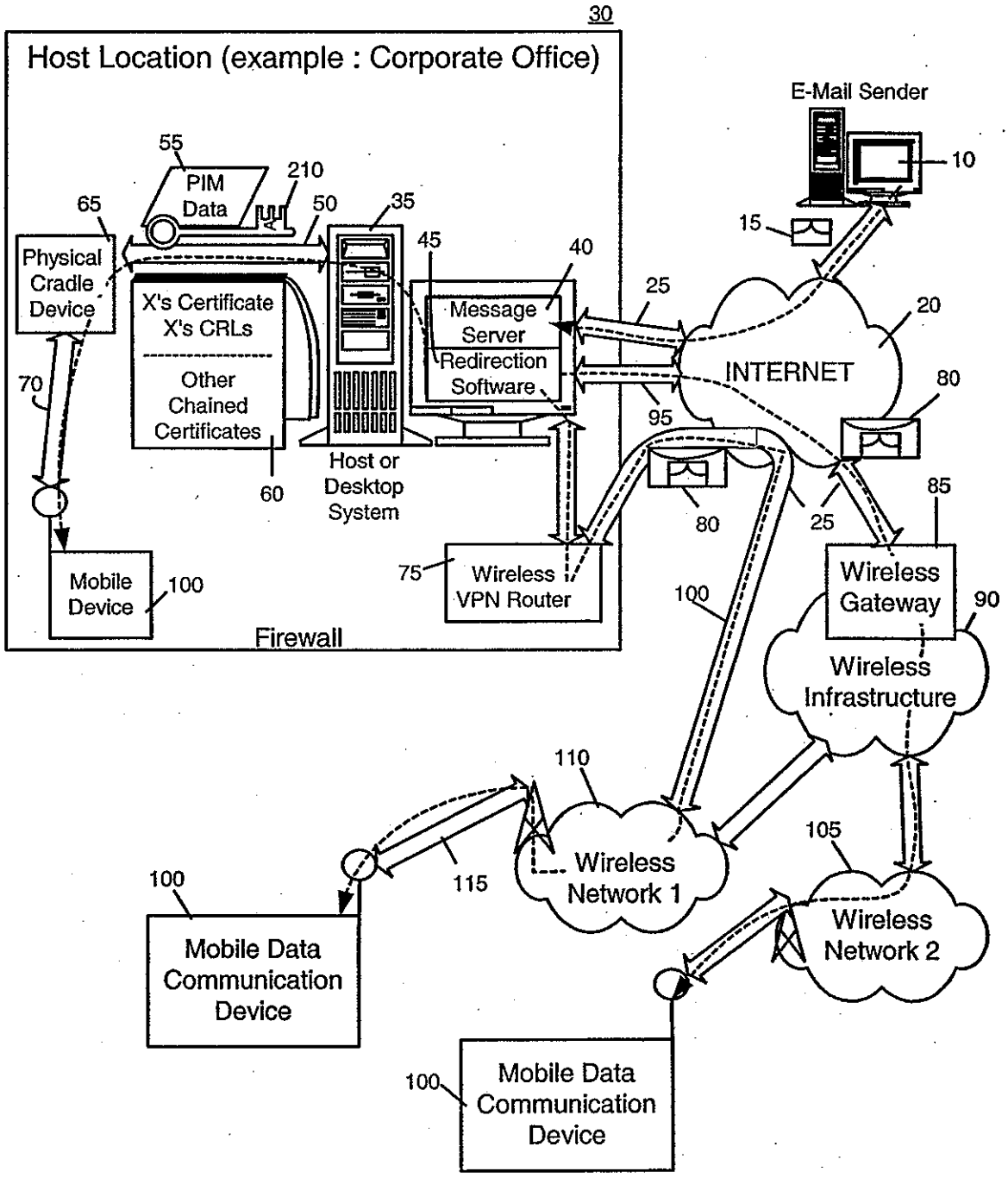

30
Host Location (example : Corporate Office)
E-Mail Sender
10
55
PIM Data
210
65
50
35
45
40
Physical Cradle Device
X's Certificate
X's CRLs
Other Chained Certificates
60
Host or Desktop System
Message Server
Redirection Software
15
25
20
INTERNET
80
95
70
Mobile Device
100
75
Wireless VPN Router
Firewall
80
25
85
Wireless Gateway
90
Wireless Infrastructure
100
110
Wireless Network 1
115
105
Wireless Network 2
100
Mobile Data Communication Device
100
Mobile Data Communication Device

Fig. 1

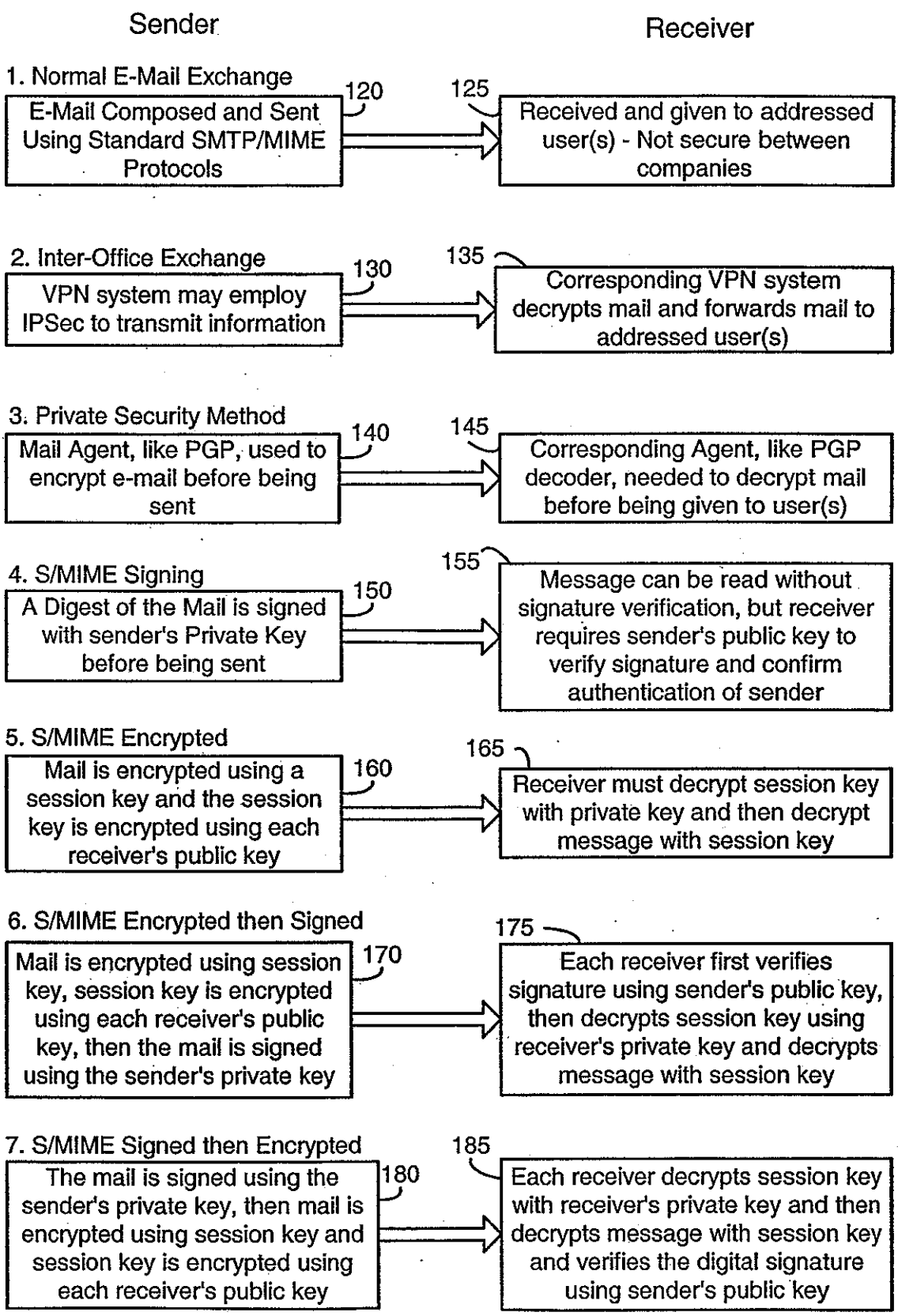

Sender
Receiver
1. Normal E-Mail Exchange
E-Mail Composed and Sent Using Standard SMTP/MIME Protocols
120
125
Received and given to addressed user(s) - Not secure between companies
2. Inter-Office Exchange
VPN system may employ IPSec to transmit information
130
135
Corresponding VPN system decrypts mail and forwards mail to addressed user(s)
3. Private Security Method
Mail Agent, like PGP, used to encrypt e-mail before being sent
140
145
Corresponding Agent, like PGP decoder, needed to decrypt mail before being given to user(s)
4. S/MIME Signing
A Digest of the Mail is signed with sender's Private Key before being sent
150
155
Message can be read without signature verification, but receiver requires sender's public key to verify signature and confirm authentication of sender
5. S/MIME Encrypted
Mail is encrypted using a session key and the session key is encrypted using each receiver's public key
160
165
Receiver must decrypt session key with private key and then decrypt message with session key
6. S/MIME Encrypted then Signed
Mail is encrypted using session key, session key is encrypted using each receiver's public key, then the mail is signed using the sender's private key
170
175
Each receiver first verifies signature using sender's public key, then decrypts session key using receiver's private key and decrypts message with session key
7. S/MIME Signed then Encrypted
The mail is signed using the sender's private key, then mail is encrypted using session key and session key is encrypted using each receiver's public key
180
185
Each receiver decrypts session key with receiver's private key and then decrypts message with session key and verifies the digital signature using sender's public key

