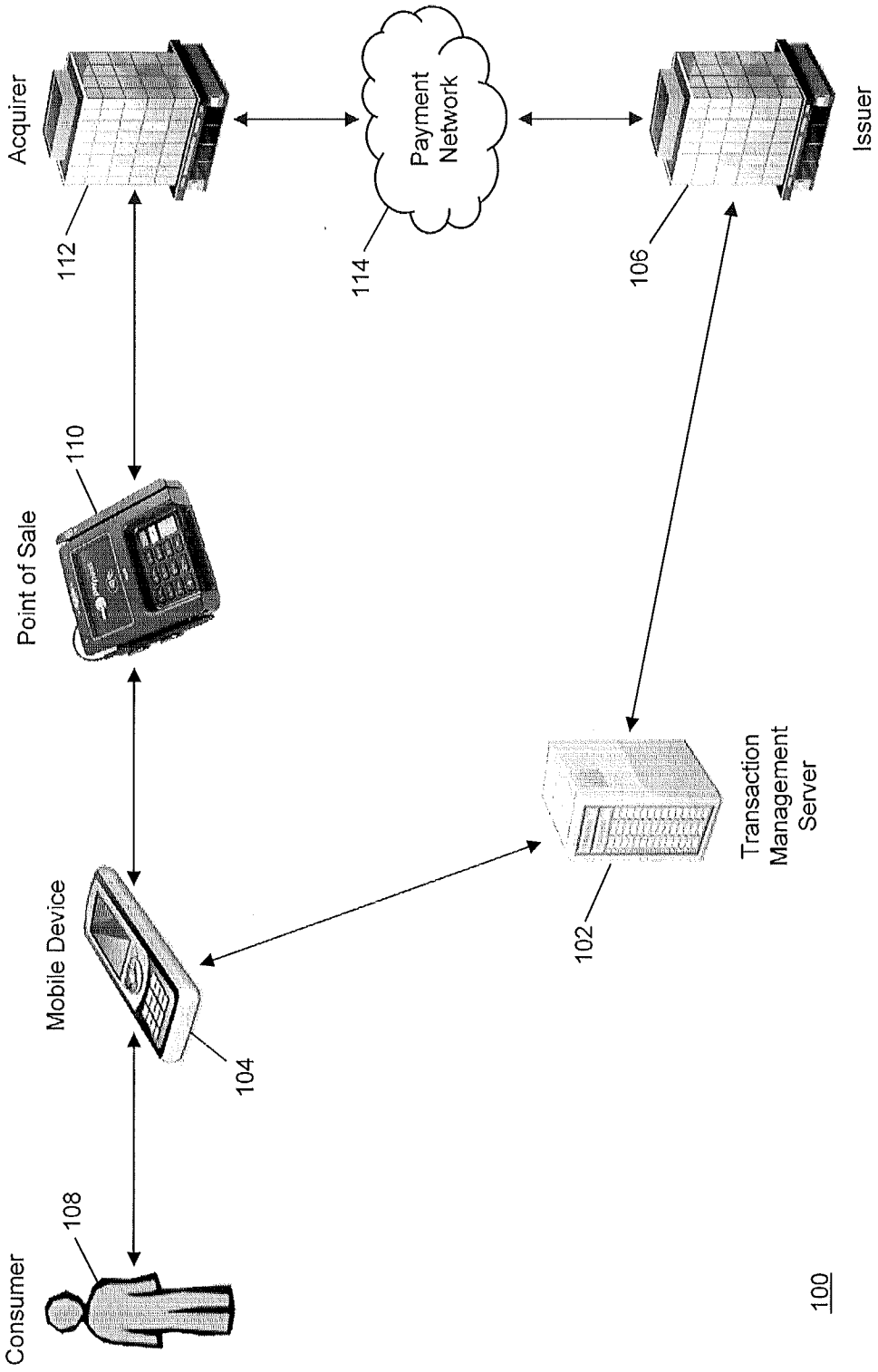

Acquirer
112
Payment Network
114
Issuer
106
Point of Sale
110
Mobile Device
104
Transaction Management Server
102
Consumer
108
100

