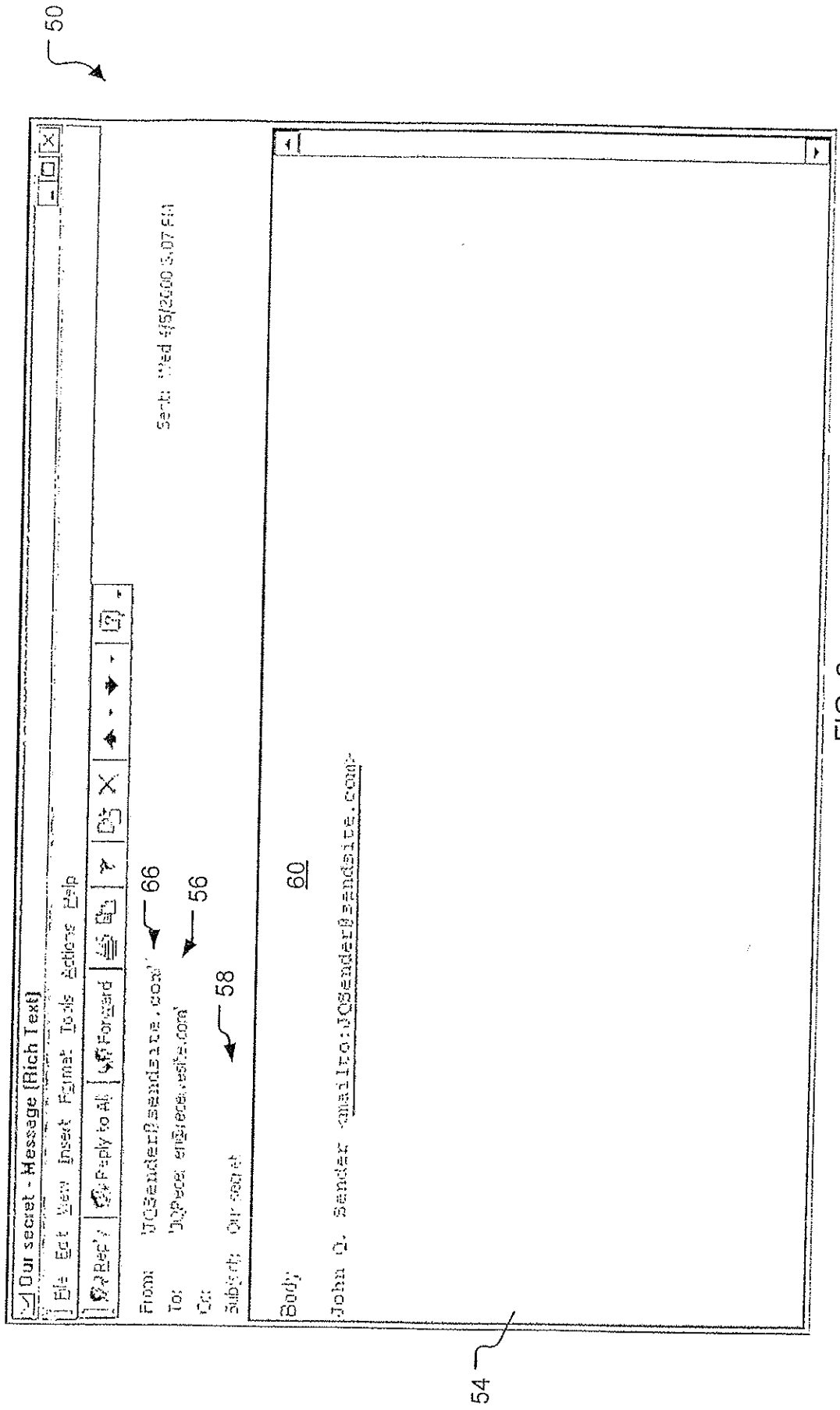

50
Our secret - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
From: 'JQSender@senderdomain.com'
To: 'JQPeer@peerdomain.com'
Cc:
Subject: Our secret
Sent: Wed 4/5/2000 3:07 PM
66
56
58
Body
60
John Q. Sender <mailto:JQSender@senderdomain.com>
54