Fig. 2

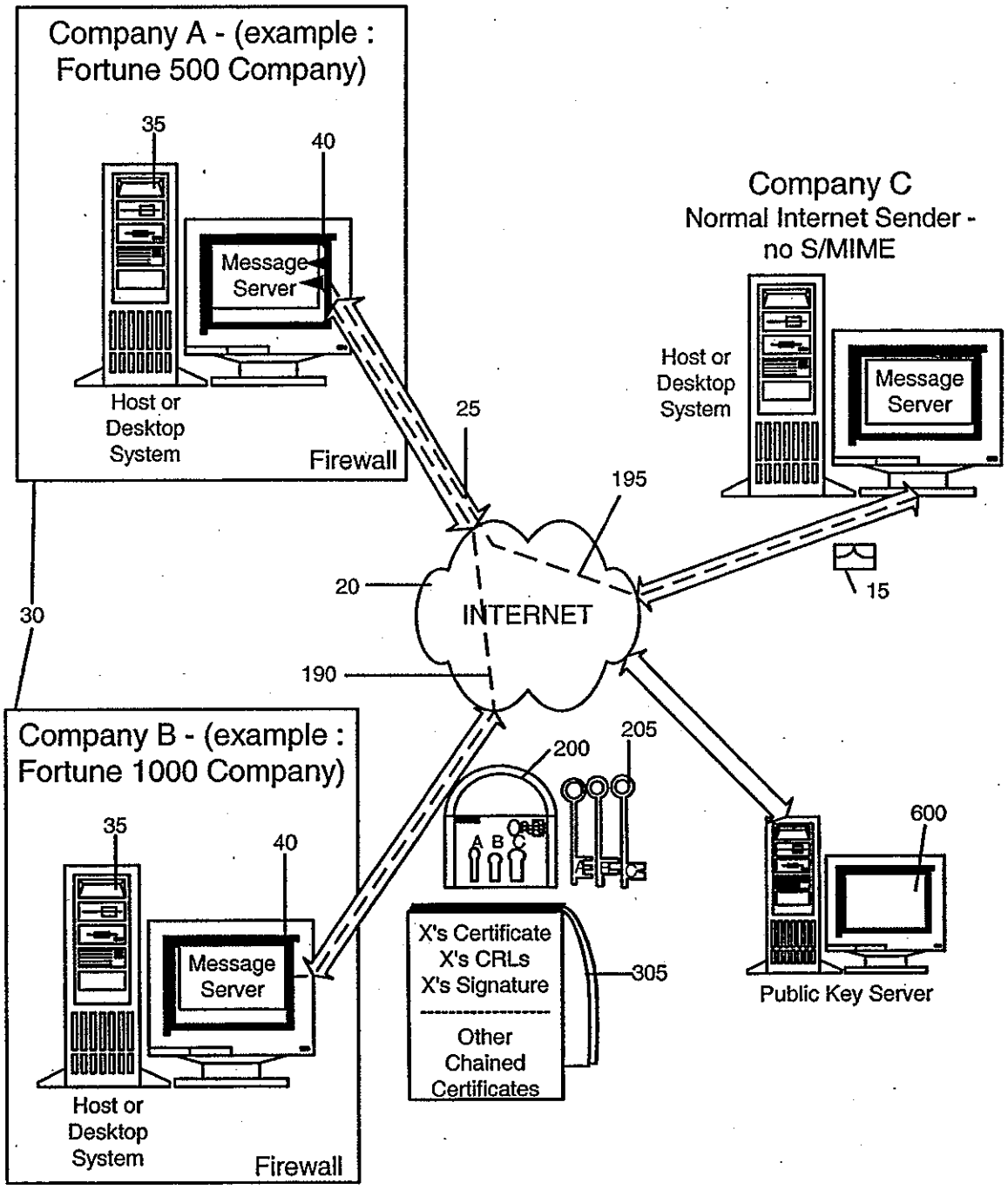

Company A - (example : Fortune 500 Company)
35
40
Message Server
Host or Desktop System
Firewall
Company C
Normal Internet Sender - no S/MIME
Host or Desktop System
Message Server
25
195
20
INTERNET
15
30
190
Company B - (example : Fortune 1000 Company)
35
40
Message Server
Host or Desktop System
Firewall
200
205
A B C
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
305
600
Public Key Server

Fig. 3

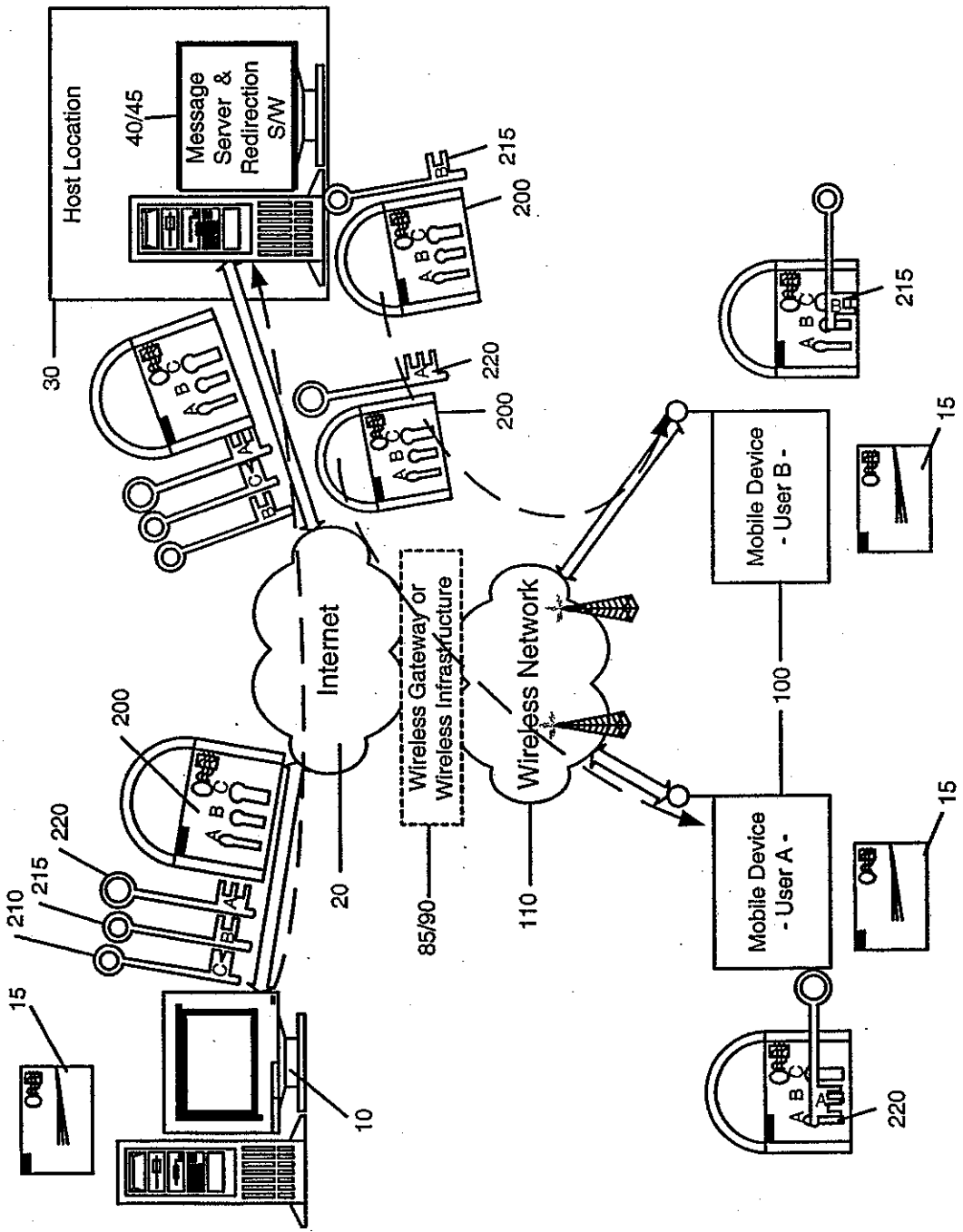

Host Location
40/45
Message Server & Redirection S/W
30
Internet
20
Wireless Gateway or Wireless Infrastructure
85/90
Wireless Network
110
Mobile Device - User B -
Mobile Device - User A -
100
10
15
200
210
215
220

Fig. 4

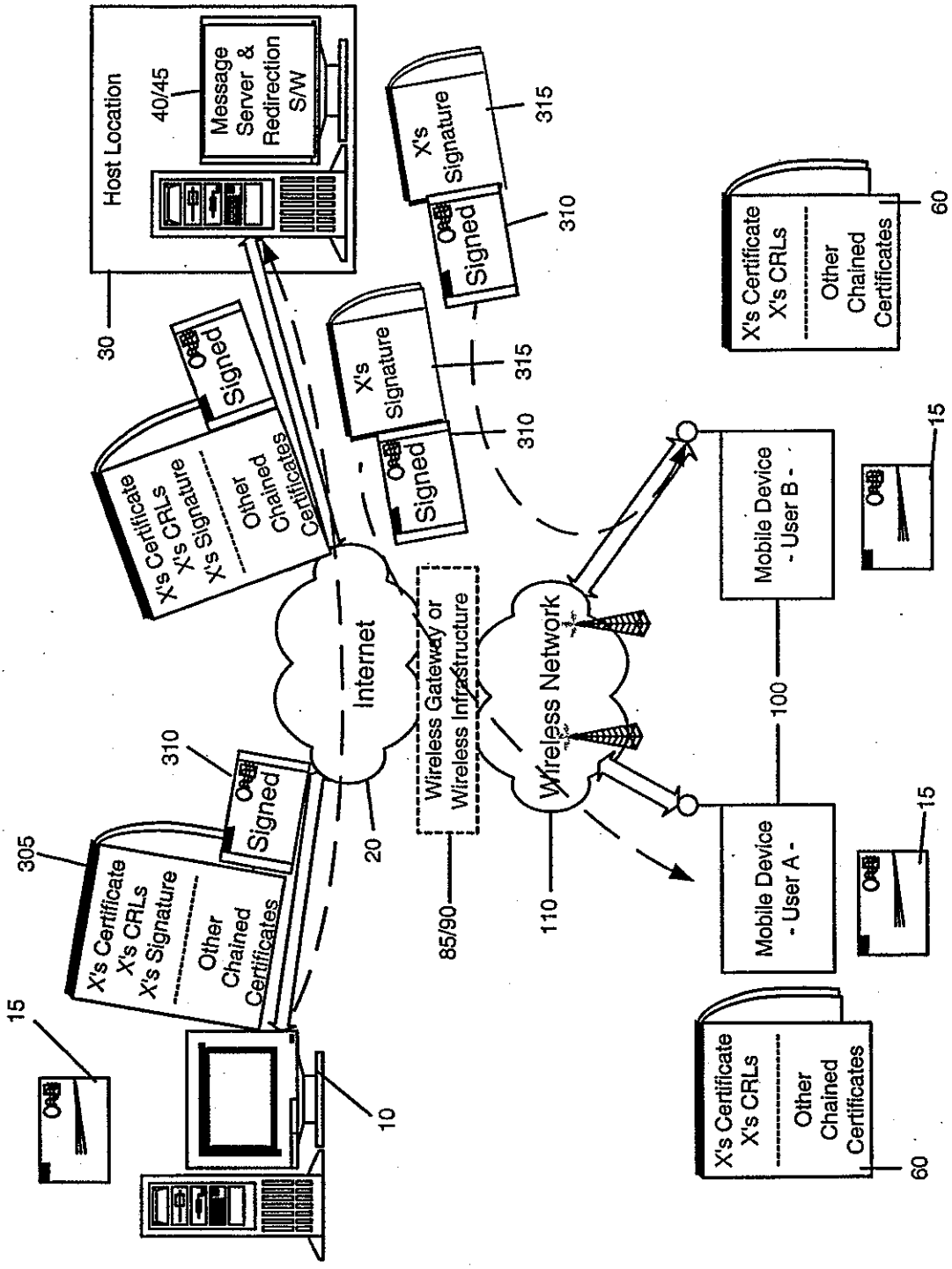

Host Location
40/45
Message Server & Redirection S/W
30
X's Signature
315
Signed
310
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
305
Internet
20
Wireless Gateway or Wireless Infrastructure
85/90
Wireless Network
110
Mobile Device - User A -
Mobile Device - User B -
100
10
15
60

