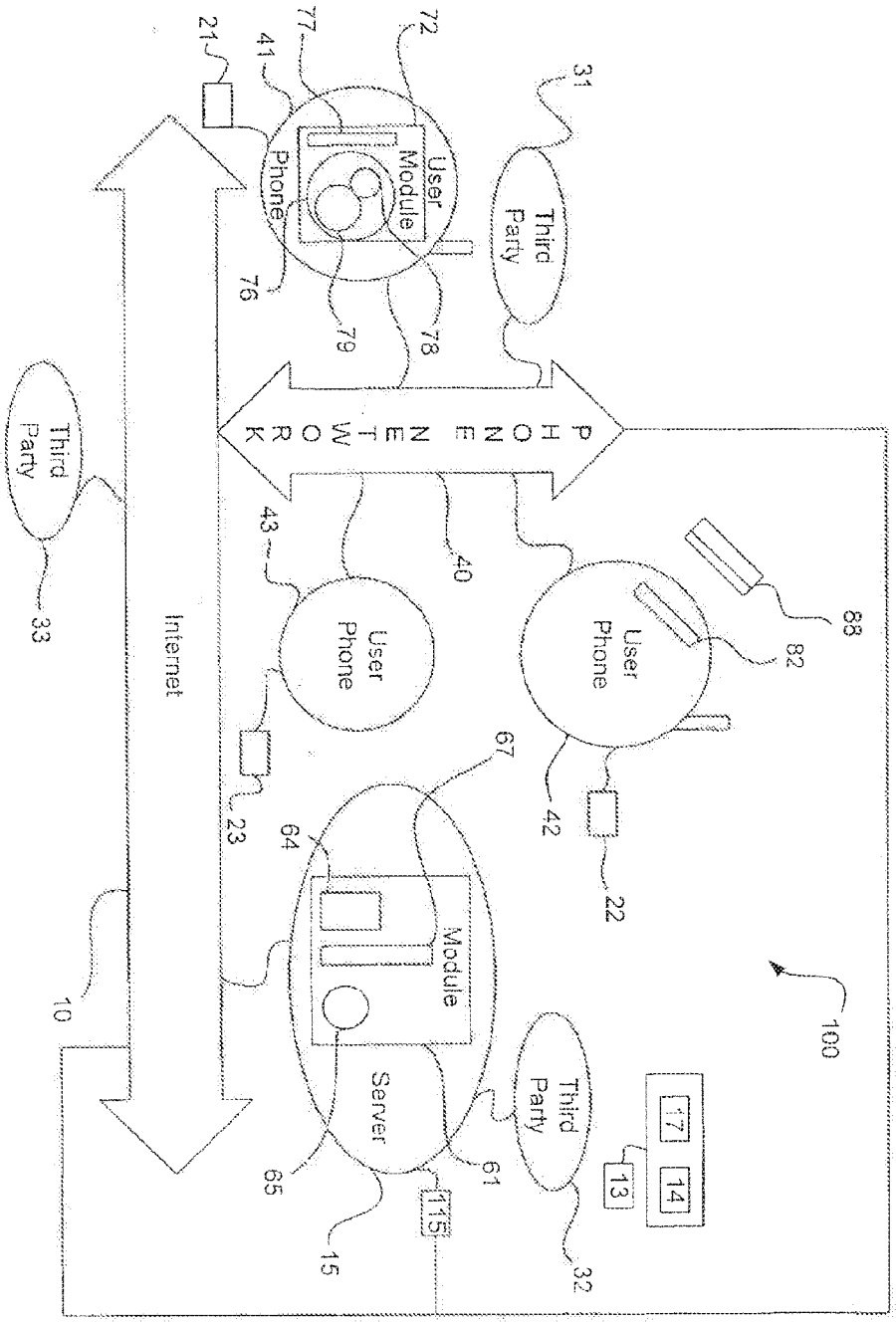
Third Party
33
Internet
10
Third Party
31
User Module
Phone
21
41
77
72
76
79
78
PHONE NETWORK
43
40
User Phone
23
User Phone
88
82
42
22
67
64
Module
Server
65
15
61
115
Third Party
32
17
14
13
100

FIG. 1

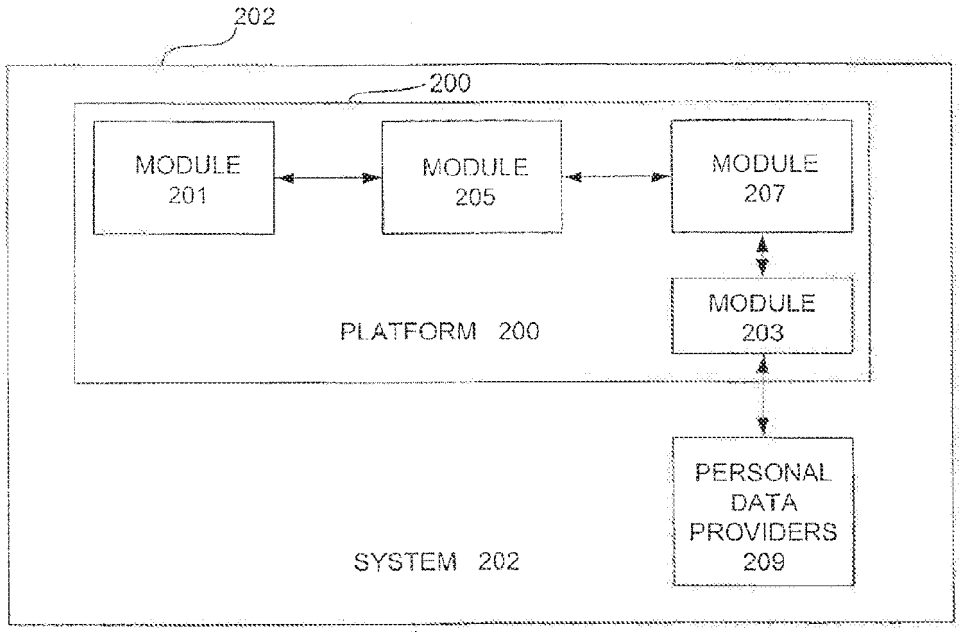
202
200
MODULE 201
MODULE 205
MODULE 207
MODULE 203
PLATFORM 200
PERSONAL DATA PROVIDERS 209
SYSTEM 202

FIG. 2

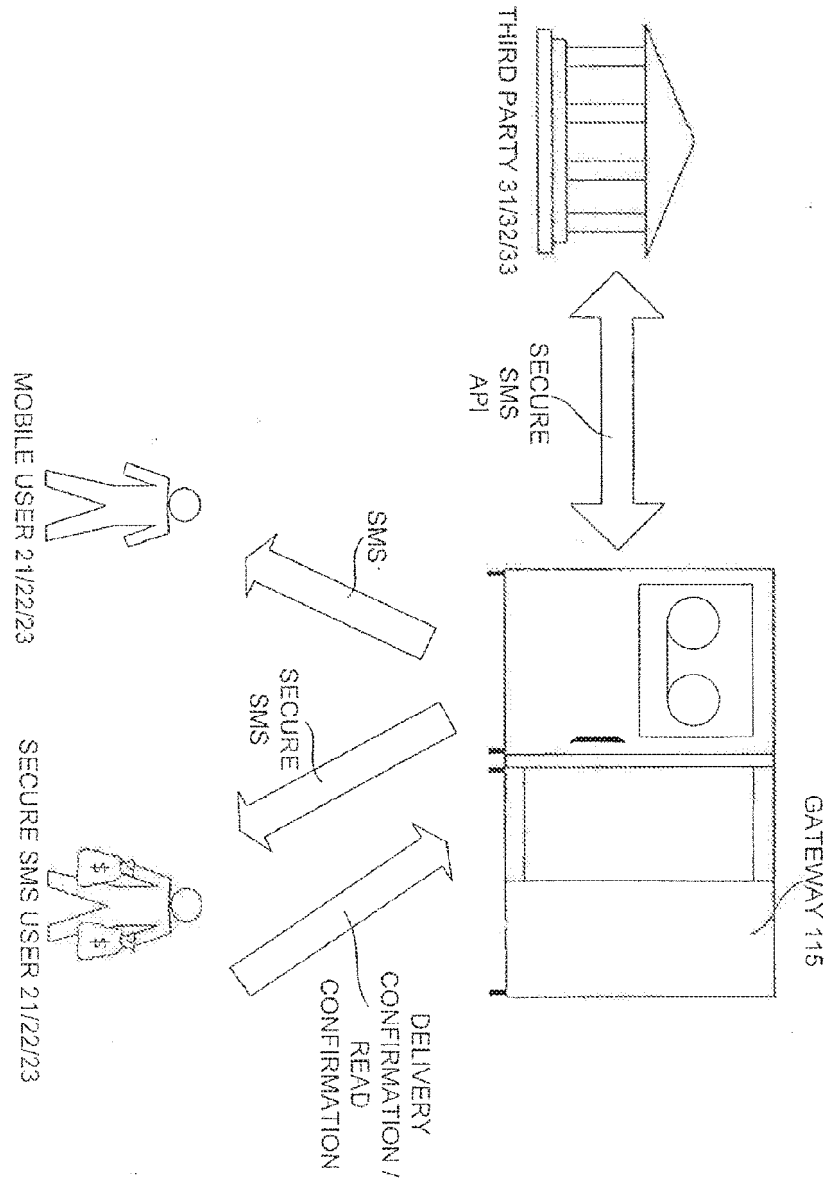
THIRD PARTY 31/32/33
SECURE SMS API
GATEWAY 115
SMS
SECURE SMS
DELIVERY CONFIRMATION / READ CONFIRMATION
MOBILE USER 21/22/23
SECURE SMS USER 21/22/23