FIG. 2c

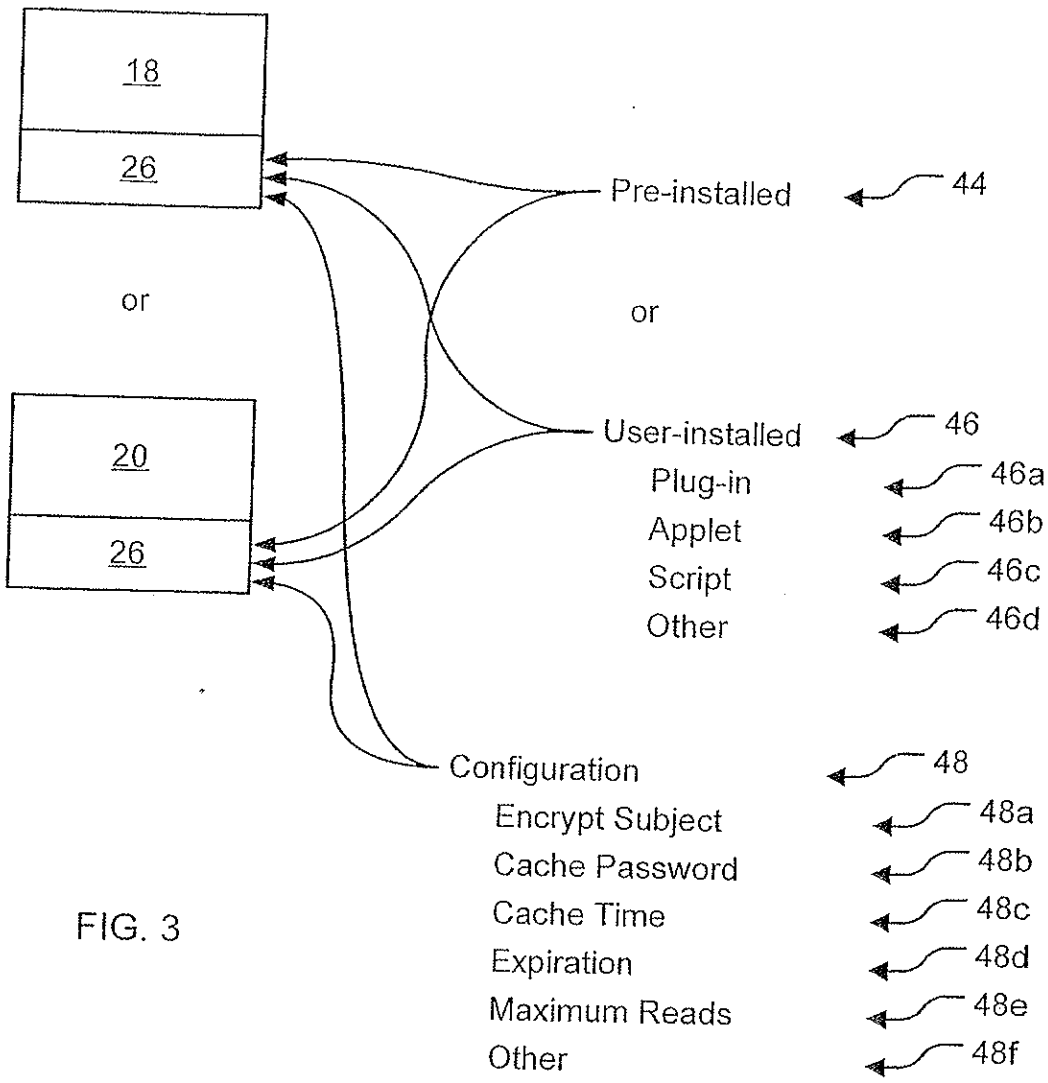

18
26
or
20
26
Pre-installed
44
or
User-installed
46
Plug-in
46a
Applet
46b
Script
46c
Other
46d
Configuration
48
Encrypt Subject
48a
Cache Password
48b
Cache Time
48c
Expiration
48d
Maximum Reads
48e
Other
48f

FIG. 3

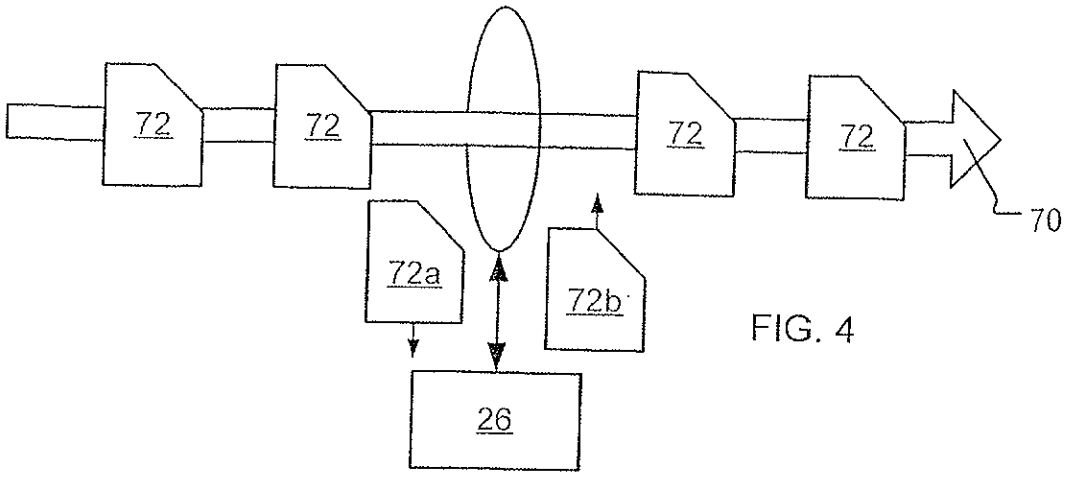


FIG. 4

FIG. 7

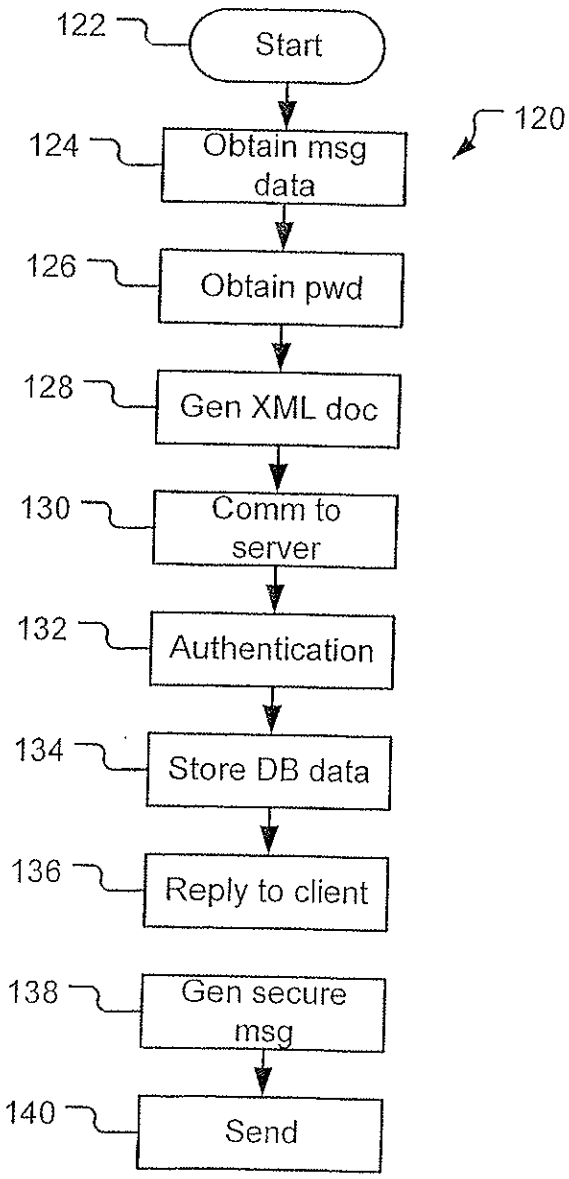
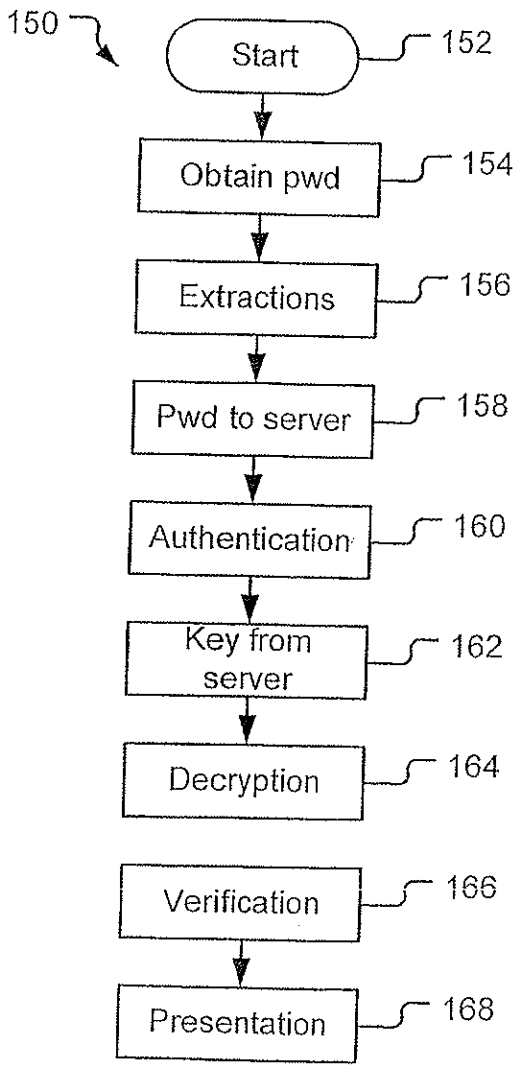