Fig. 5

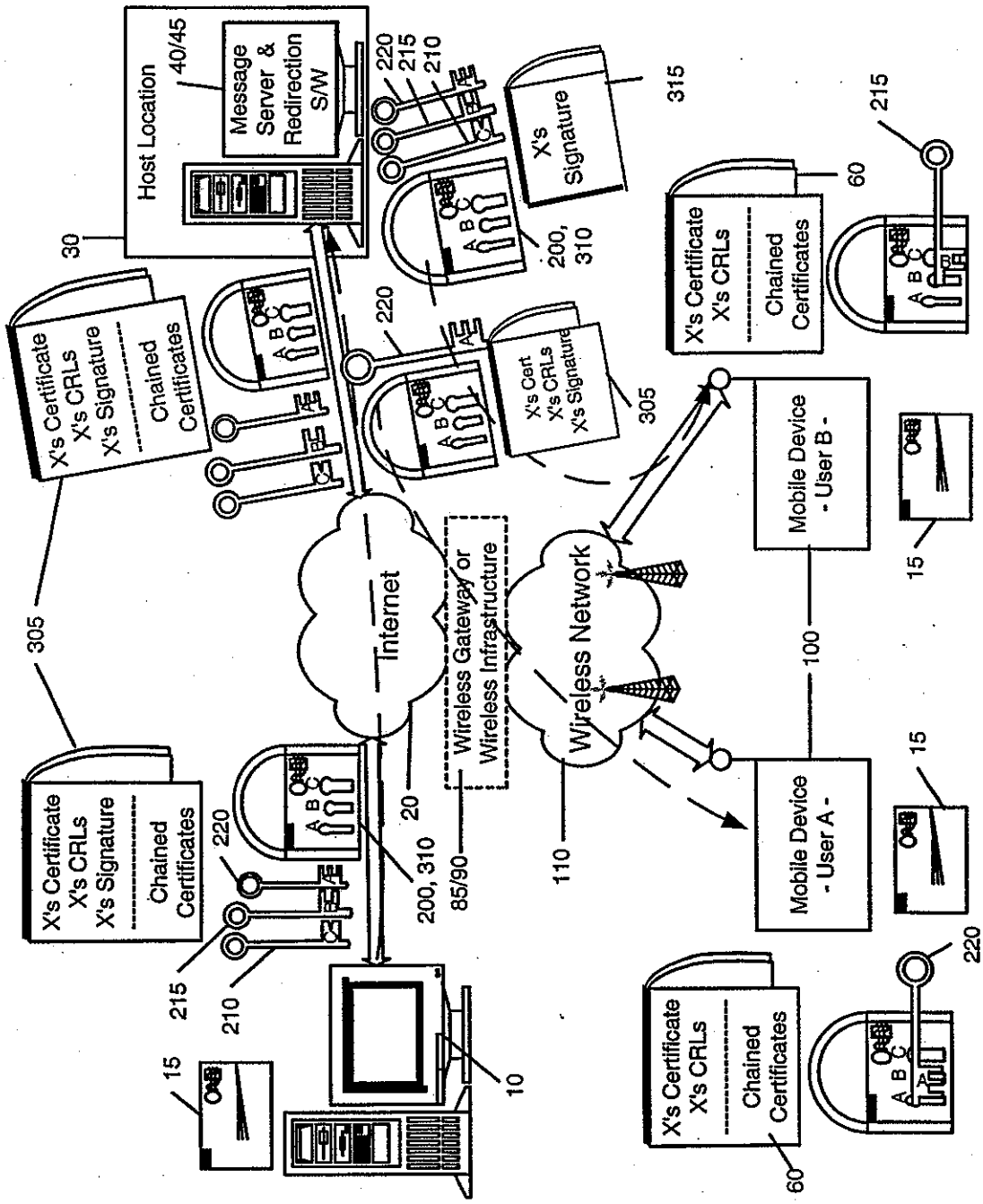

Host Location
40/45
Message Server & Redirection S/W
220
215
210
30
X's Signature
315
200, 310
X's Certificate
X's CRLs
X's Signature
Chained Certificates
220
X's Cert
X's CRLs
X's Signature
305
X's Certificate
X's CRLs
Chained Certificates
60
215
Internet
Wireless Gateway or
Wireless Infrastructure
Wireless Network
Mobile Device
- User B -
15
100
305
X's Certificate
X's CRLs
X's Signature
Chained Certificates
220
215
210
200, 310
85/90
20
110
Mobile Device
- User A -
15
X's Certificate
X's CRLs
Chained Certificates
60
220
15
10

Fig. 6

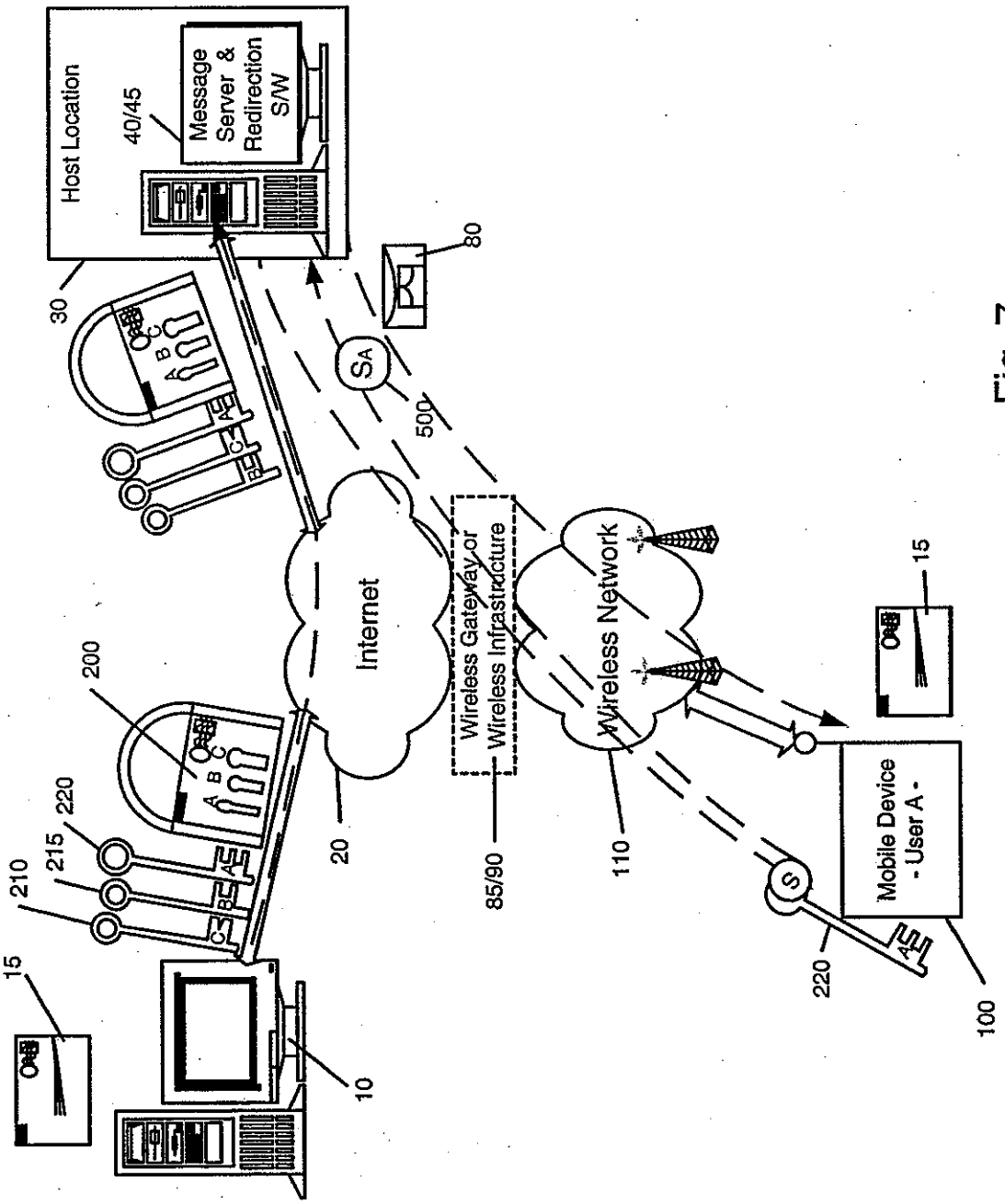

Host Location
40/45
Message Server & Redirection S/W
30
80
$S_A$
500
Internet
20
Wireless Gateway or Wireless Infrastructure
85/90
Wireless Network
110
15
Mobile Device - User A -
100
220
200
210
215
220
10
15