FIG. 3

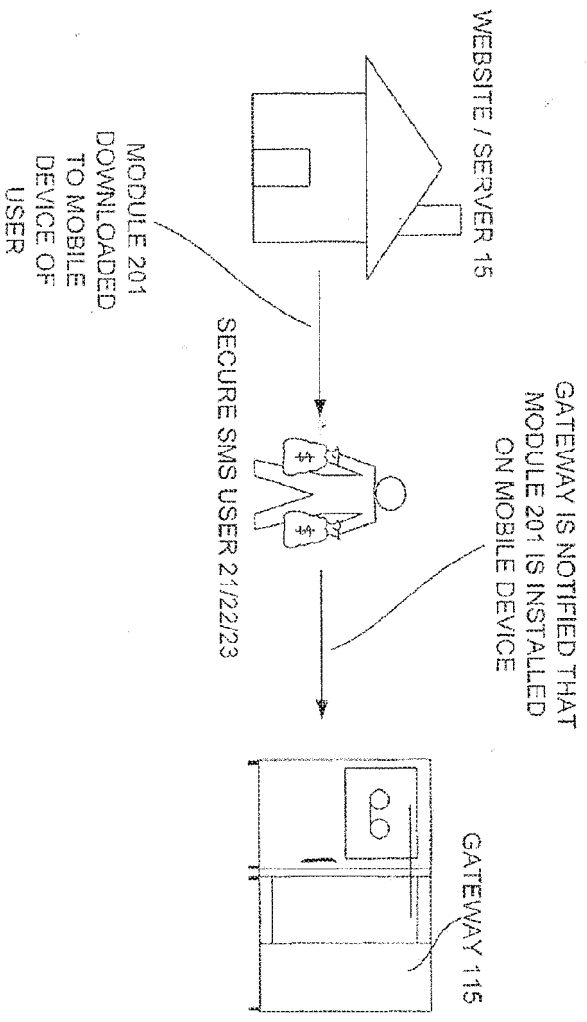
WEBSITE / SERVER 15
MODULE 201 DOWNLOADED TO MOBILE DEVICE OF USER
SECURE SMS USER 21/22/23
GATEWAY IS NOTIFIED THAT MODULE 201 IS INSTALLED ON MOBILE DEVICE
GATEWAY 115

FIG. 4

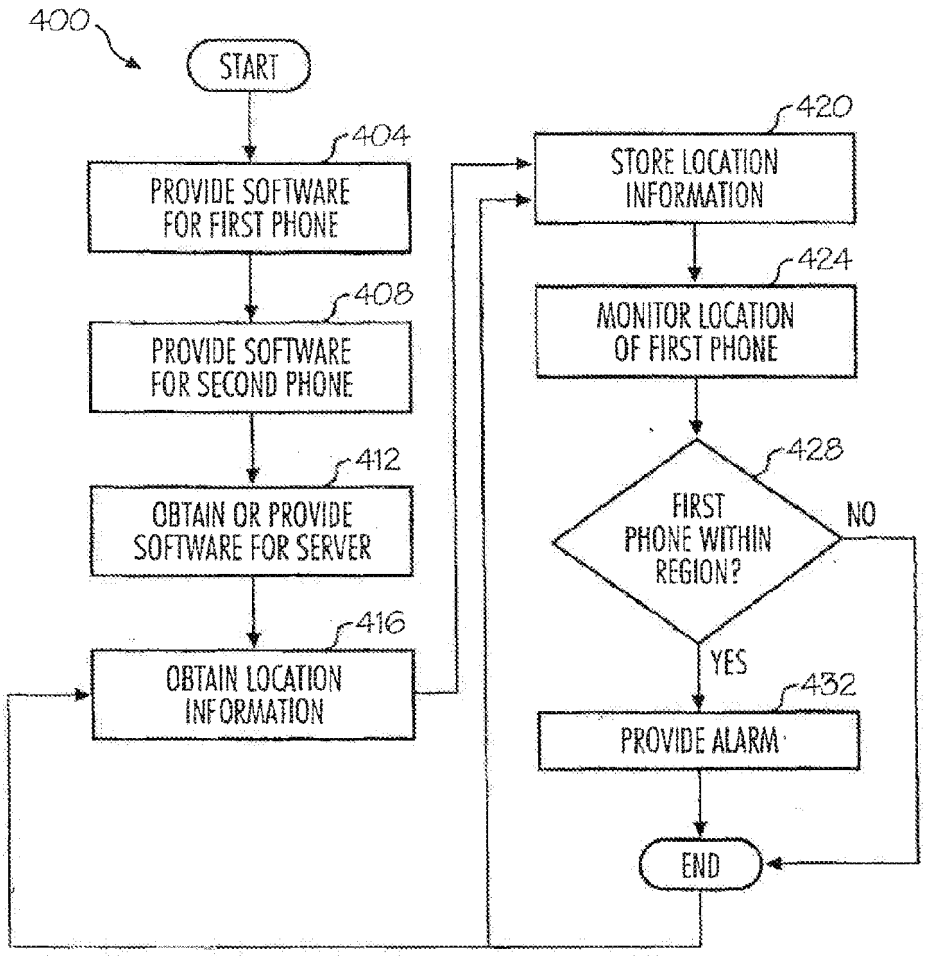
400
START
404
PROVIDE SOFTWARE FOR FIRST PHONE
408
PROVIDE SOFTWARE FOR SECOND PHONE
412
OBTAIN OR PROVIDE SOFTWARE FOR SERVER
416
OBTAIN LOCATION INFORMATION
420
STORE LOCATION INFORMATION
424
MONITOR LOCATION OF FIRST PHONE
428
FIRST PHONE WITHIN REGION?
NO
YES
432
PROVIDE ALARM
END

Fig. 4A

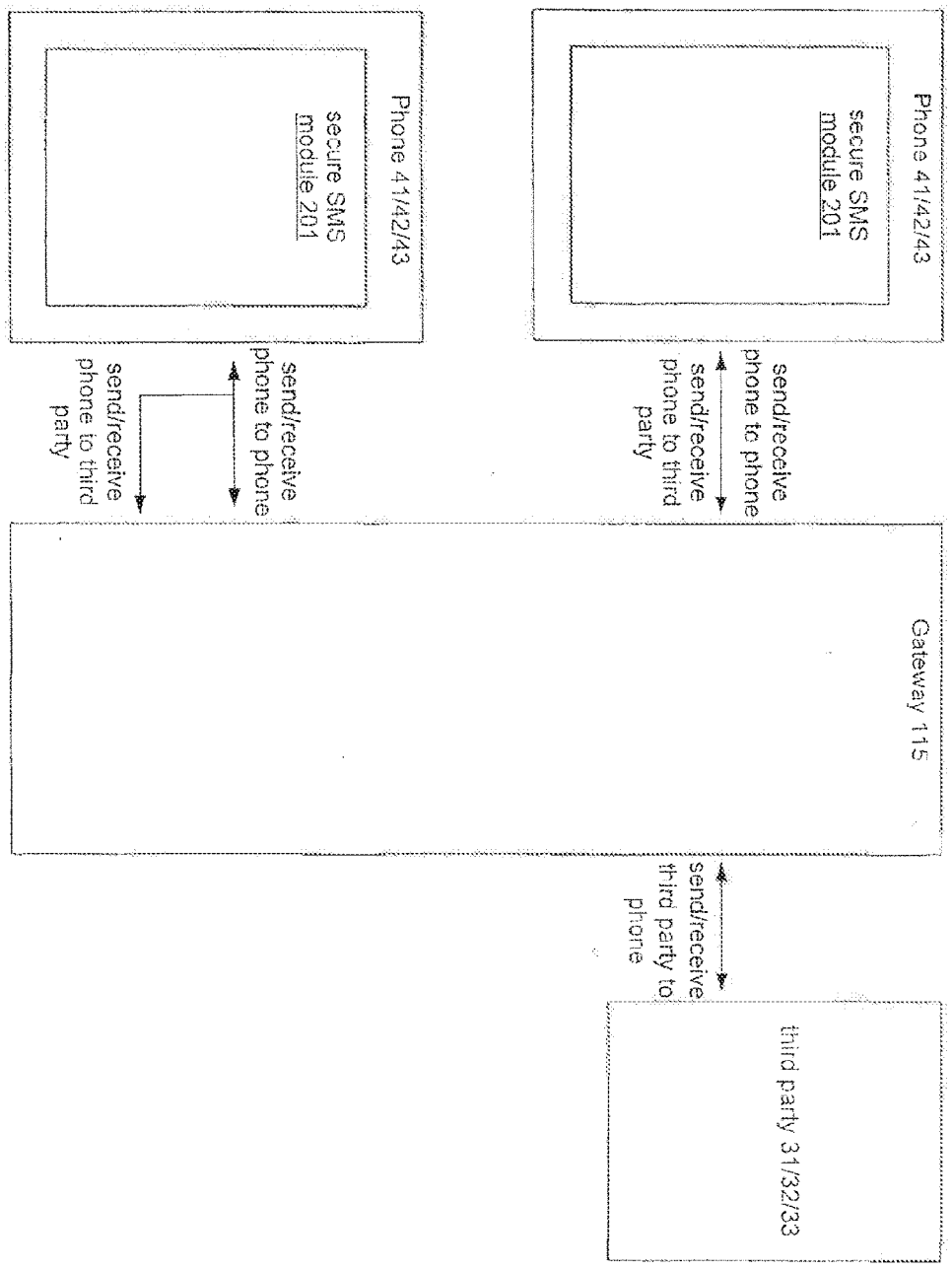
Phone 41/42/43
secure SMS module 201
send/receive phone to phone
send/receive phone to third party
Phone 41/42/43
secure SMS module 201
send/receive phone to phone
send/receive phone to third party
Gateway 115
send/receive third party to phone
third party 31/32/33