FIG. 1

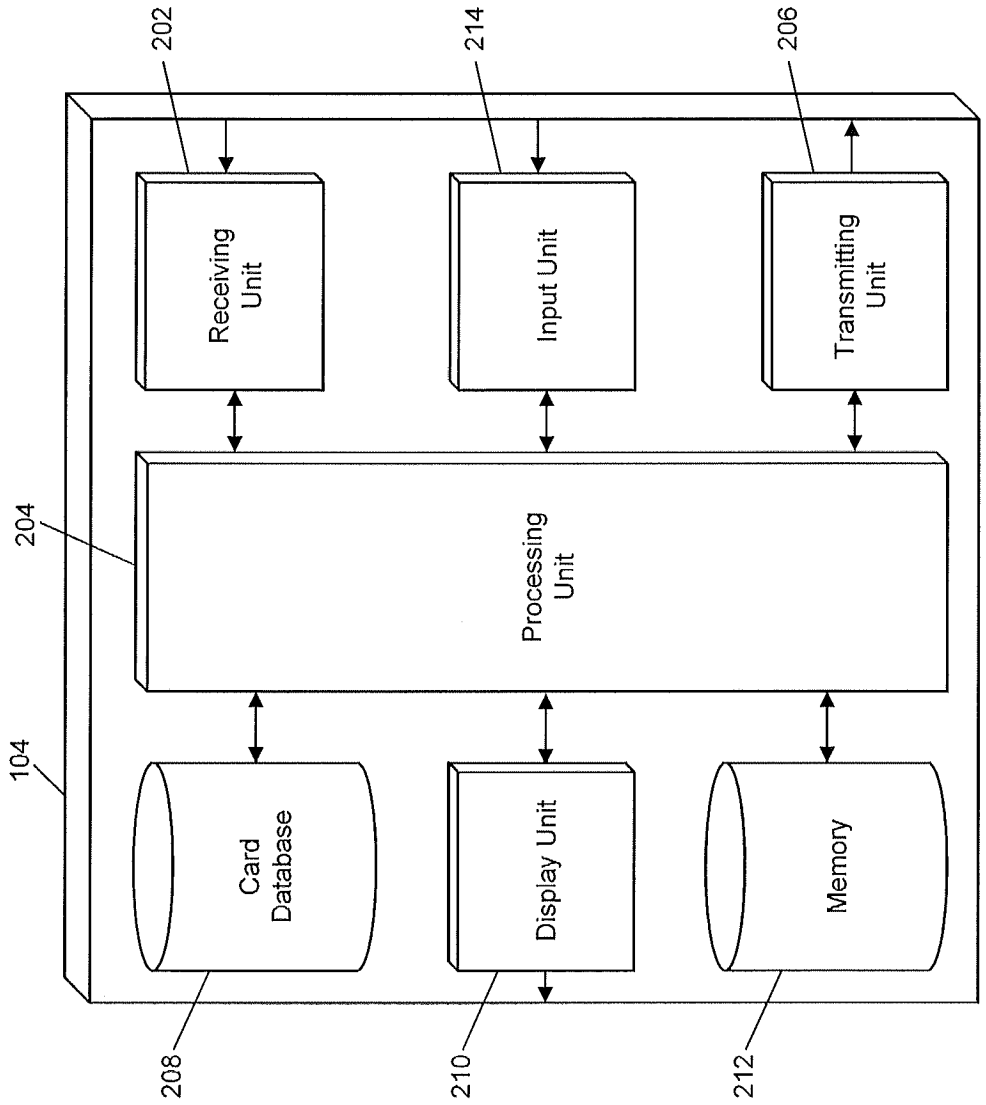

202
214
206
Receiving Unit
Input Unit
Transmitting Unit
204
Processing Unit
104
Card Database
Display Unit
Memory
208
210
212