FIG. 8



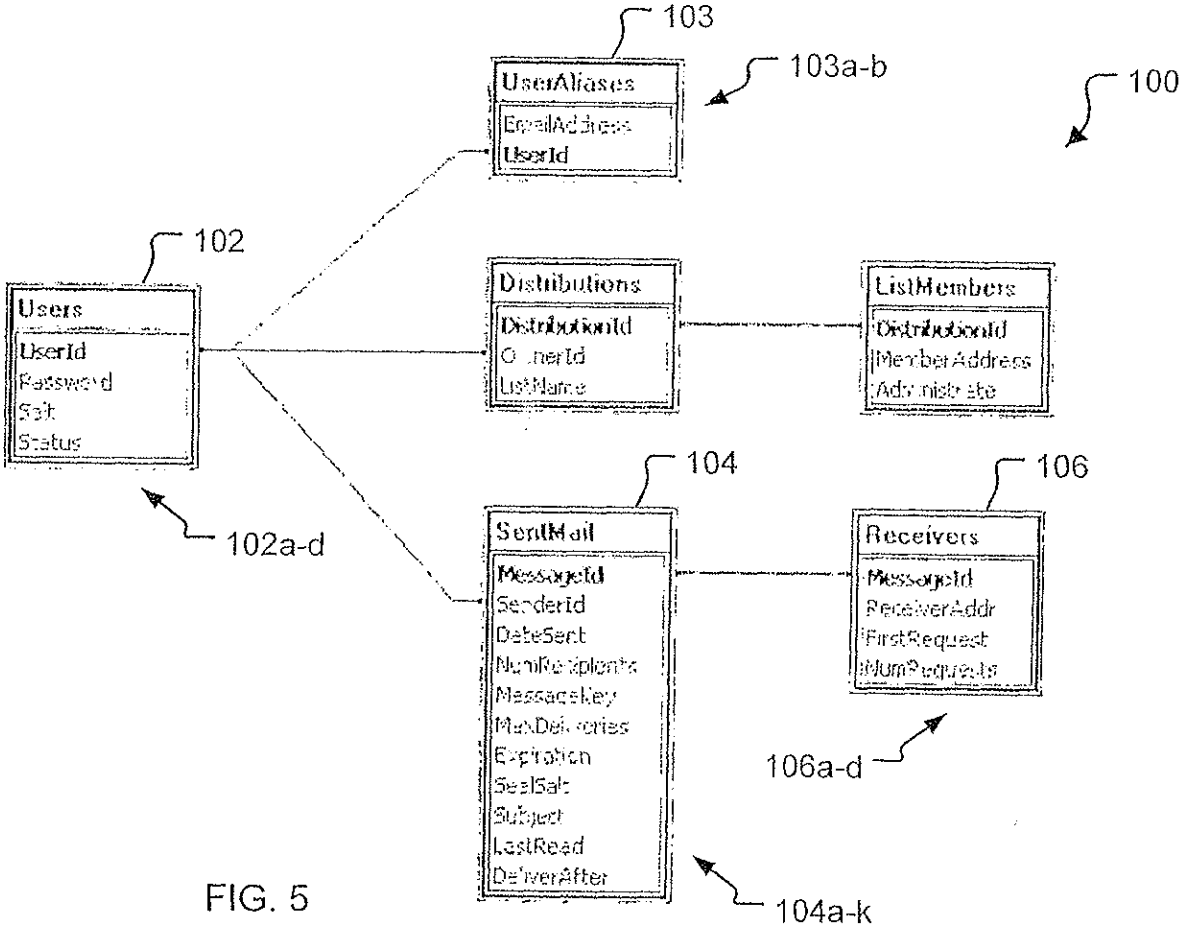

103
103a-b
100
UserAliases
EmailAddress
UserId
102
Users
UserId
Password
Salt
Status
Distributions
DistributionId
OwnerId
ListName
ListMembers
DistributionId
MemberAddress
Administrate
102a-d
104
106
SentMail
MessageId
SenderId
DateSent
NumRecipients
MessageKey
MaxDeliveries
Expiration
SealSalt
Subject
LastRead
DeliverAfter
Receivers
MessageId
ReceiverAddr
FirstRequest
NumRequests
106a-d
104a-k

FIG. 5

FIG. 6a: Basic user information table (Users)

Column Name	Type	Description
UserId	integer	Internal user identifier
Password	raw	Hash of user's password
Salt	integer	Salt added to password before hash
Status	varchar	User's current registration/usage status

FIG. 6b: Sent messages table (SentMail)