Fig. 7

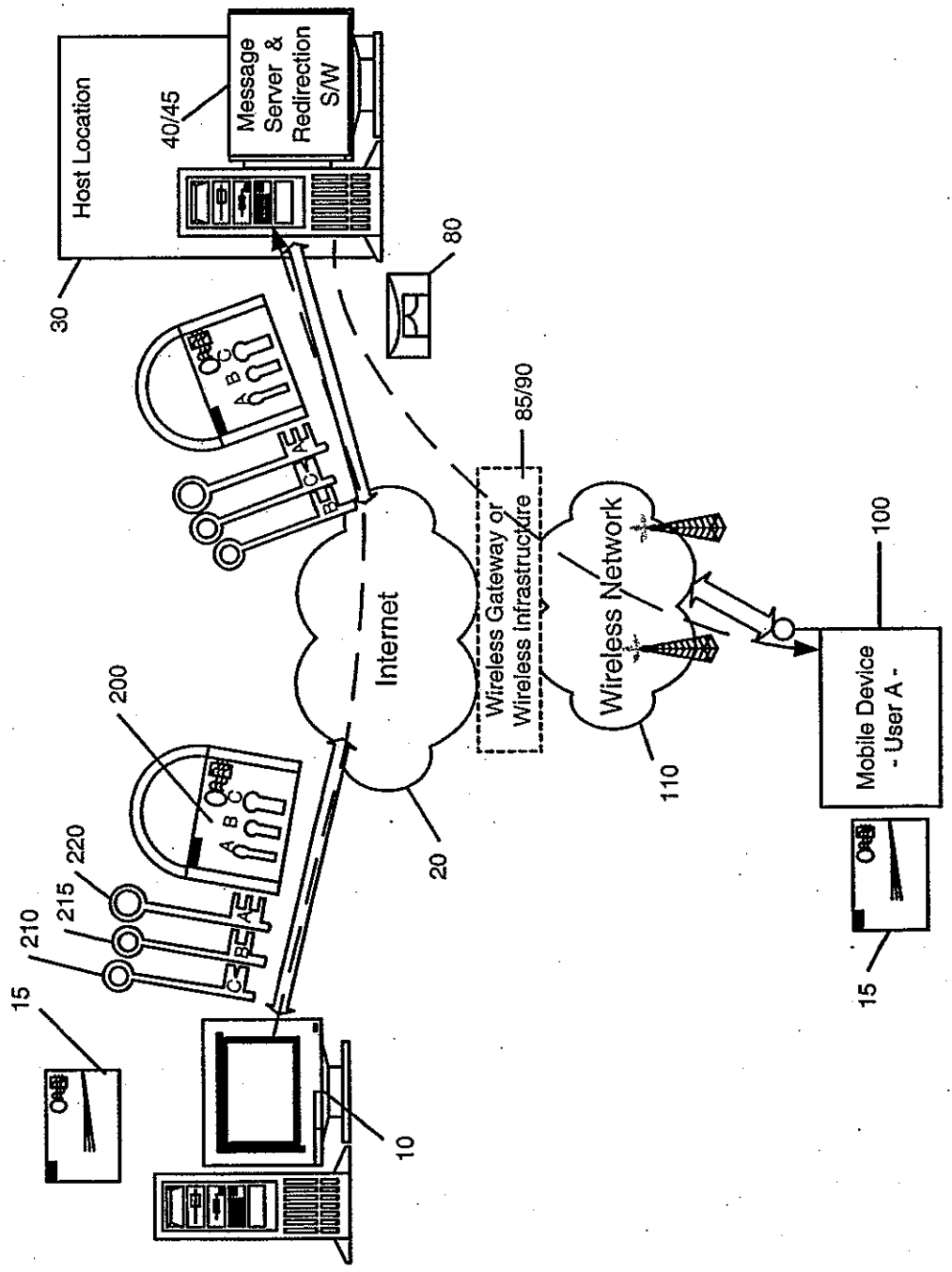

Host Location
40/45
Message Server & Redirection S/W
30
80
85/90
Wireless Gateway or Wireless Infrastructure
Internet
Wireless Network
100
Mobile Device - User A -
110
20
200
220
215
210
15
10
15

Fig. 8

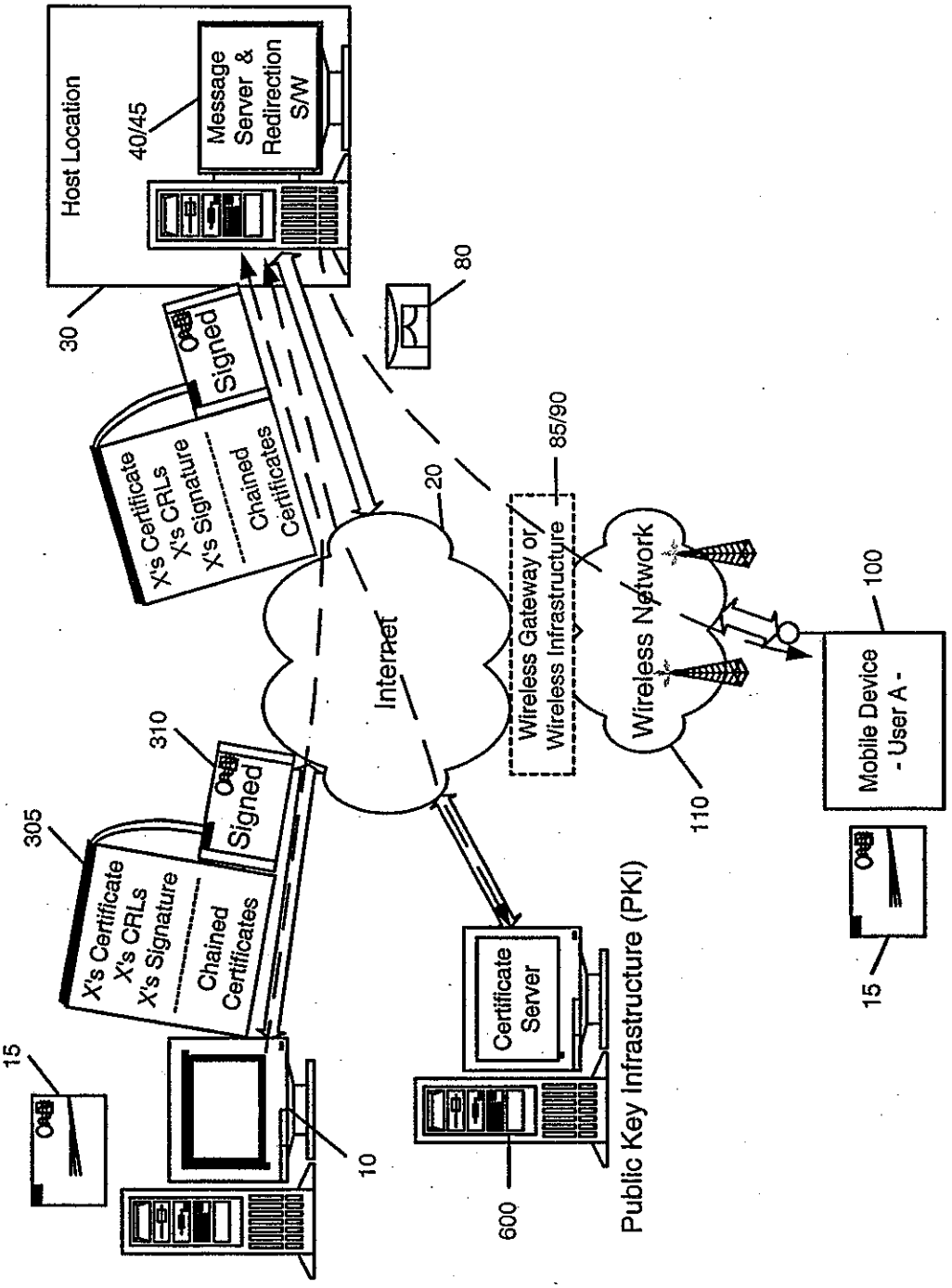

Host Location
40/45
Message Server & Redirection S/W
30
80
X's Certificate
X's CRLs
X's Signature
Chained Certificates
Signed
20
Internet
85/90
Wireless Gateway or Wireless Infrastructure
Wireless Network
110
100
Mobile Device - User A -
15
310
305
X's Certificate
X's CRLs
X's Signature
Chained Certificates
Signed
15
10
Certificate Server
600
Public Key Infrastructure (PKI)