FIG. 2

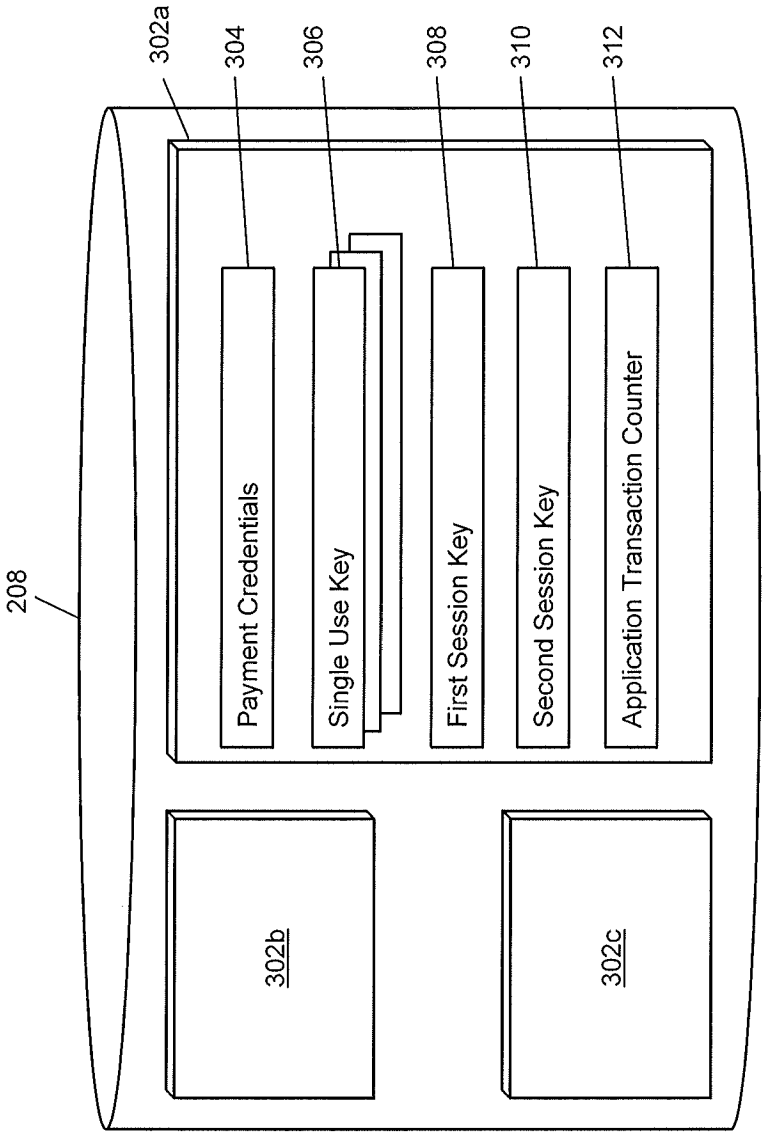

208
302a
304
306
308
310
312
Payment Credentials
Single Use Key
First Session Key
Second Session Key
Application Transaction Counter
302b
302c