Column Name	Type	Description
MessageId	integer	Unique email identifier
SenderId	integer	Internal sender identifier (ref to Users)
DateSent	date	Time and date record entered
NumRecipients	integer	Number of users message was sent to
MessageKey	raw	Key used to encrypt/decrypt message
MaxDeliveries	integer	Maximum times key is delivered to each user
Expiration	date	Time after which message should not be delivered
SealSalt	integer	Secret salt added to hash to form seal
Subject	varchar	The subject of the message
LastRead	date	The date the message was last read
DeliverAfter	date	The date after which the message may be read

FIG. 6c: Email destinations (Receivers)

Column Name	Type	Description
MessageId	integer	Email message's identifier (ref to SentMail)
ReceiverAddr	integer	Receiver's e-mail address
FirstRequest	date	Time the receiver first attempts to read
NumRequests	integer	Number of times receiver requested to read

FIG. 6d: Alternate user identities (UserAliases)

Column Name	Type	Description
EmailAddress	varchar	Alternate email address
UserId	integer	Reference to Users table.

FIG. 6e: Distribution list master (Distributions)

Column Name	Type	Description
DistributionId	integer	Unique list identifier
OwnerId	integer	User who owns list (ref to Users).
ListName	varchar	Email address of this list

FIG. 6f: Distribution list members (ListMembers)

Column Name	Type	Description
DistributionId	integer	Reference to Distributions
MemberAddress	varchar	Name of alias on the list
Administrate	char	Y=member can update list, N=cannot

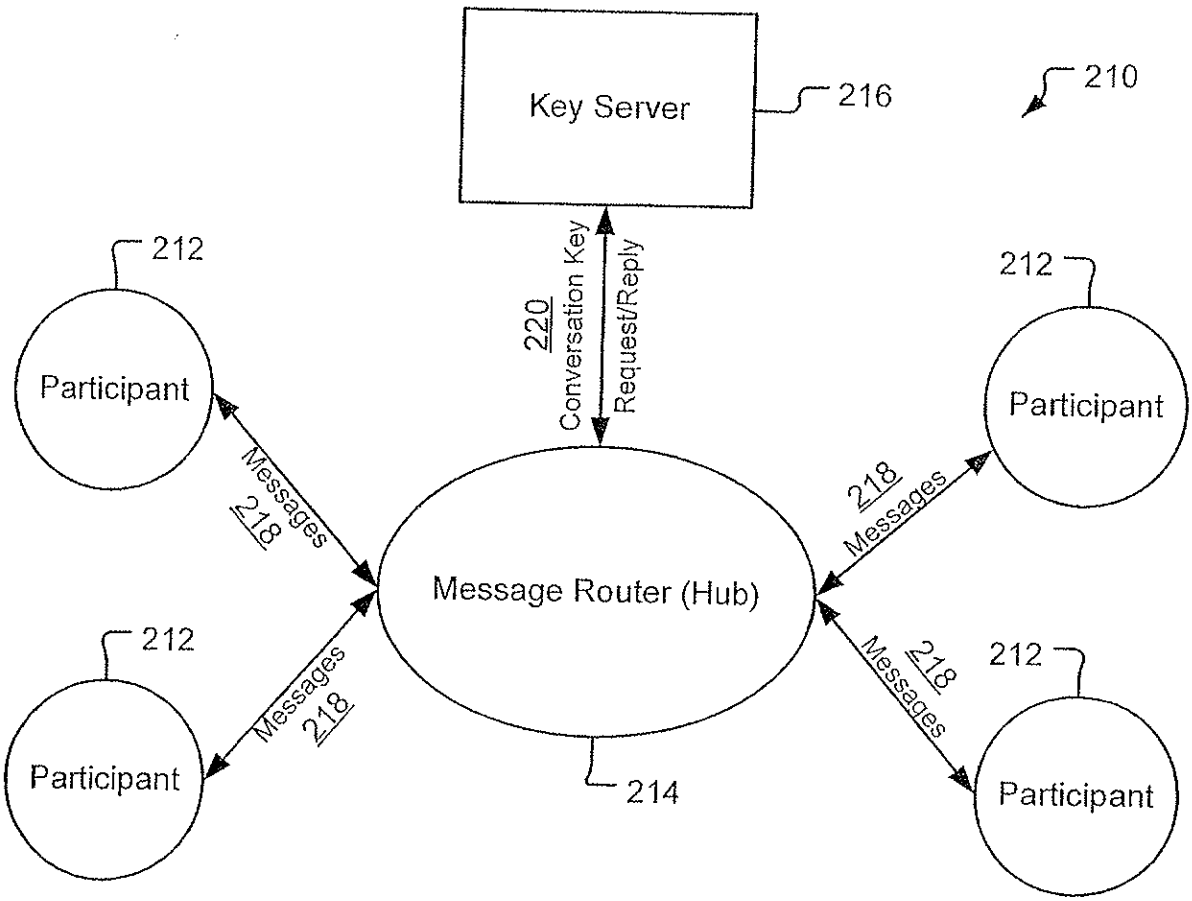

Key Server
216
210
212
Participant
220
Conversation Key
Request/Reply
212
Participant
Messages
218
Message Router (Hub)
218
Messages
212
Participant
Messages
218
218
Messages
212
Participant
214