FIG. 5

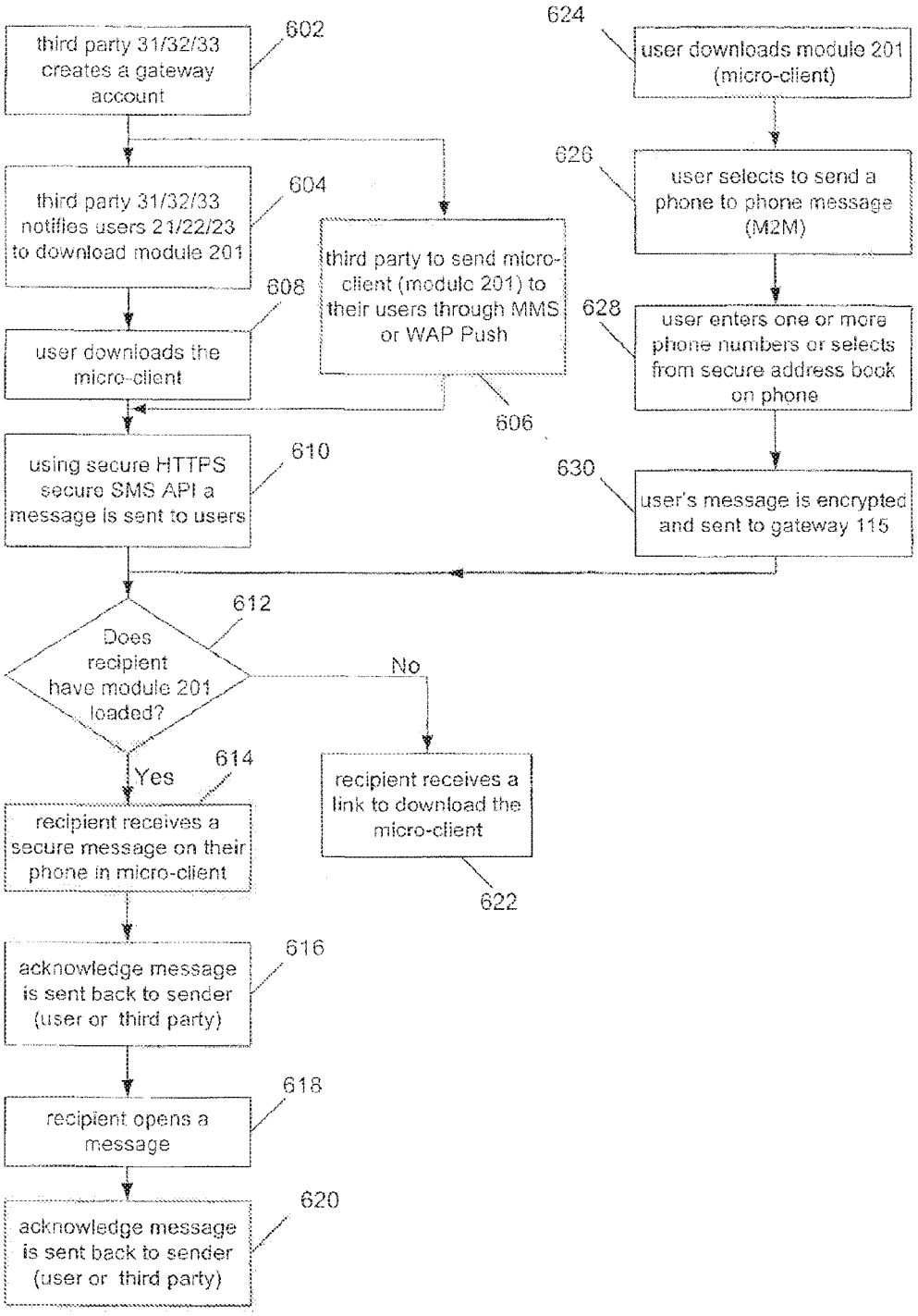
third party 31/32/33 creates a gateway account
602
third party 31/32/33 notifies users 21/22/23 to download module 201
604
user downloads the micro-client
608
third party to send micro-client (module 201) to their users through MMS or WAP Push
606
using secure HTTPS secure SMS API a message is sent to users
610
Does recipient have module 201 loaded?
612
Yes
No
recipient receives a secure message on their phone in micro-client
614
recipient receives a link to download the micro-client
622
acknowledge message is sent back to sender (user or third party)
616
recipient opens a message
618
acknowledge message is sent back to sender (user or third party)
620
user downloads module 201 (micro-client)
624
user selects to send a phone to phone message (M2M)
626
user enters one or more phone numbers or selects from secure address book on phone
628
user's message is encrypted and sent to gateway 115
630

FIG. 6

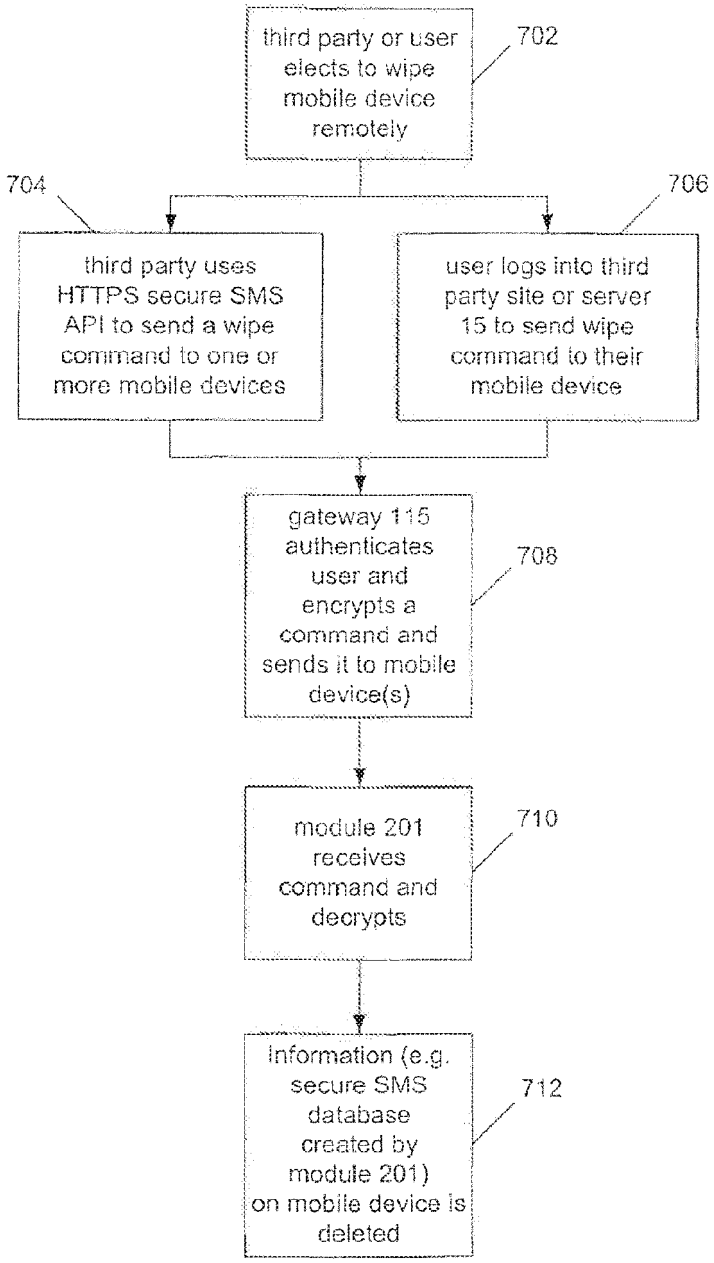
third party or user elects to wipe mobile device remotely
702
704
706
third party uses HTTPS secure SMS API to send a wipe command to one or more mobile devices
user logs into third party site or server 15 to send wipe command to their mobile device
gateway 115 authenticates user and encrypts a command and sends it to mobile device(s)
708
module 201 receives command and decrypts
710
Information (e.g. secure SMS database created by module 201) on mobile device is deleted
712