Fig. 9

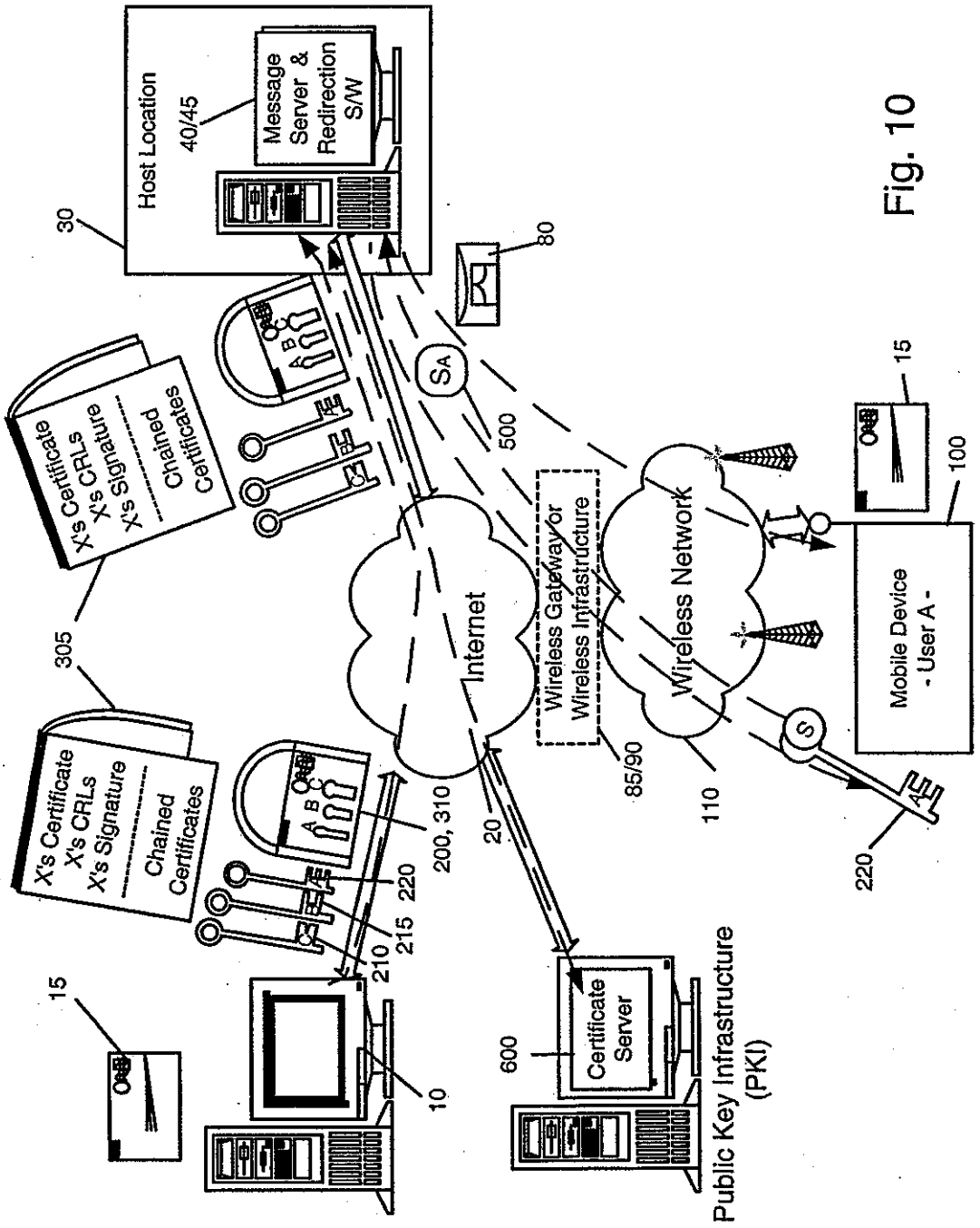

Host Location
40/45
Message Server & Redirection S/W
30
80
SA
500
X's Certificate
X's CRLs
X's Signature
Chained Certificates
305
Internet
Wireless Gateway or Wireless Infrastructure
85/90
Wireless Network
110
15
100
Mobile Device - User A -
S
220
200, 310
20
215
210
10
15
600
Certificate Server
Public Key Infrastructure (PKI)

Fig. 10

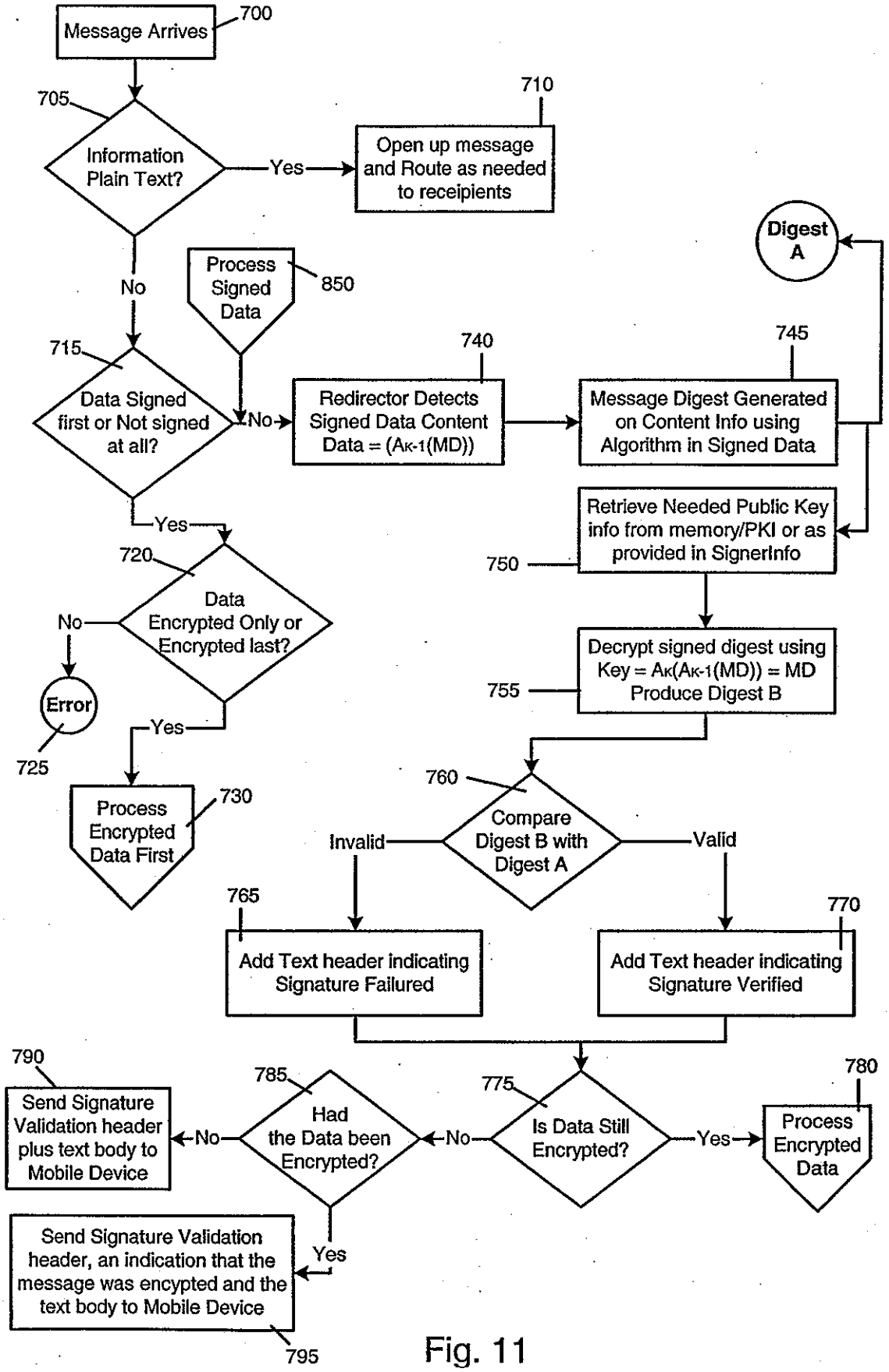

Message Arrives
700
705
Information Plain Text?
Yes
710
Open up message and Route as needed to receipients
No
Process Signed Data
850
Digest A
715
Data Signed first or Not signed at all?
No
740
Redirector Detects Signed Data Content Data = (AK-1(MD))
745
Message Digest Generated on Content Info using Algorithm in Signed Data
Retrieve Needed Public Key info from memory/PKI or as provided in SignerInfo
750
Yes
720
Data Encrypted Only or Encrypted last?
No
Error
725
Yes
Decrypt signed digest using Key = AK(AK-1(MD)) = MD Produce Digest B
755
760
Compare Digest B with Digest A
Invalid
Valid
Process Encrypted Data First
730
765
Add Text header indicating Signature Failured
770
Add Text header indicating Signature Verified
790
Send Signature Validation header plus text body to Mobile Device
785
Had the Data been Encrypted?
No
775
Is Data Still Encrypted?
No
Yes
780
Process Encrypted Data
Send Signature Validation header, an indication that the message was encypted and the text body to Mobile Device
Yes
795

Fig. 11

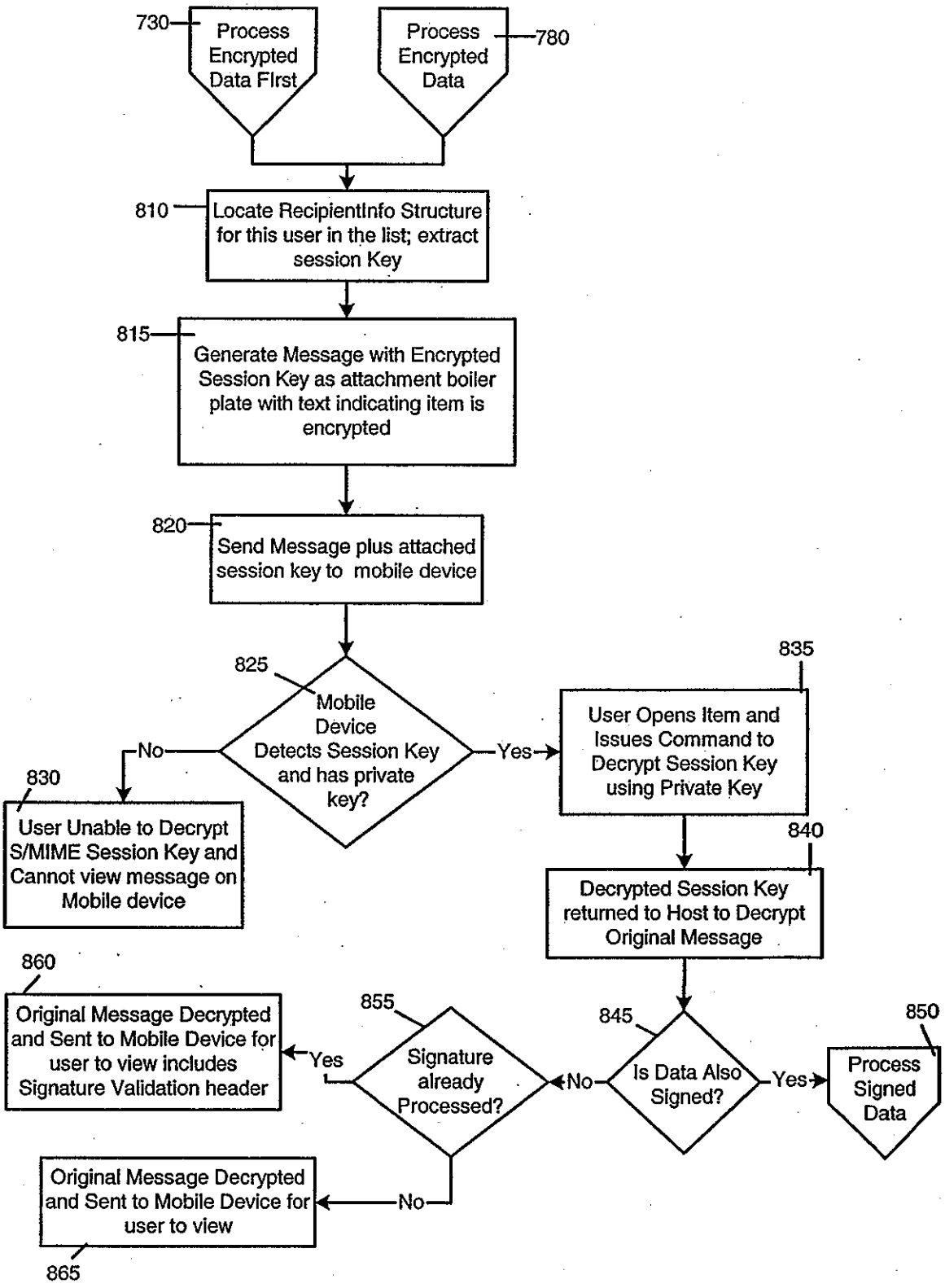

730
Process Encrypted Data FIrst
Process Encrypted Data
780
810
Locate RecipientInfo Structure for this user in the list; extract session Key
815
Generate Message with Encrypted Session Key as attachment boiler plate with text indicating item is encrypted
820
Send Message plus attached session key to mobile device
825
Mobile Device Detects Session Key and has private key?
No
Yes
830
User Unable to Decrypt S/MIME Session Key and Cannot view message on Mobile device
835
User Opens Item and Issues Command to Decrypt Session Key using Private Key
840
Decrypted Session Key returned to Host to Decrypt Original Message
845
Is Data Also Signed?
No
Yes
850
Process Signed Data
855
Signature already Processed?
Yes
No
860
Original Message Decrypted and Sent to Mobile Device for user to view includes Signature Validation header
Original Message Decrypted and Sent to Mobile Device for user to view
865