FIG. 9

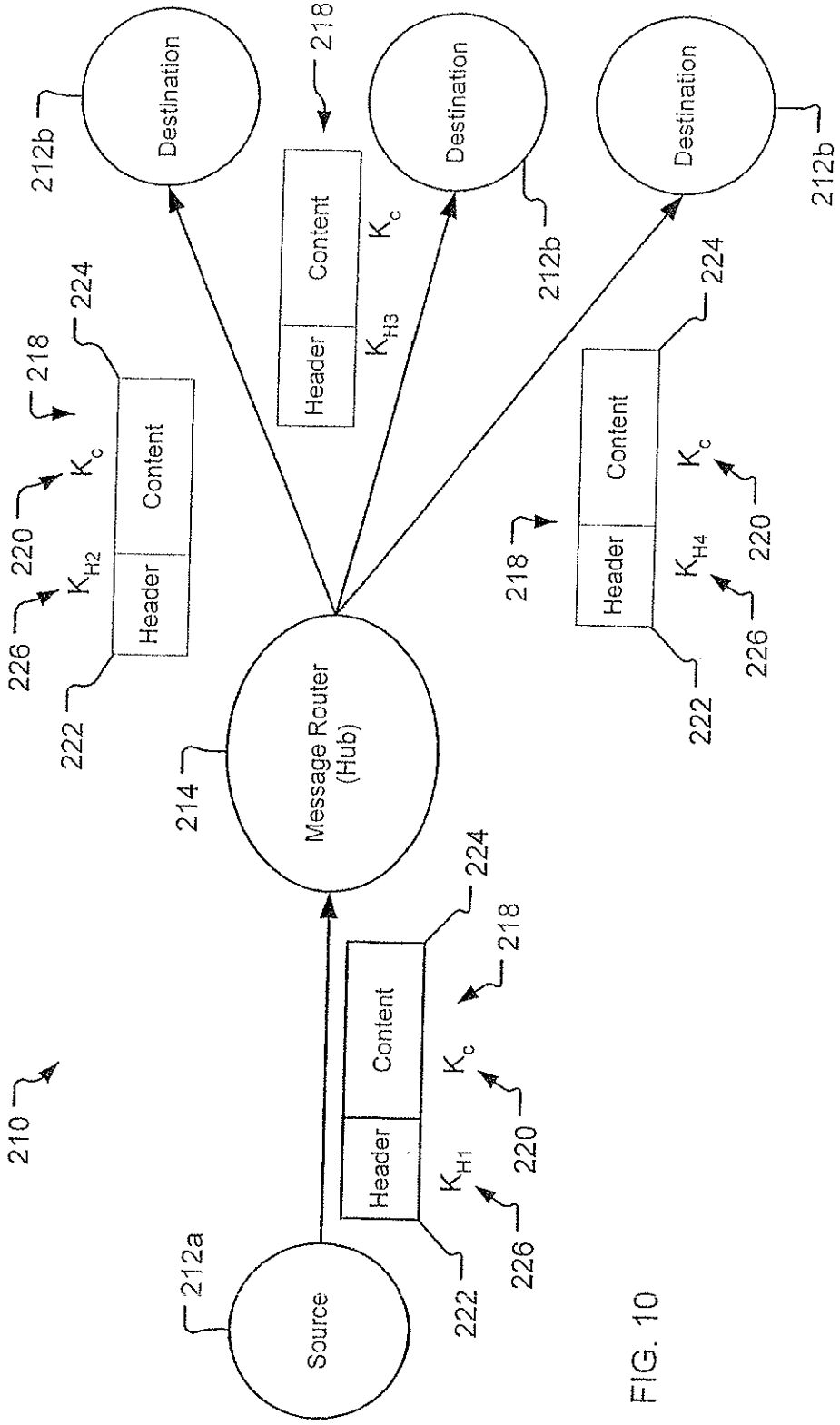

210
212a
Source
214
Message Router (Hub)
212b
Destination
212b
Destination
212b
Destination
218
224
Header
Content
K_{H1}
K_c
220
222
226
218
224
Header
Content
K_{H2}
K_c
220
222
226
218
224
Header
Content
K_{H3}
K_c
218
224
Header
Content
K_{H4}
K_c
220
222
226

FIG. 10

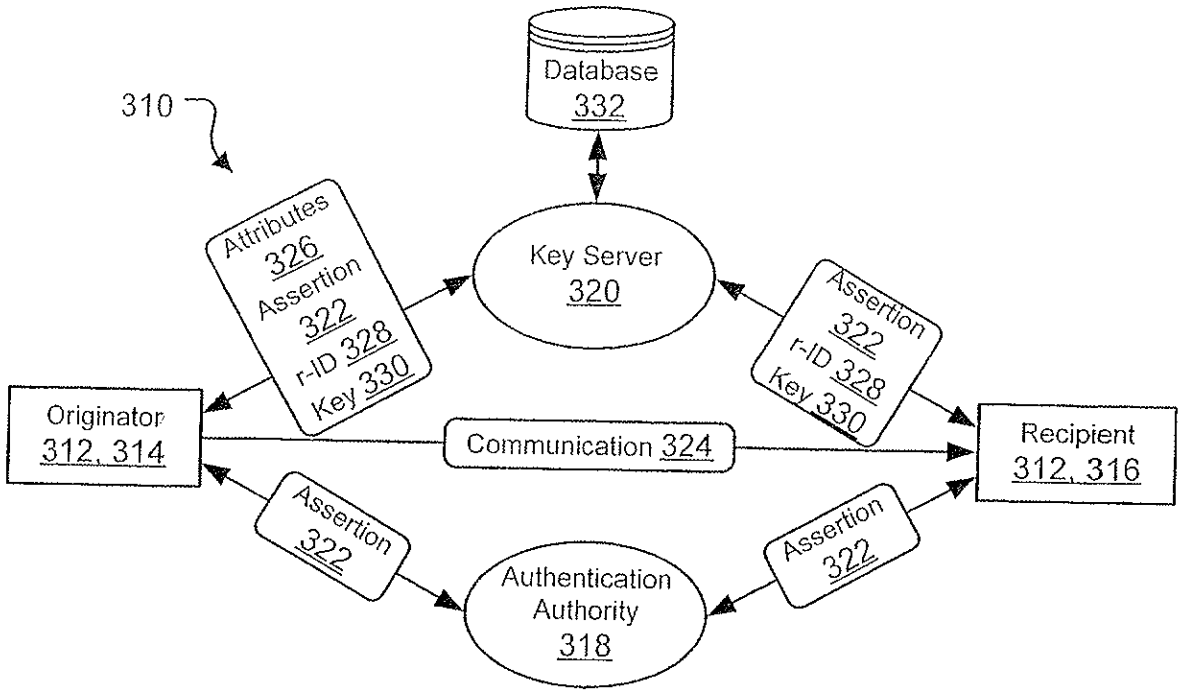

310
Database
332
Attributes
326
Assertion
322
r-ID 328
Key 330
Key Server
320
Assertion
322
r-ID 328
Key 330
Originator
312, 314
Communication 324
Recipient
312, 316
Assertion
322
Authentication
Authority
318
Assertion
322