FIG. 7

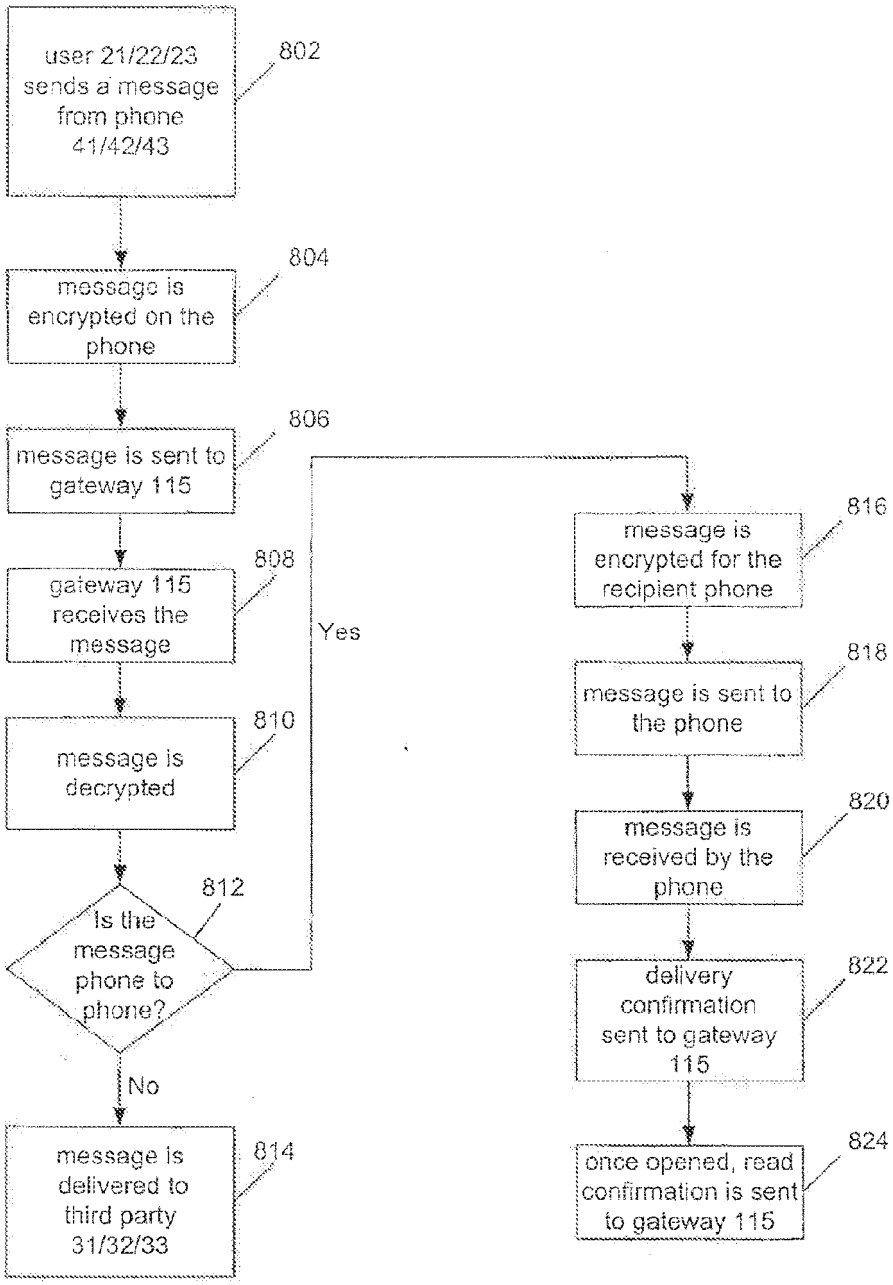
user 21/22/23 sends a message from phone 41/42/43
802
message is encrypted on the phone
804
message is sent to gateway 115
806
gateway 115 receives the message
808
message is decrypted
810
Is the message phone to phone?
812
Yes
No
message is delivered to third party 31/32/33
814
message is encrypted for the recipient phone
816
message is sent to the phone
818
message is received by the phone
820
delivery confirmation sent to gateway 115
822
once opened, read confirmation is sent to gateway 115
824

FIG. 8

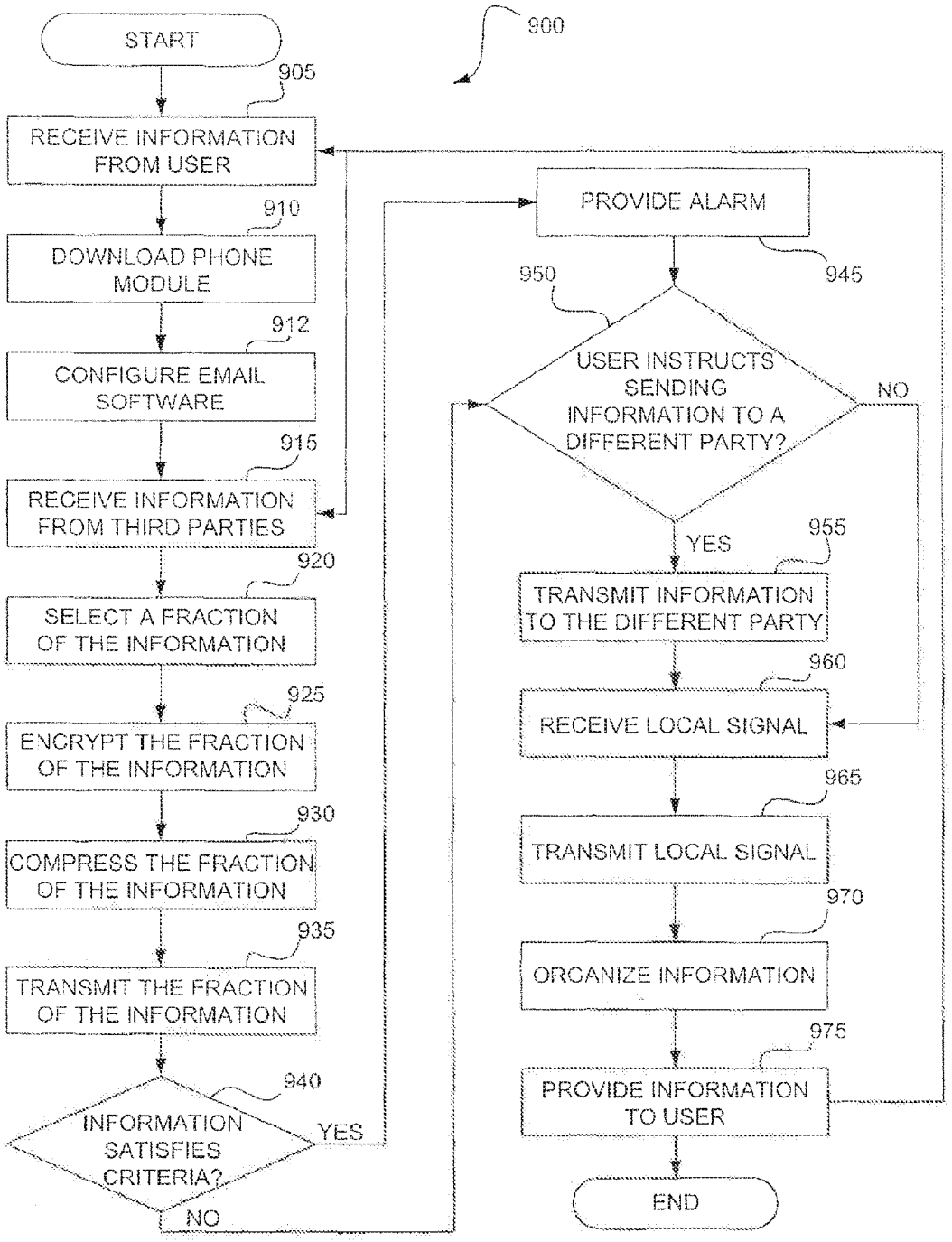
900
START
905
RECEIVE INFORMATION FROM USER
910
DOWNLOAD PHONE MODULE
912
CONFIGURE EMAIL SOFTWARE
915
RECEIVE INFORMATION FROM THIRD PARTIES
920
SELECT A FRACTION OF THE INFORMATION
925
ENCRYPT THE FRACTION OF THE INFORMATION
930
COMPRESS THE FRACTION OF THE INFORMATION
935
TRANSMIT THE FRACTION OF THE INFORMATION
940
INFORMATION SATISFIES CRITERIA?
YES
NO
PROVIDE ALARM
945
950
USER INSTRUCTS SENDING INFORMATION TO A DIFFERENT PARTY?
NO
YES
955
TRANSMIT INFORMATION TO THE DIFFERENT PARTY
960
RECEIVE LOCAL SIGNAL
965
TRANSMIT LOCAL SIGNAL
970
ORGANIZE INFORMATION
975
PROVIDE INFORMATION TO USER
END