Fig. 12

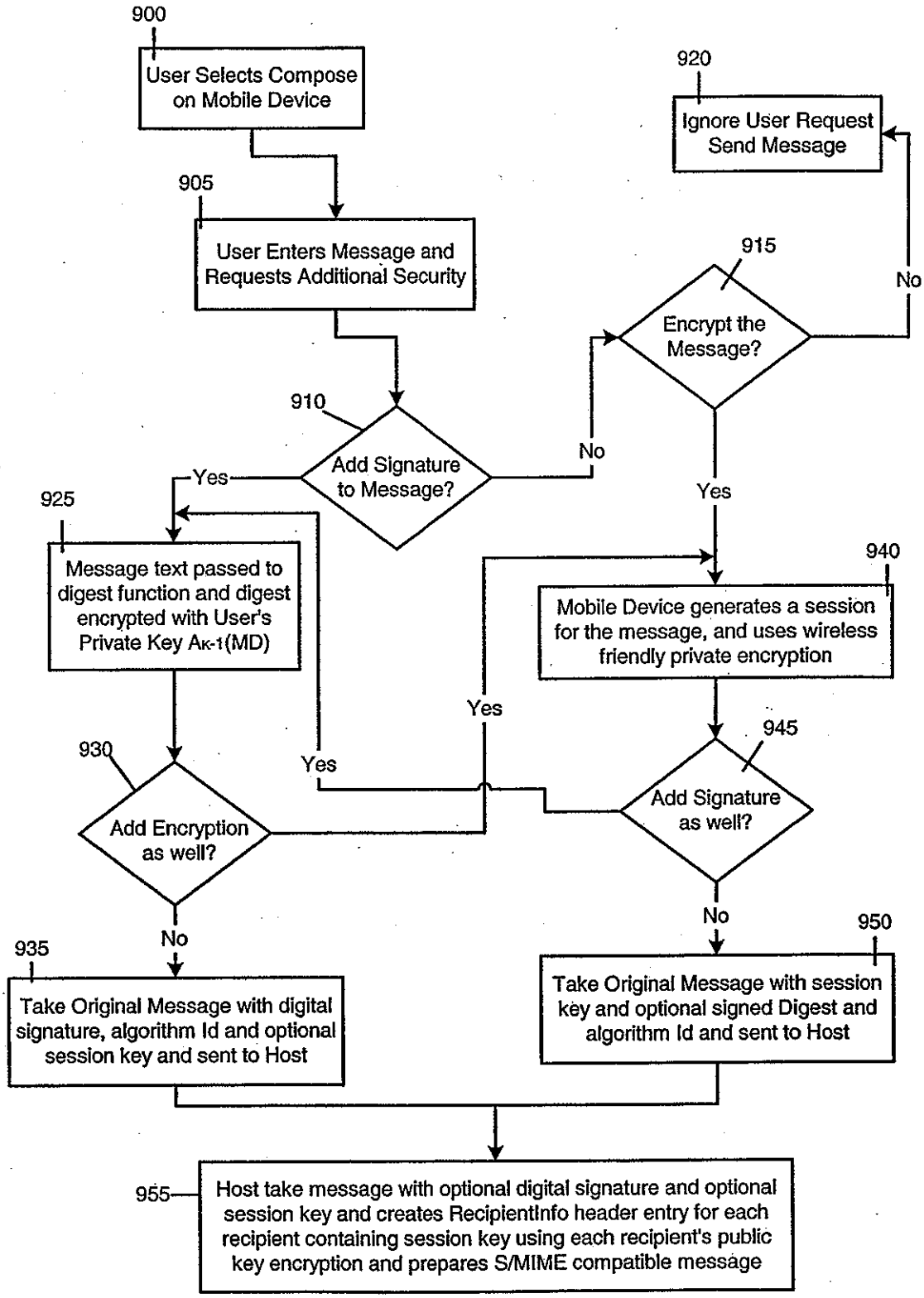

900
User Selects Compose on Mobile Device
905
User Enters Message and Requests Additional Security
910
Add Signature to Message?
Yes
No
925
Message text passed to digest function and digest encrypted with User's Private Key AK-1(MD)
930
Add Encryption as well?
Yes
No
935
Take Original Message with digital signature, algorithm Id and optional session key and sent to Host
915
Encrypt the Message?
No
Yes
920
Ignore User Request Send Message
940
Mobile Device generates a session for the message, and uses wireless friendly private encryption
945
Add Signature as well?
Yes
No
950
Take Original Message with session key and optional signed Digest and algorithm Id and sent to Host
955
Host take message with optional digital signature and optional session key and creates RecipientInfo header entry for each recipient containing session key using each recipient's public key encryption and prepares S/MIME compatible message

Fig. 13

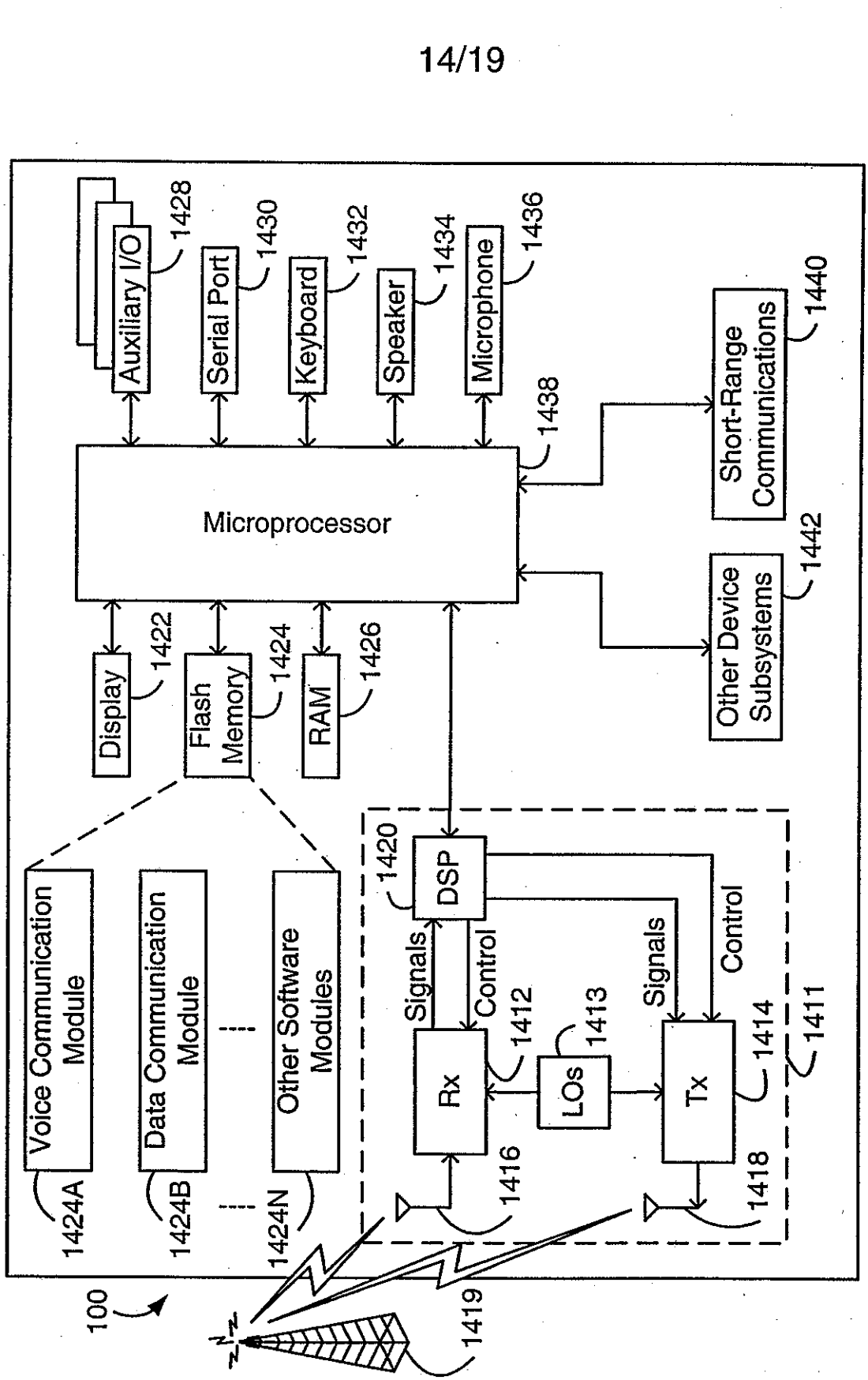

Auxiliary I/O
1428
Serial Port
1430
Keyboard
1432
Speaker
1434
Microphone
1436
1438
Microprocessor
Short-Range Communications
1440
Other Device Subsystems
1442
Display
1422
Flash Memory
1424
RAM
1426
Voice Communication Module
Data Communication Module
Other Software Modules
1424A
1424B
1424N
1420
DSP
Signals
Control
Signals
Control
Rx
1412
LOs
1413
Tx
1414
1411
1416
1418
100
1419