FIG. 11

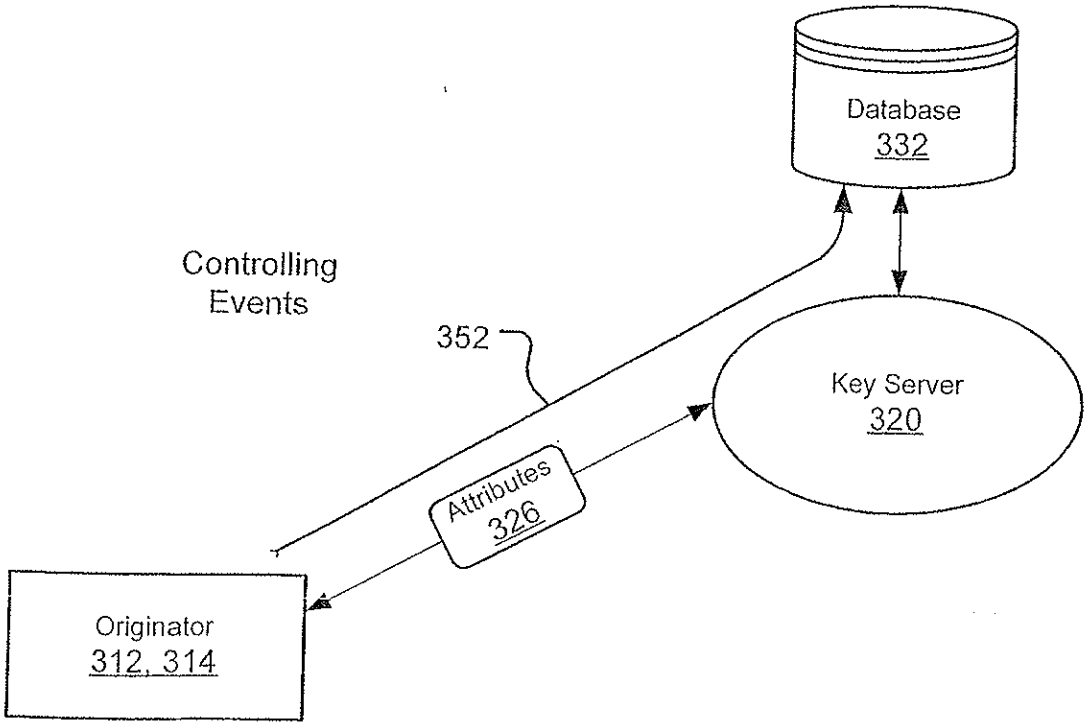

Database
332
Controlling
Events
352
Key Server
320
Attributes
326
Originator
312, 314

FIG. 12

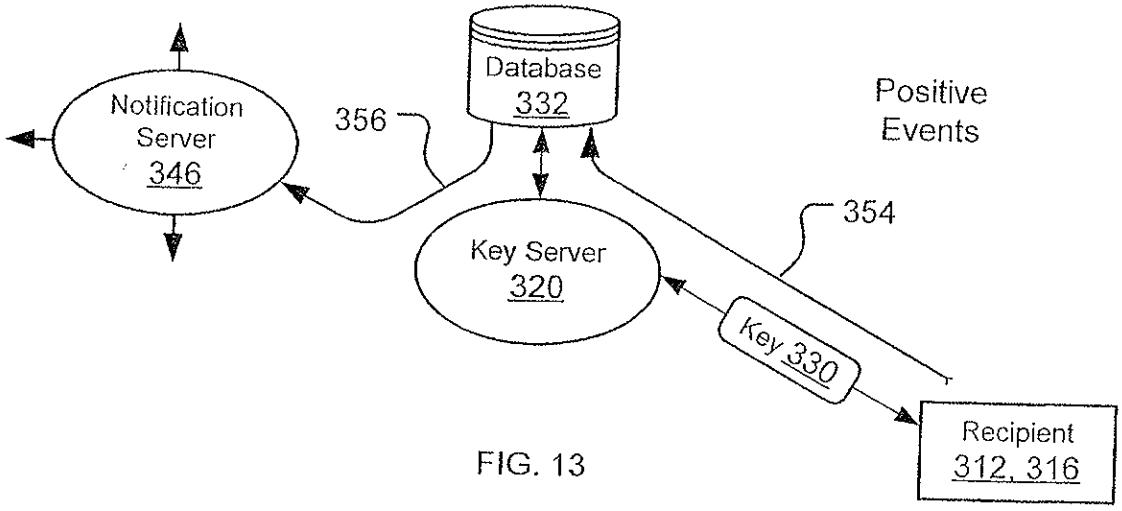

Database
332
Notification
Server
346
356
Positive
Events
354
Key Server
320
Key 330
Recipient
312, 316

FIG. 13

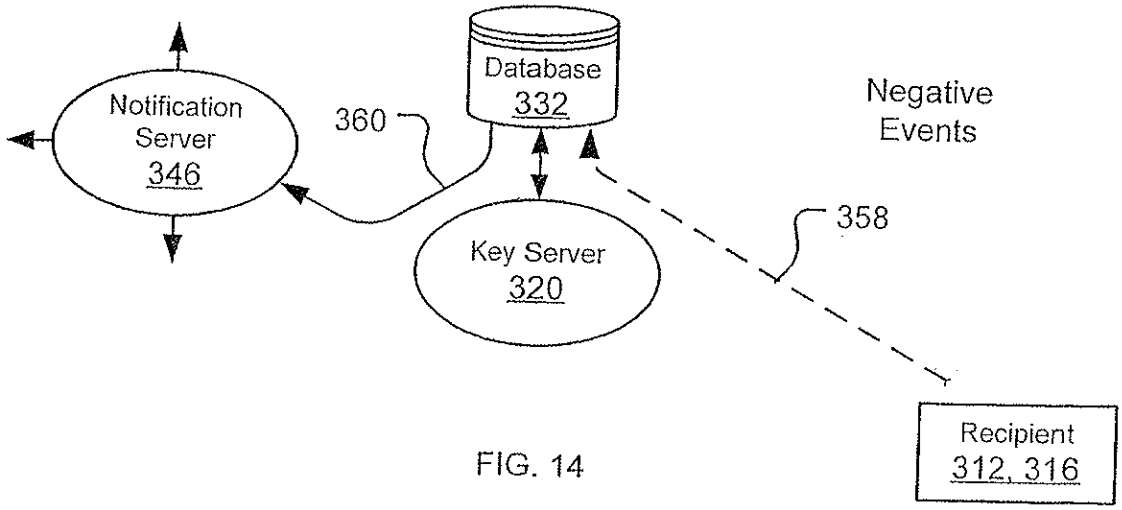

Database
332
Notification
Server
346
360
Negative
Events
358
Key Server
320
Recipient
312, 316