FIG. 9

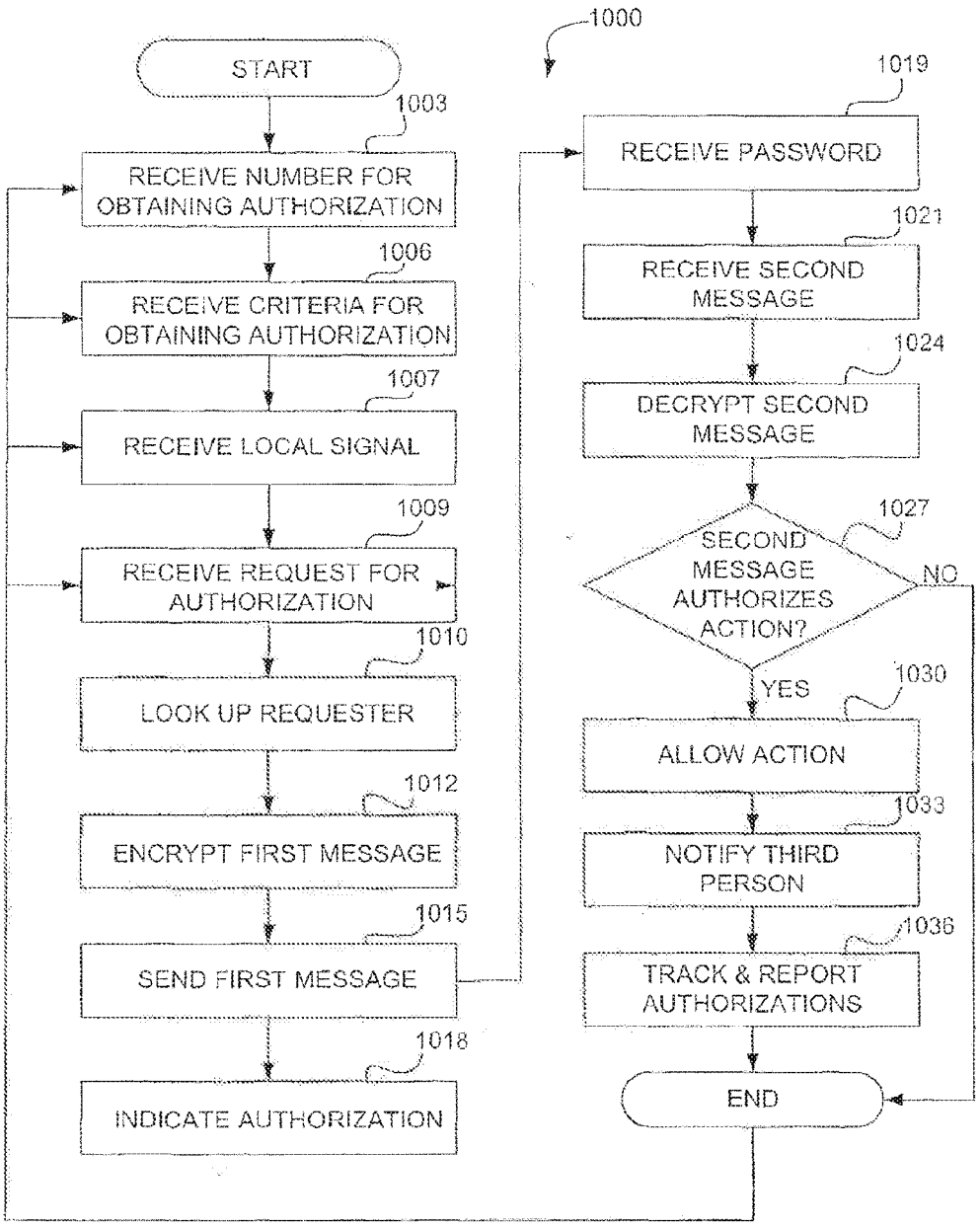
1000
START
1003
RECEIVE NUMBER FOR OBTAINING AUTHORIZATION
1006
RECEIVE CRITERIA FOR OBTAINING AUTHORIZATION
1007
RECEIVE LOCAL SIGNAL
1009
RECEIVE REQUEST FOR AUTHORIZATION
1010
LOOK UP REQUESTER
1012
ENCRYPT FIRST MESSAGE
1015
SEND FIRST MESSAGE
1018
INDICATE AUTHORIZATION
1019
RECEIVE PASSWORD
1021
RECEIVE SECOND MESSAGE
1024
DECRYPT SECOND MESSAGE
1027
SECOND MESSAGE AUTHORIZES ACTION?
NO
YES
1030
ALLOW ACTION
1033
NOTIFY THIRD PERSON
1036
TRACK & REPORT AUTHORIZATIONS
END

FIG. 10

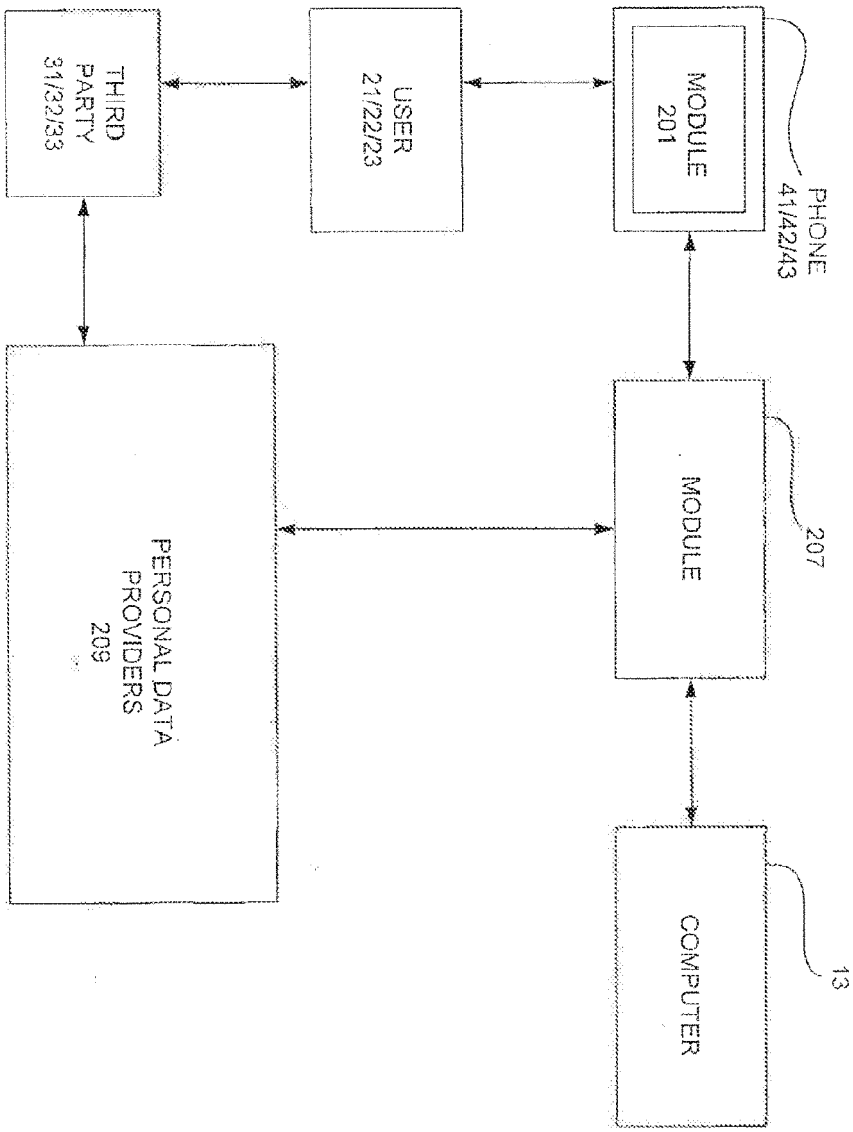
THIRD PARTY 31/32/33
USER 21/22/23
MODULE 201
PHONE 41/42/43
PERSONAL DATA PROVIDERS 209
MODULE 207
COMPUTER 13