FIG. 14

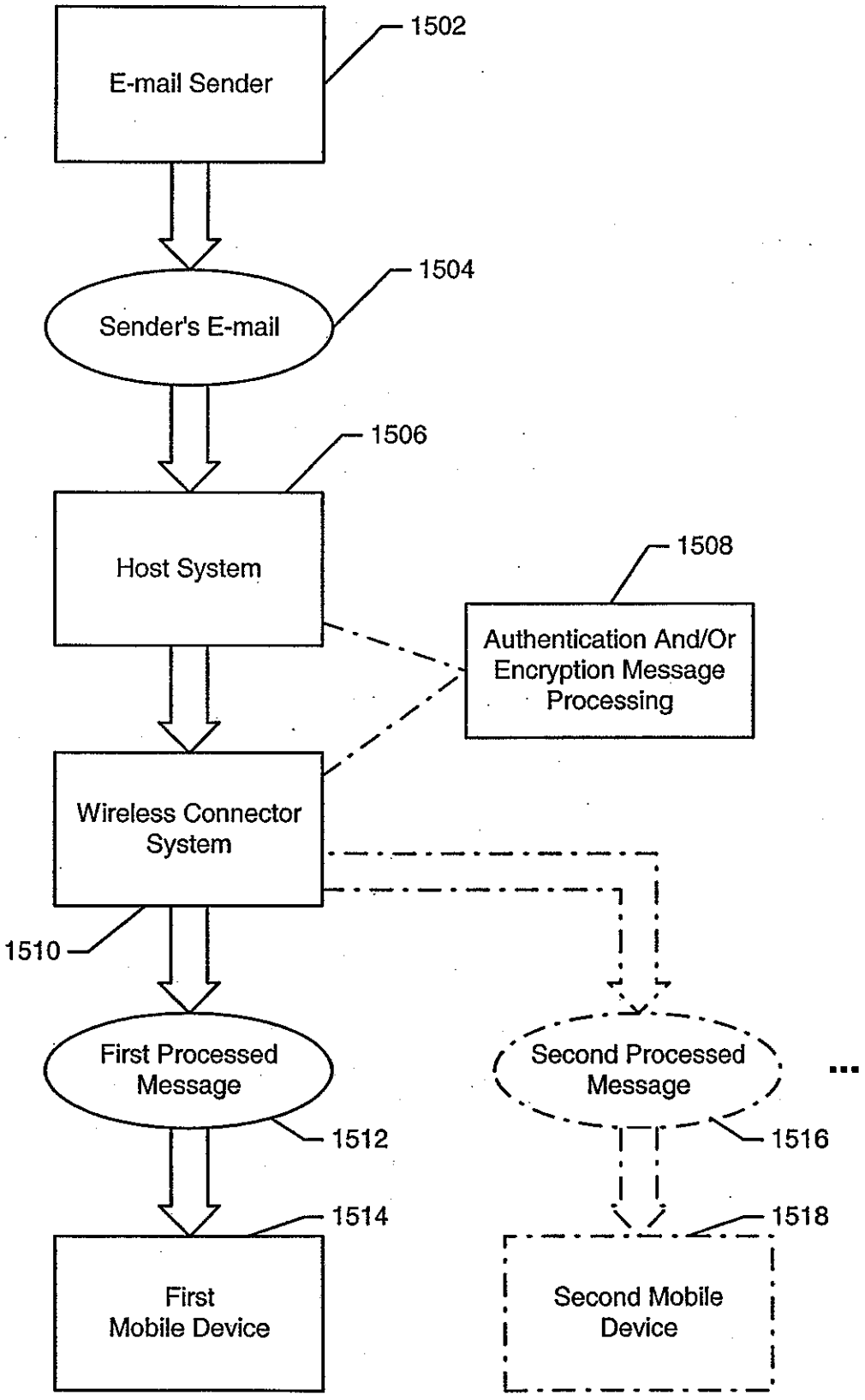

E-mail Sender
1502
Sender's E-mail
1504
1506
Host System
1508
Authentication And/Or Encryption Message Processing
Wireless Connector System
1510
First Processed Message
1512
Second Processed Message
1516
...
1514
1518
First Mobile Device
Second Mobile Device

Fig. 15

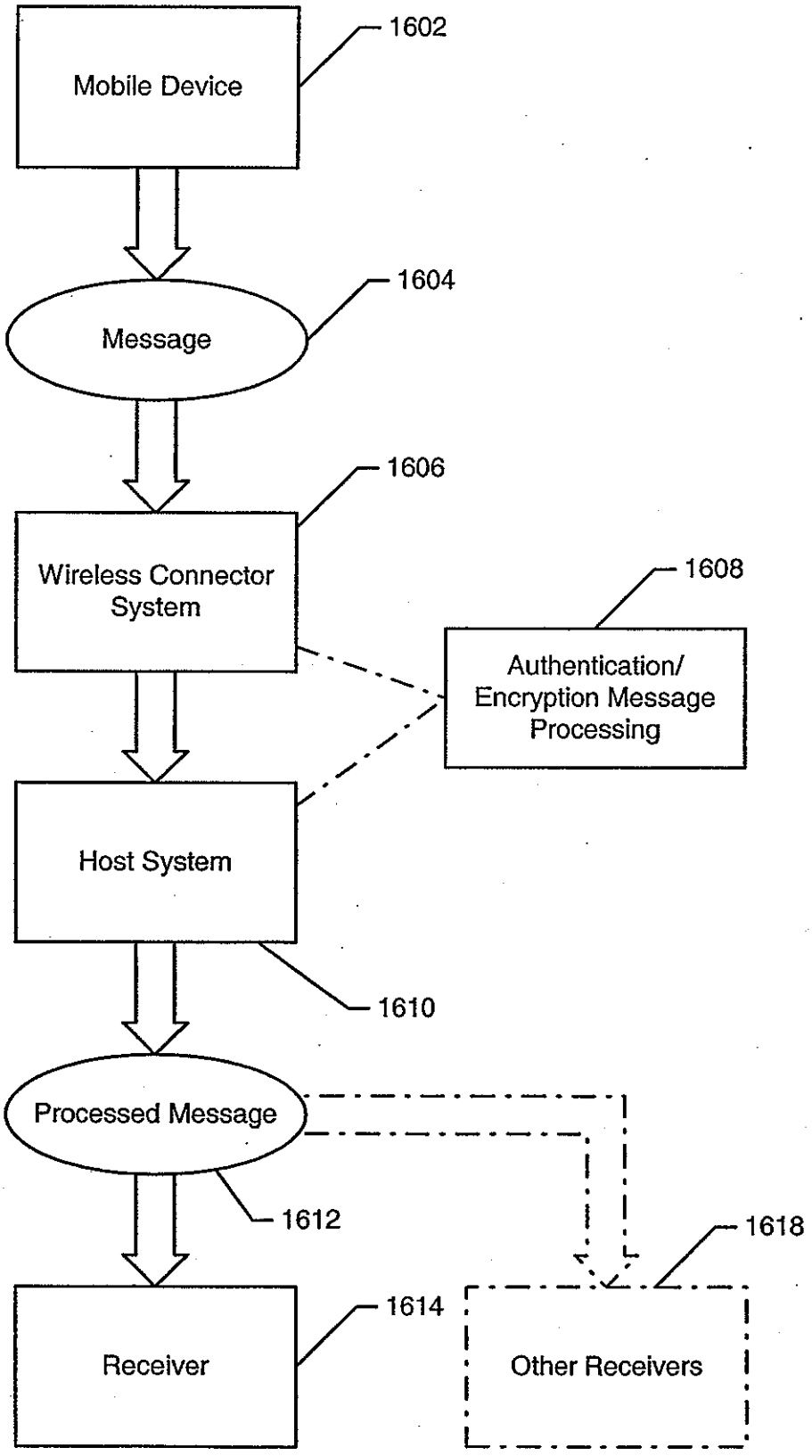

Mobile Device
1602
Message
1604
Wireless Connector System
1606
Authentication/ Encryption Message Processing
1608
Host System
1610
Processed Message
1612
Receiver
1614
Other Receivers
1618