FIG. 14

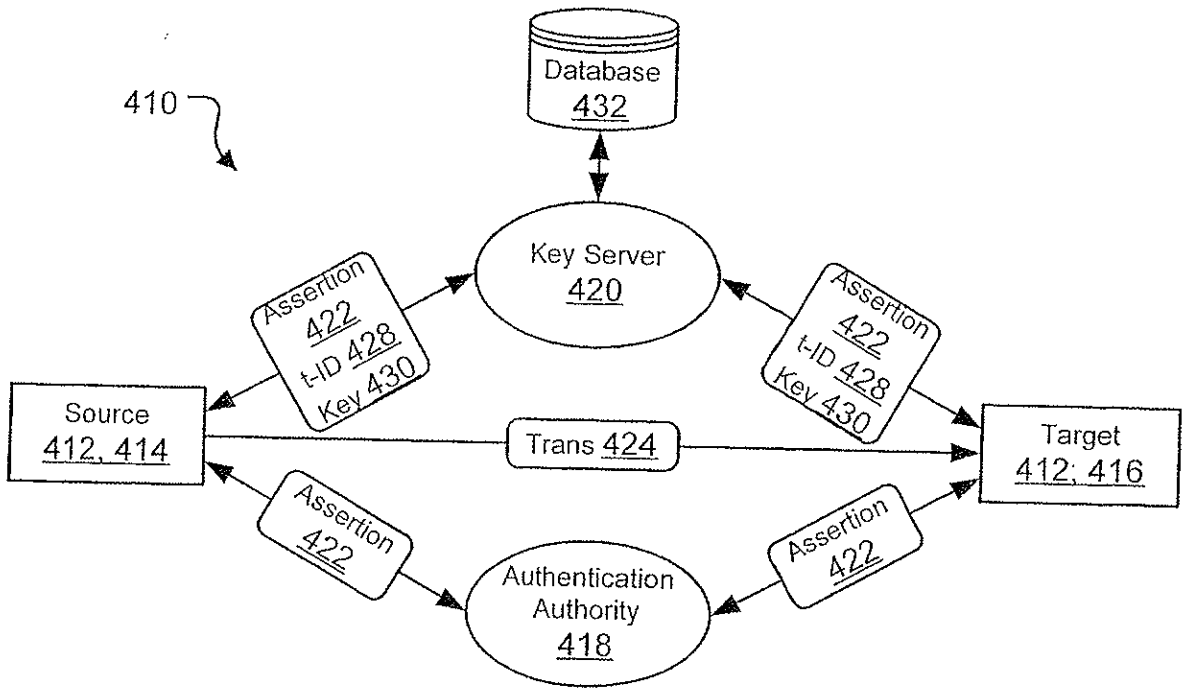

410
Database
432
Key Server
420
Assertion
422
t-ID 428
Key 430
Assertion
422
t-ID 428
Key 430
Source
412, 414
Trans 424
Target
412; 416
Assertion
422
Assertion
422
Authentication
Authority
418