FIG. 11

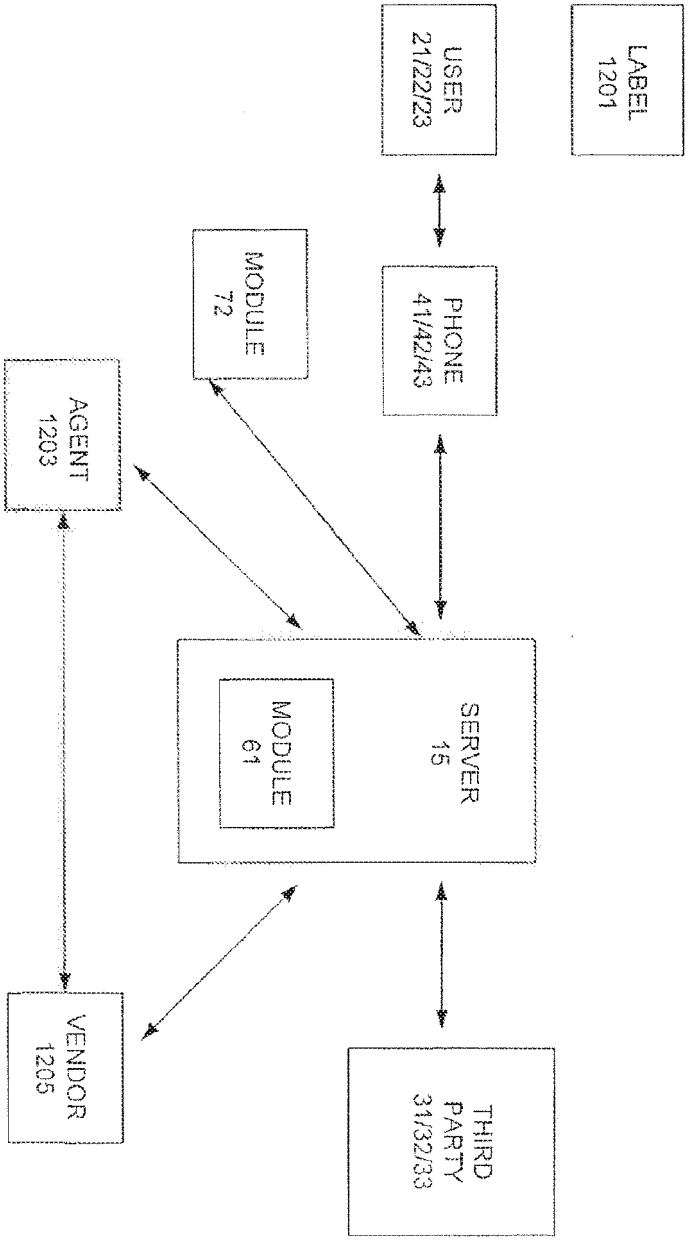
USER
21/22/23
LABEL
1201
PHONE
41/42/43
MODULE
72
AGENT
1203
SERVER
15
MODULE
61
VENDOR
1205
THIRD
PARTY
31/32/33

FIG. 12

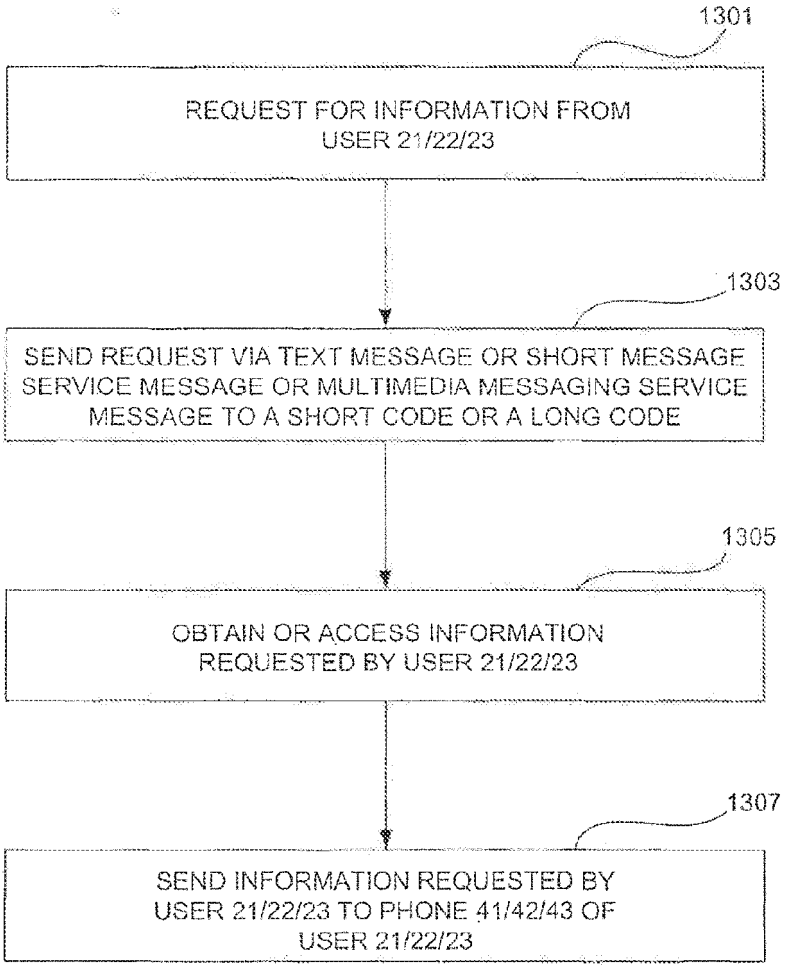
1301
REQUEST FOR INFORMATION FROM USER 21/22/23
1303
SEND REQUEST VIA TEXT MESSAGE OR SHORT MESSAGE SERVICE MESSAGE OR MULTIMEDIA MESSAGING SERVICE MESSAGE TO A SHORT CODE OR A LONG CODE
1305
OBTAIN OR ACCESS INFORMATION REQUESTED BY USER 21/22/23
1307
SEND INFORMATION REQUESTED BY USER 21/22/23 TO PHONE 41/42/43 OF USER 21/22/23

FIG. 13

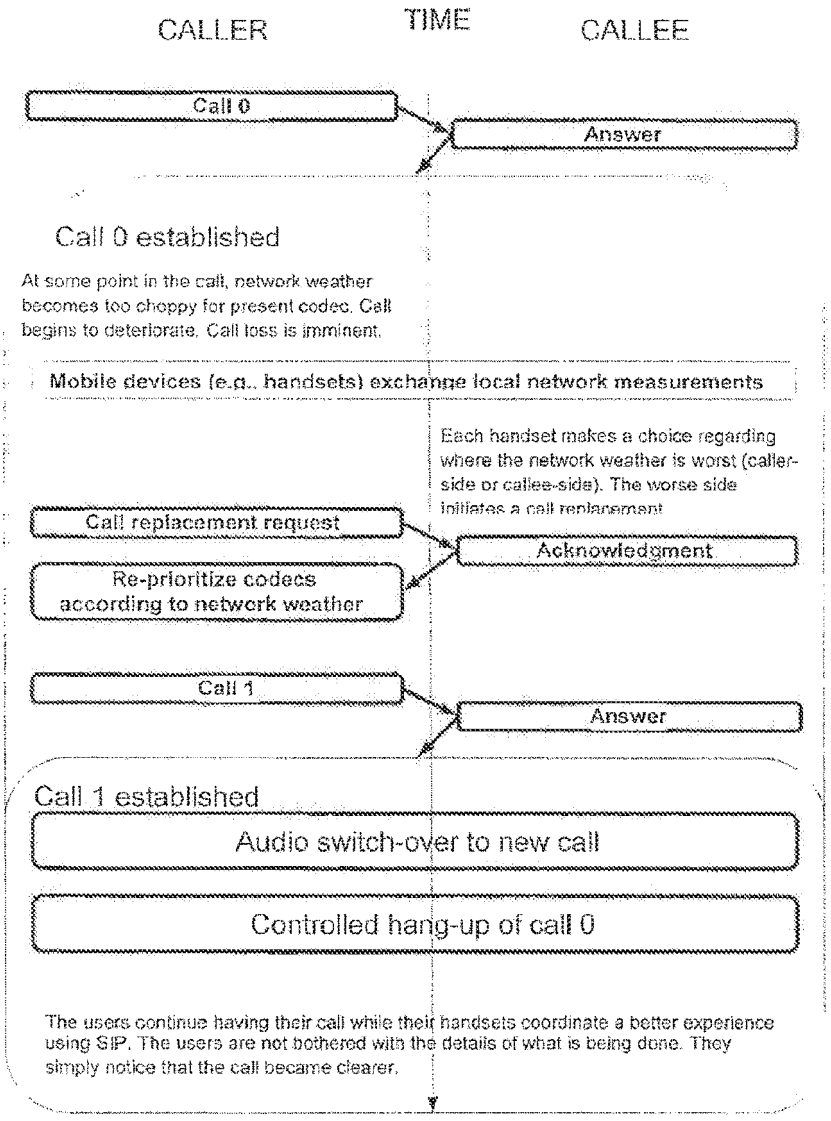
CALLER
TIME
CALLEE
Call 0
Answer
Call 0 established
At some point in the call, network weather becomes too choppy for present codec. Call begins to deteriorate. Call loss is imminent.
Mobile devices (e.g., handsets) exchange local network measurements
Each handset makes a choice regarding where the network weather is worst (caller-side or callee-side). The worse side initiates a call replacement
Call replacement request
Acknowledgment
Re-prioritize codecs according to network weather
Call 1
Answer
Call 1 established
Audio switch-over to new call
Controlled hang-up of call 0
The users continue having their call while their handsets coordinate a better experience using SIP. The users are not bothered with the details of what is being done. They simply notice that the call became clearer.