Fig. 16

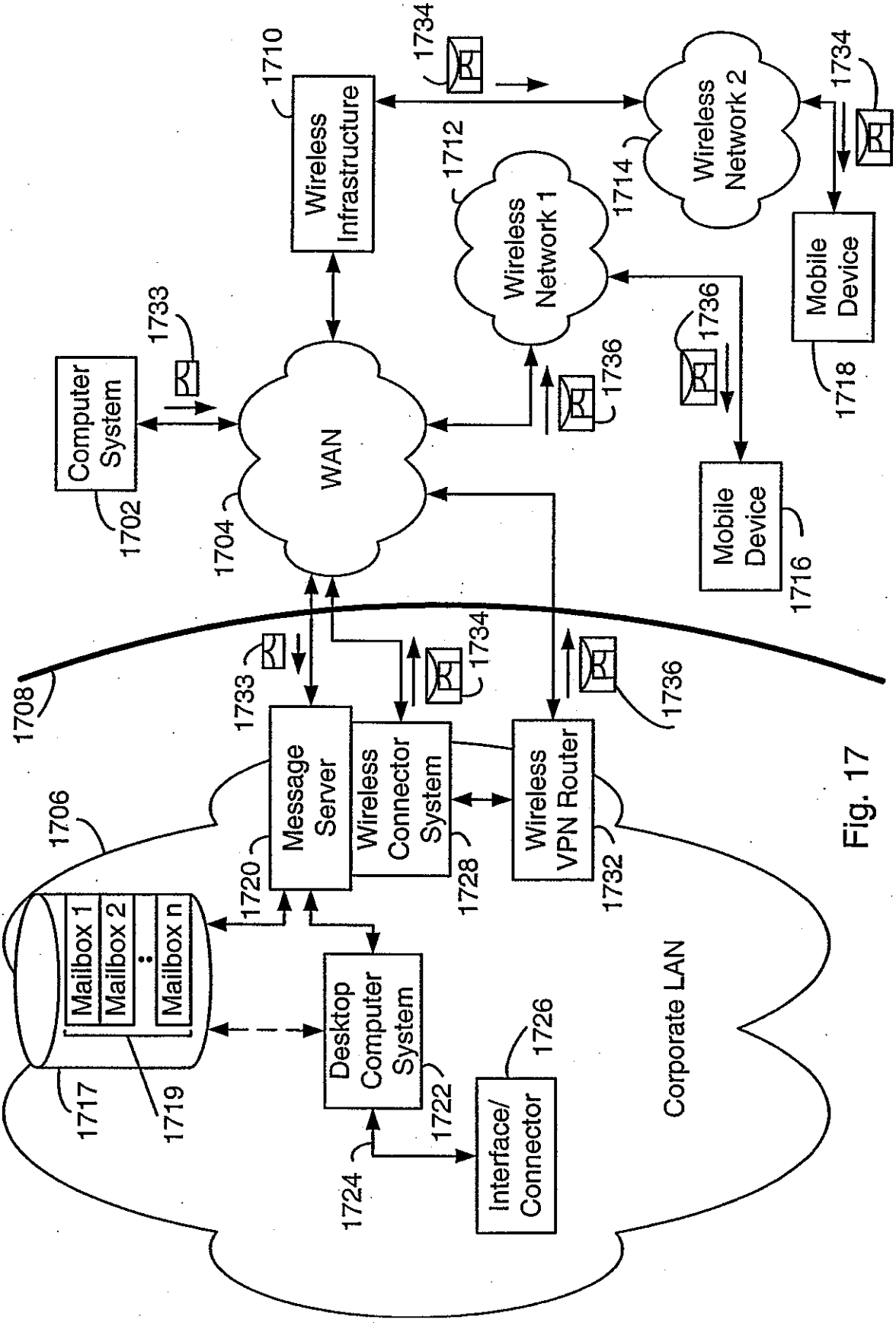

Wireless Infrastructure
1710
1734
Wireless Network 2
1714
1734
Wireless Network 1
1712
Mobile Device
1718
1736
1736
Computer System
1733
1702
WAN
1704
Mobile Device
1716
1708
1733
1734
1736
Message Server
1720
Wireless Connector System
1728
Wireless VPN Router
1732
1706
Mailbox 1
Mailbox 2
Mailbox n
1717
1719
Desktop Computer System
1722
1724
Interface/ Connector
1726
Corporate LAN

Fig. 17

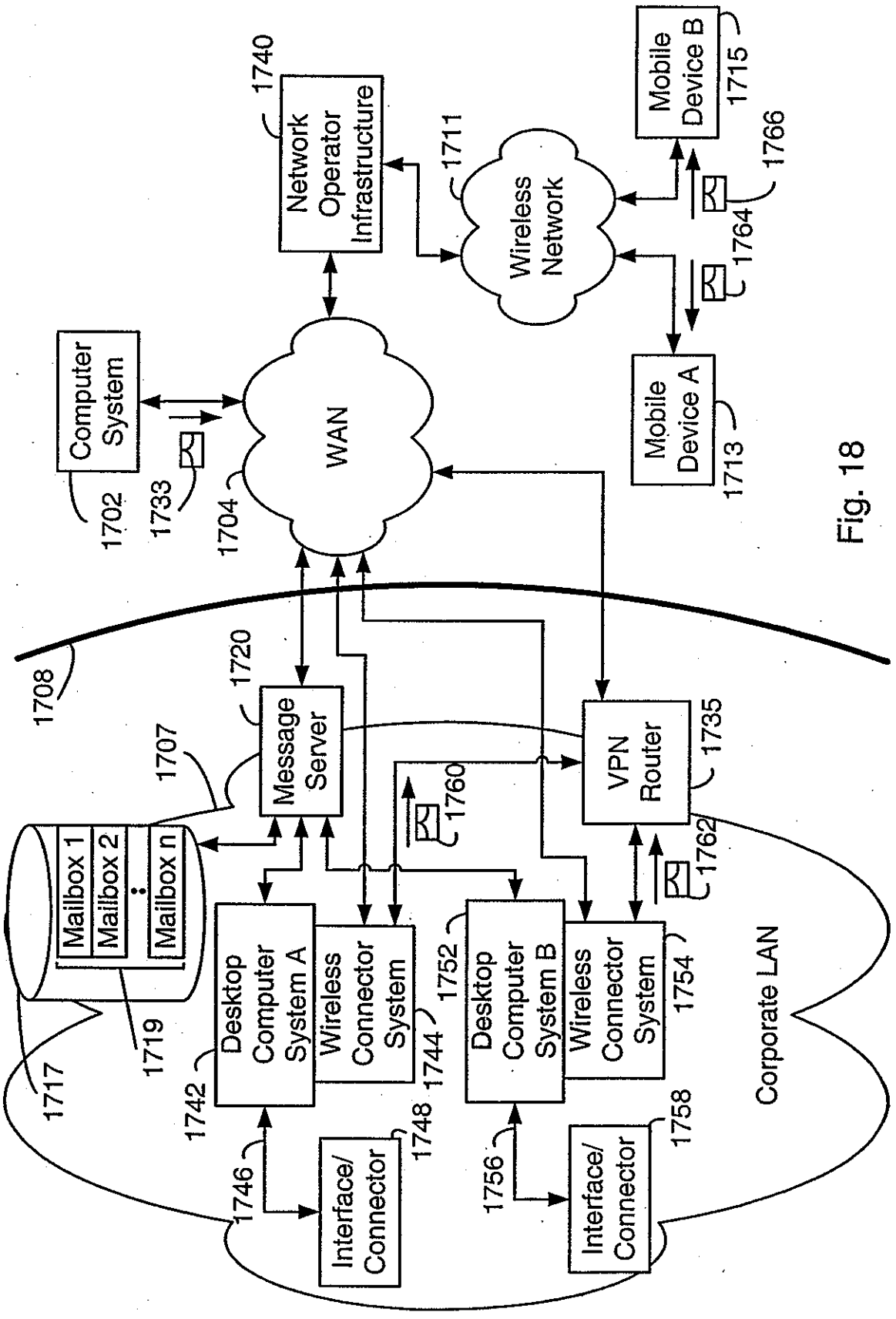

Corporate LAN
1708
1717
Mailbox 1
Mailbox 2
Mailbox n
1719
1707
Message Server
1720
Desktop Computer System A
1742
Wireless Connector System
1744
Desktop Computer System B
1752
Wireless Connector System
1754
VPN Router
1735
1760
1762
Interface/ Connector
1746
1748
Interface/ Connector
1756
1758
WAN
1704
Computer System
1702
1733
Network Operator Infrastructure
1740
Wireless Network
1711
Mobile Device A
1713
Mobile Device B
1715
1764
1766

Fig. 18

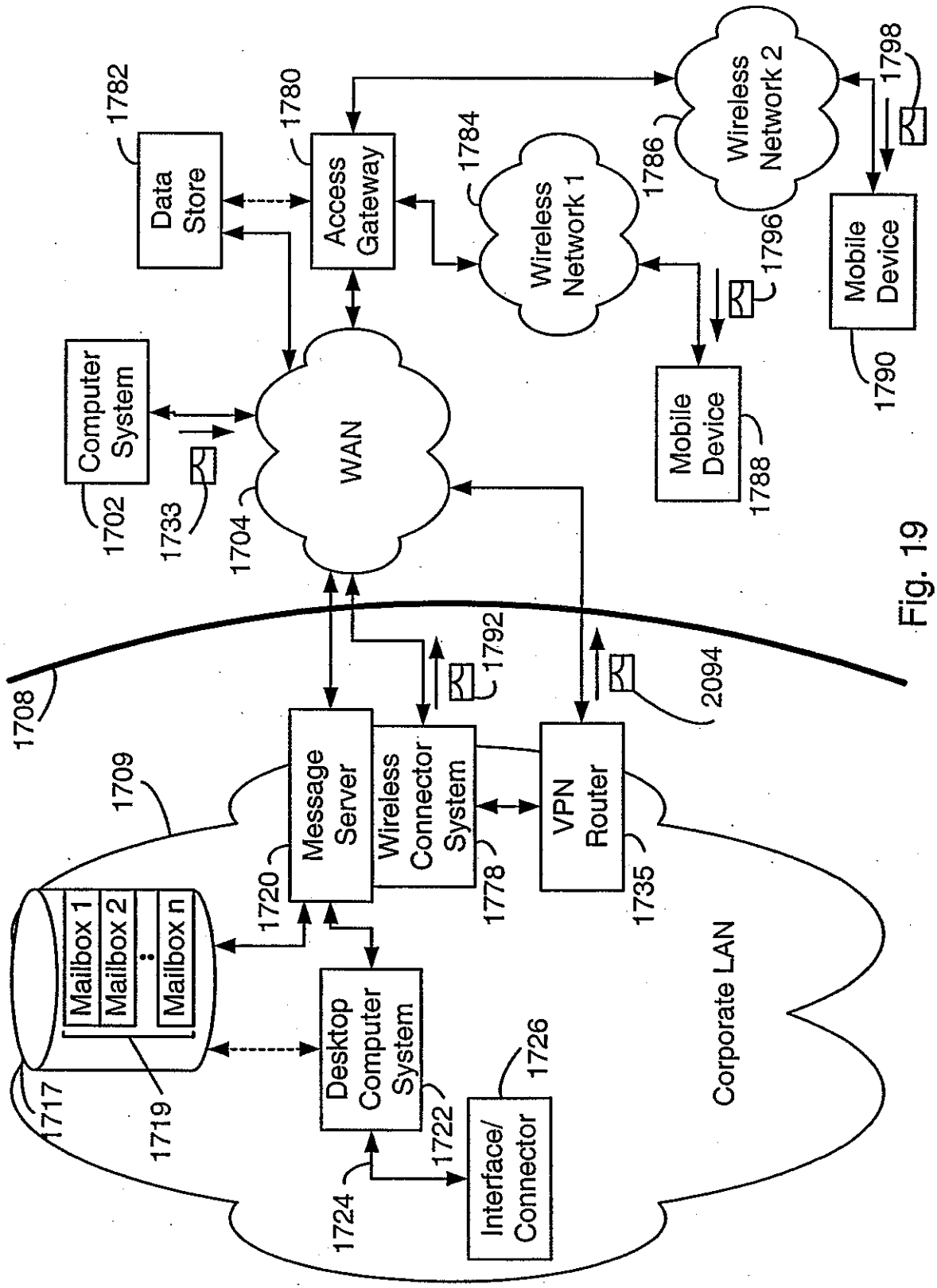

Data Store
1782
Access Gateway
1780
Wireless Network 1
1784
Wireless Network 2
1786
1798
Mobile Device
1796
1790
Computer System
1702
1733
WAN
1704
Mobile Device
1788
1708
1792
2094
1709
Message Server
1720
Wireless Connector System
1778
VPN Router
1735
Mailbox 1
Mailbox 2
Mailbox n
1717
1719
Desktop Computer System
1722
1724
Interface/ Connector
1726
Corporate LAN

Fig. 19