FIG. 15

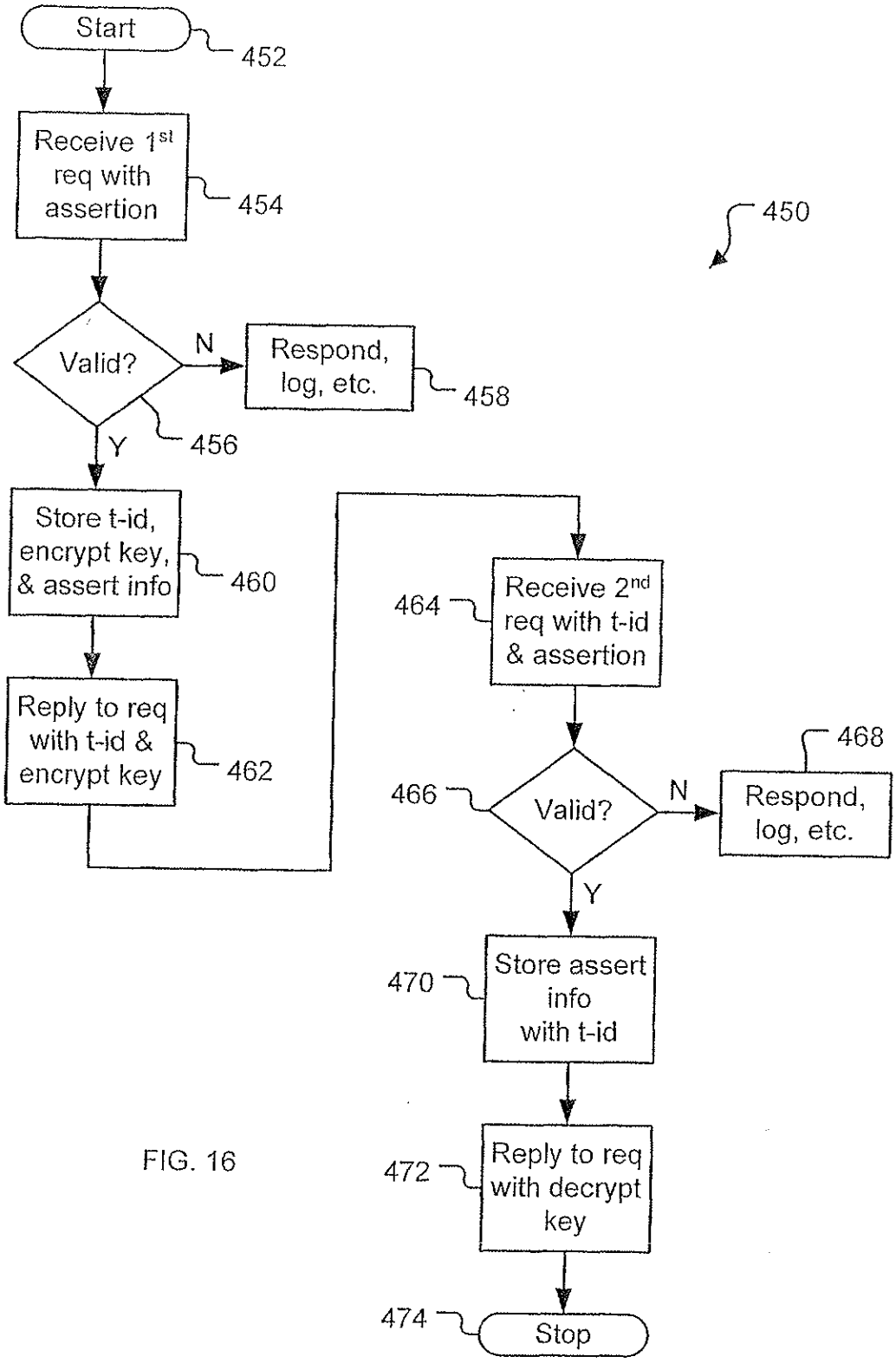

Start
452
Receive 1st req with assertion
454
450
Valid?
N
Respond, log, etc.
458
456
Y
Store t-id, encrypt key, & assert info
460
Reply to req with t-id & encrypt key
462
464
Receive 2nd req with t-id & assertion
466
Valid?
N
468
Respond, log, etc.
Y
470
Store assert info with t-id
472
Reply to req with decrypt key
474
Stop

FIG. 16

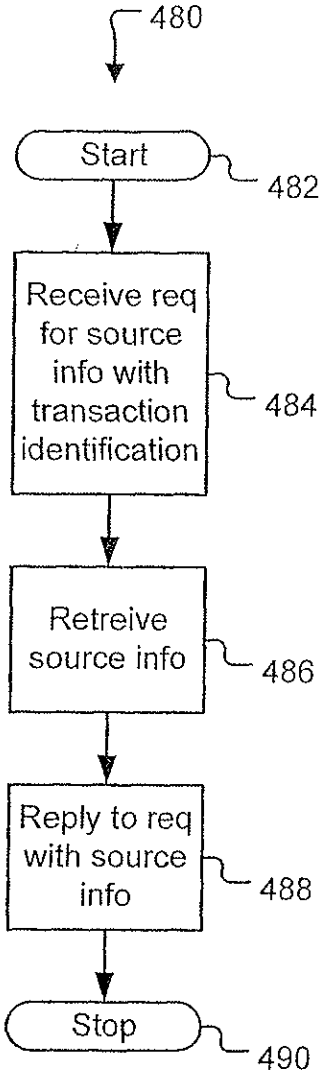

480
Start
482
Receive req for source info with transaction identification
484
Retreive source info
486
Reply to req with source info
488
Stop
490

FIG. 17

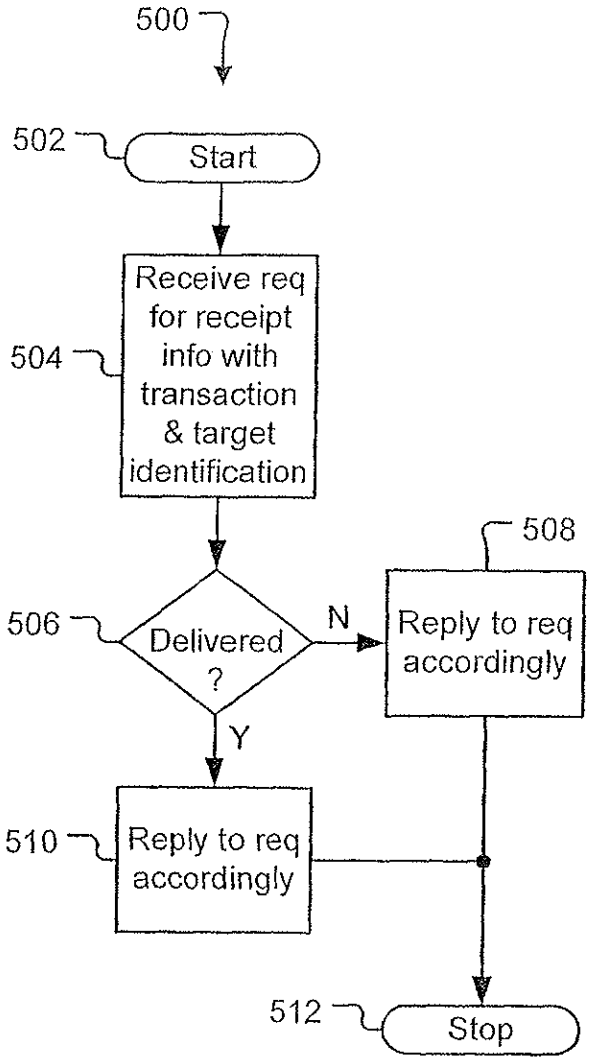

500
502
Start
Receive req for receipt info with transaction & target identification
504
506
Delivered ?
N
Y
508
Reply to req accordingly
510
Reply to req accordingly
512
Stop

FIG. 18

No	Field	Type	Description
1.	ResourceID	String	A unique ID assigned to this communication
2.	ResourceType	Integer	The application type (e.g., email, instant messaging, etc.)
3.	ResourceKey	Binary	The encryption key
4.	KeySize	Integer	The size of the key
5.	KeyCreator	String	The ID of the key creator
6.	KeyOwner	String	The ID of the key owner
7.	DateCreated	Date	The date and time when the key was created
8.	ReleaseAfter	Date	The date and time before which the key should not be released (per recipient)
9.	ExpireOn	Date	The date and time after which the key should not be released (per recipient)
10.	LastRelease	Date	The last date time the key was released (per recipient)
11.	ExpectedRequest	Date	The date and time by which the key is expected to be requested (per recipient)
12.	NumReleased	Integer	The number of times the key was released (per recipient)
13.	NumReleases	Integer	The number of times the key should be released (per recipient)

TABLE 1