FIG. 14

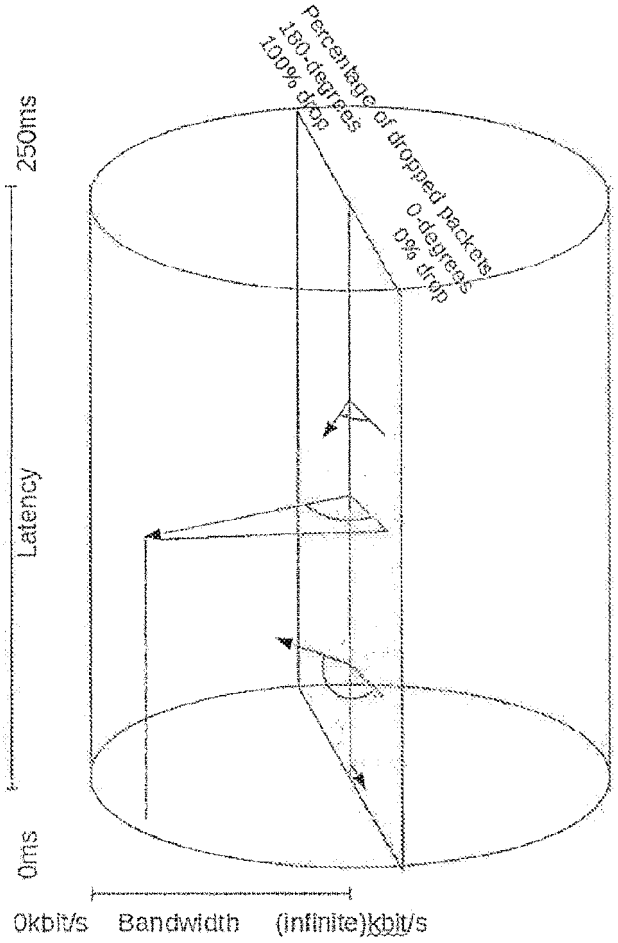
Percentage of dropped packets
180-degrees
100% drop
0-degrees
0% drop
250ms
Latency
0ms
0kbit/s
Bandwidth
(infinite)kbit/s

FIG. 15

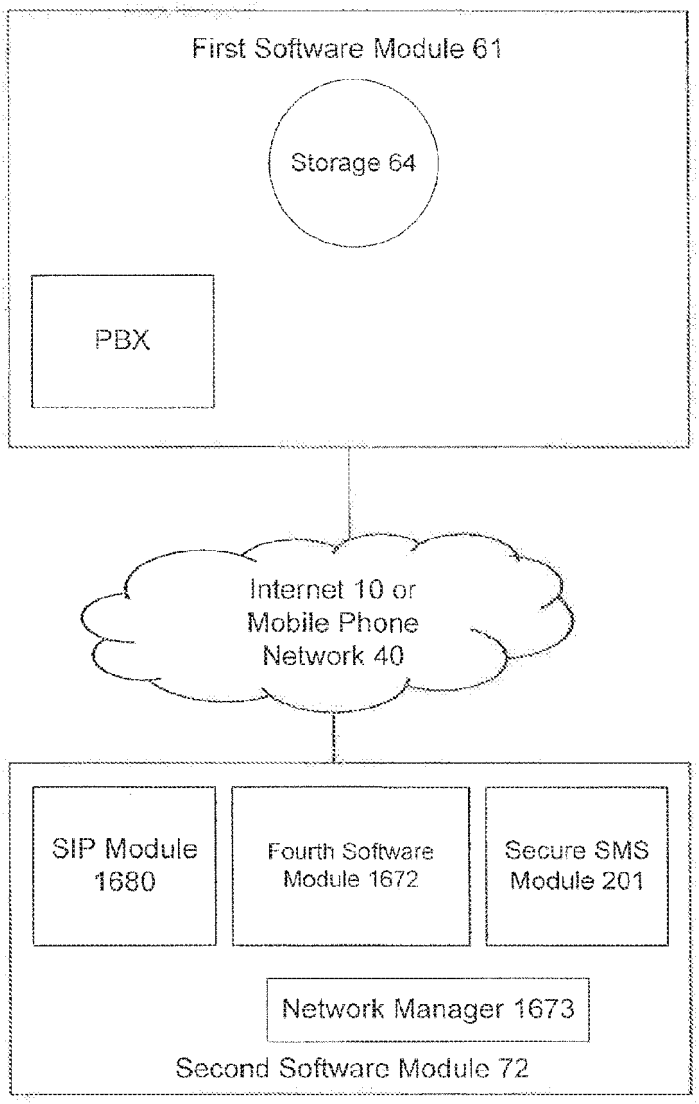
First Software Module 61
Storage 64
PBX
Internet 10 or
Mobile Phone
Network 40
SIP Module
1680
Fourth Software
Module 1672
Secure SMS
Module 201
Network Manager 1673
Second Software Module 72

FIG. 16

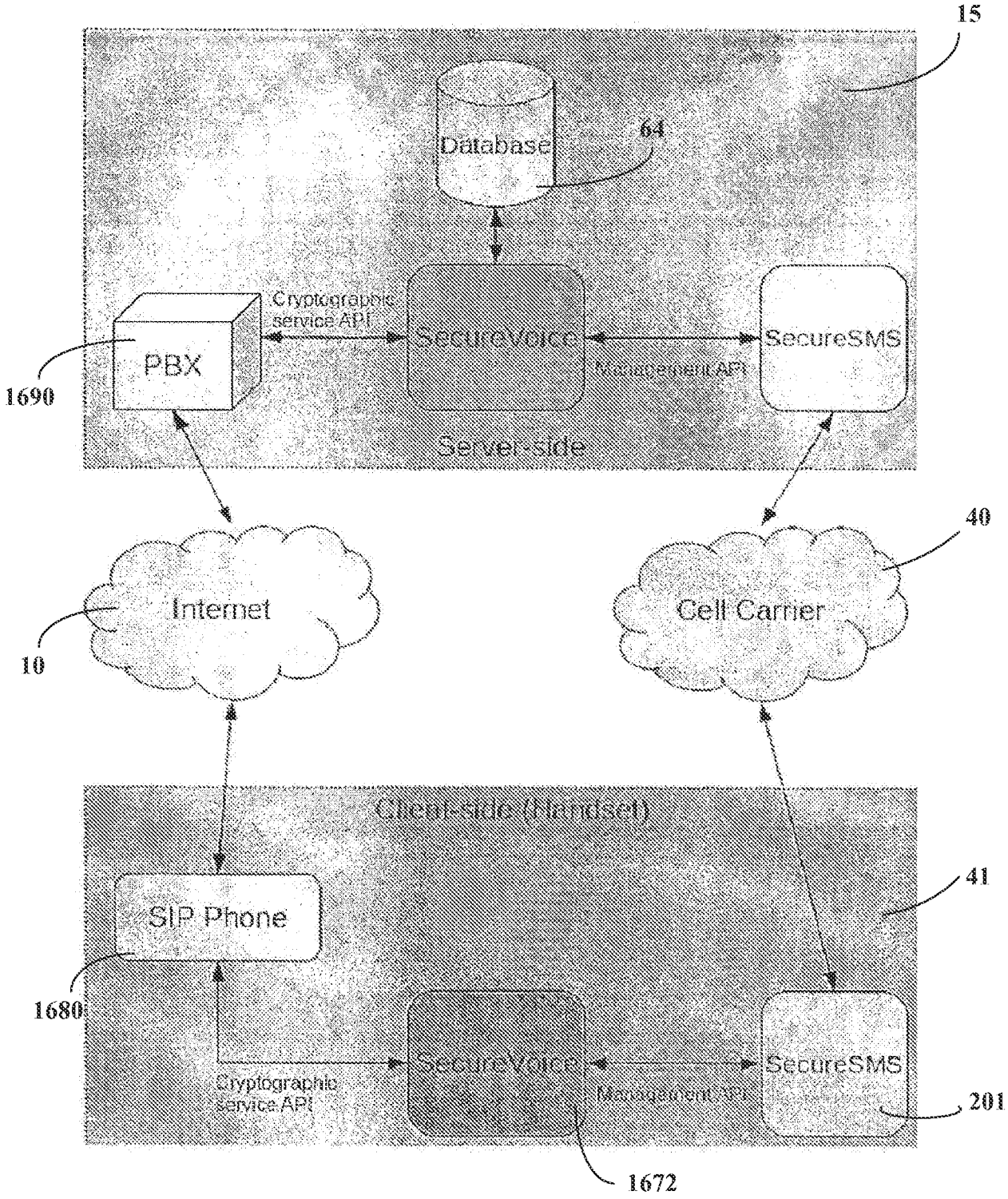
15
Database
64
Cryptographic service API
SecureVoice
SecureSMS
PBX
1690
Management API
Server-side
40
Internet
Cell Carrier
10
Client-side (Handset)
41
SIP Phone
1680
SecureVoice
SecureSMS
Cryptographic service API
Management API
201
1672

FIG. 16A

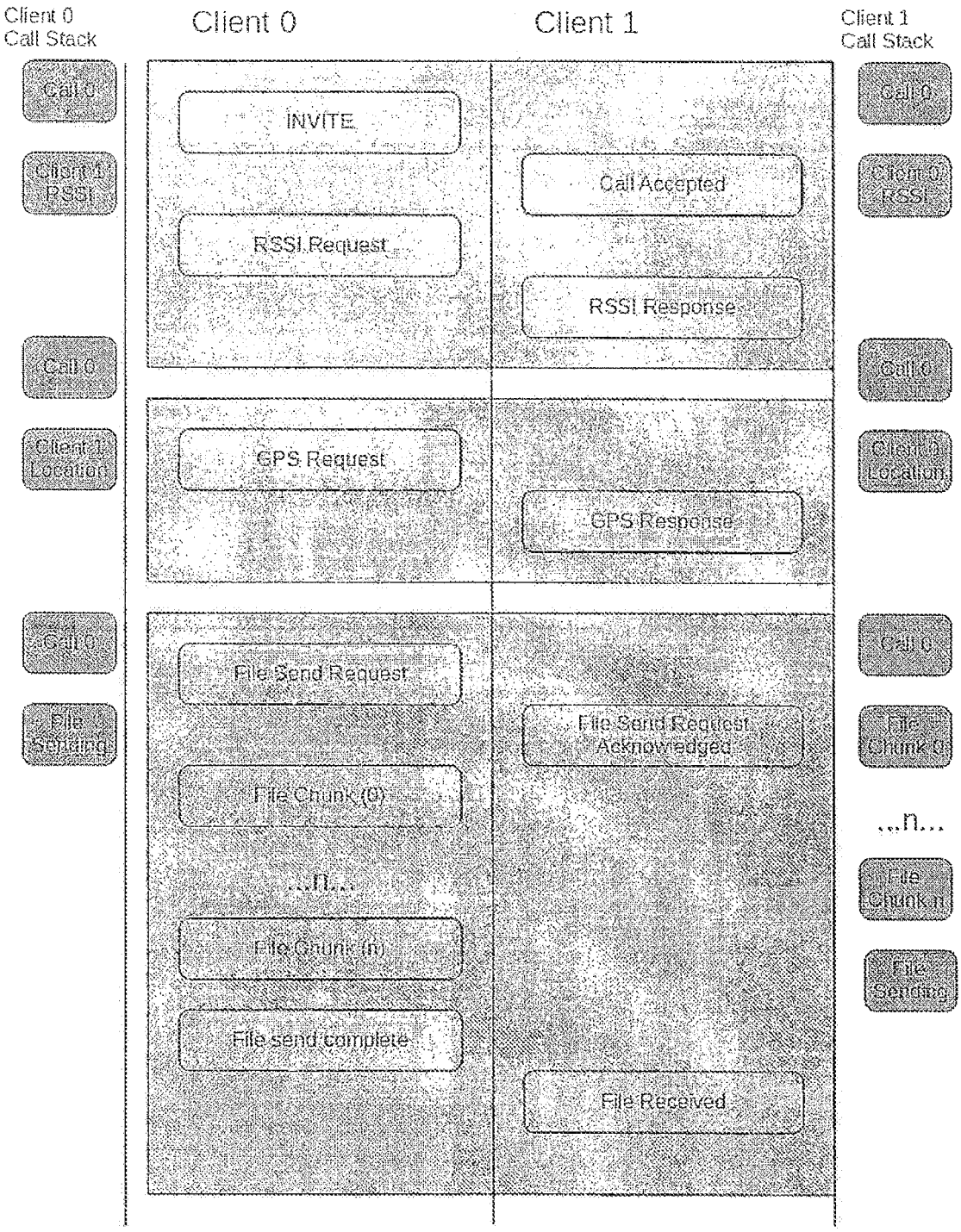
Client 0
Call Stack
Client 0
Client 1
Client 1
Call Stack
Call 0
Client 1 RSSI
Call 0
Client 1 Location
Call 0
File Sending
INVITE
RSSI Request
Call Accepted
RSSI Response
GPS Request
GPS Response
File Send Request
File Send Request Acknowledged
File Chunk (0)
...n...
File Chunk (n)
File send complete
File Received
Call 0
Client 0 RSSI
Call 0
Client 0 Location
Call 0
File Chunk 0
...n...
File Chunk n
File Sending

FIG. 17

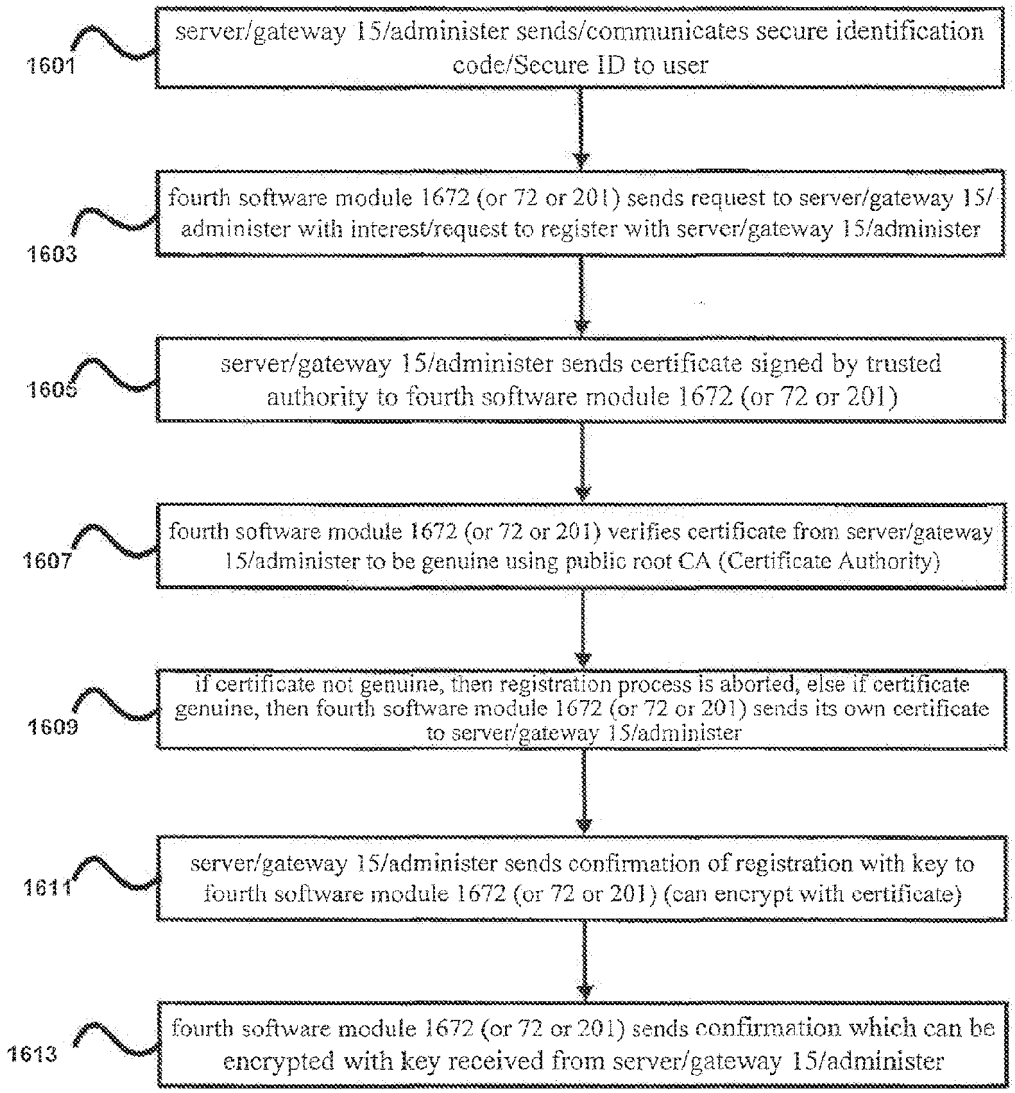
1601
server/gateway 15/administer sends/communicates secure identification code/Secure ID to user
1603
fourth software module 1672 (or 72 or 201) sends request to server/gateway 15/ administer with interest/request to register with server/gateway 15/administer
1605
server/gateway 15/administer sends certificate signed by trusted authority to fourth software module 1672 (or 72 or 201)
1607
fourth software module 1672 (or 72 or 201) verifies certificate from server/gateway 15/administer to be genuine using public root CA (Certificate Authority)
1609
if certificate not genuine, then registration process is aborted, else if certificate genuine, then fourth software module 1672 (or 72 or 201) sends its own certificate to server/gateway 15/administer
1611
server/gateway 15/administer sends confirmation of registration with key to fourth software module 1672 (or 72 or 201) (can encrypt with certificate)
1613
fourth software module 1672 (or 72 or 201) sends confirmation which can be encrypted with key received from server/gateway 15/administer

FIG. 18