FIG. 3

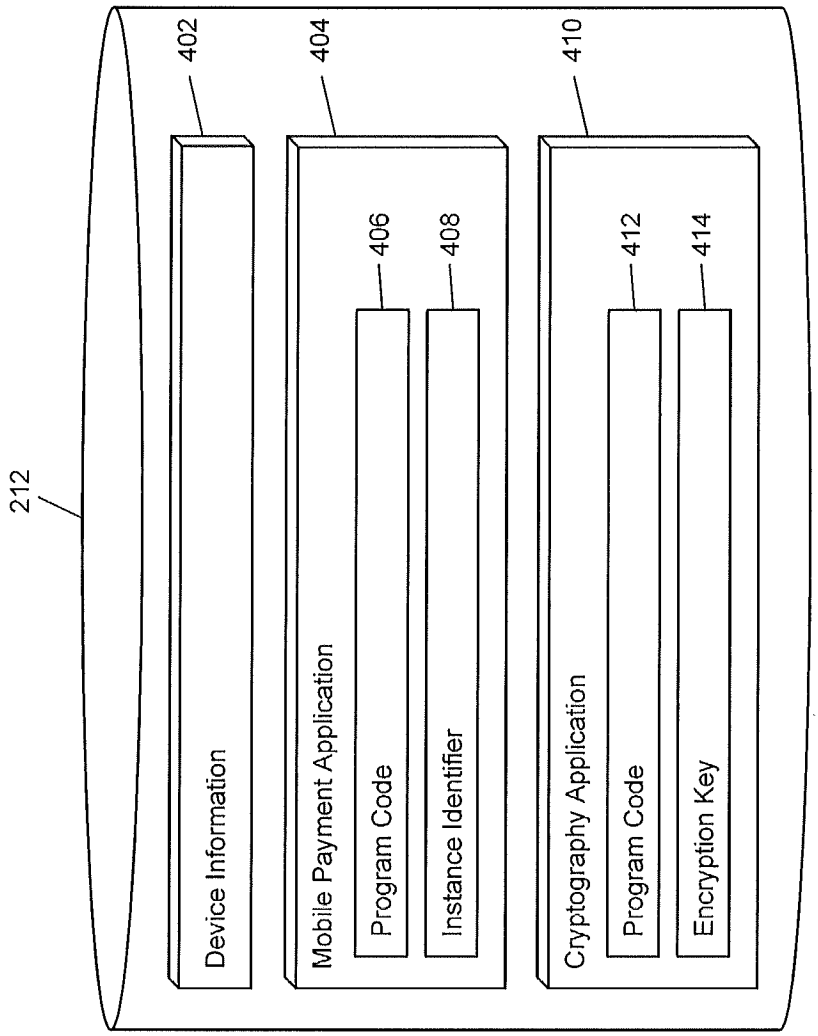

212
402
Device Information
404
Mobile Payment Application
406
Program Code
408
Instance Identifier
410
Cryptography Application
412
Program Code
414
Encryption Key

FIG. 4

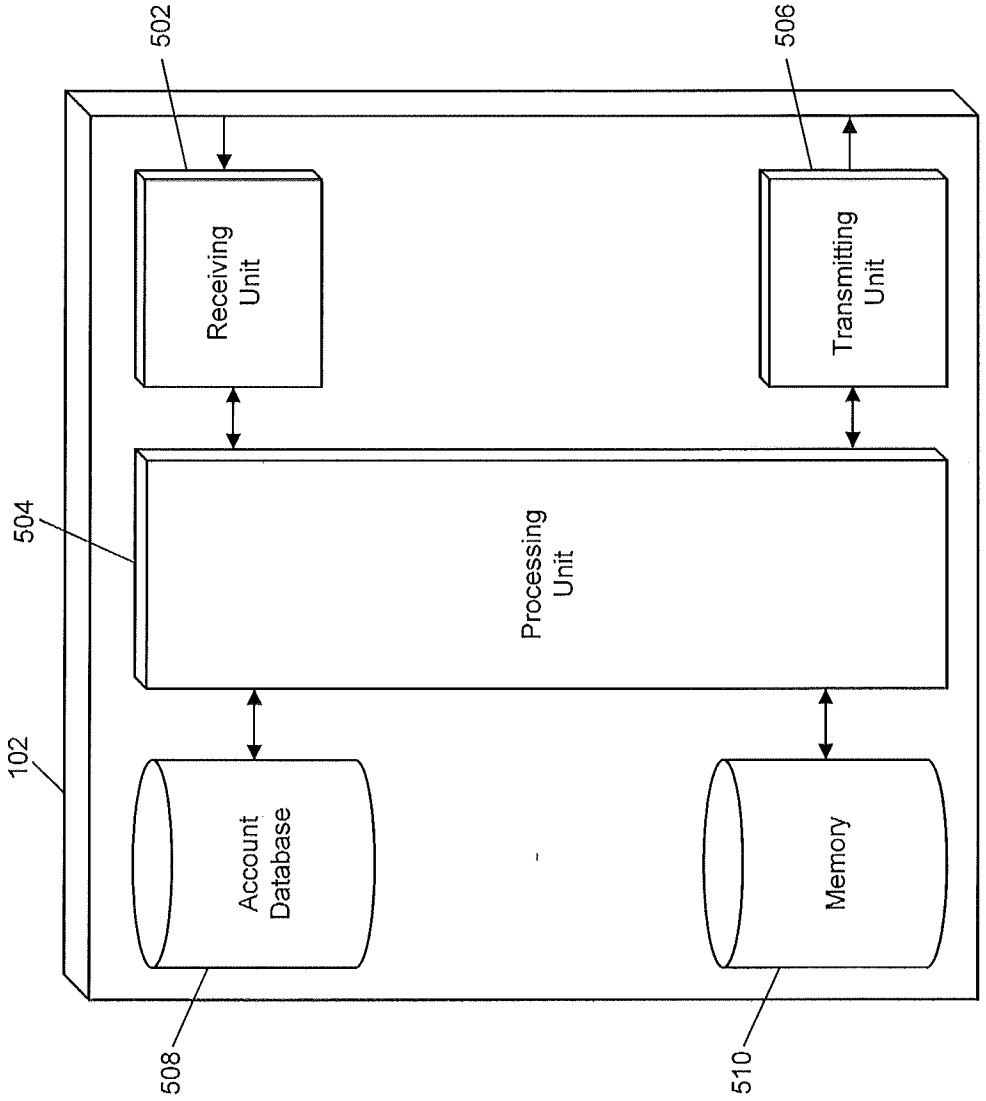

502
506
Receiving Unit
Transmitting Unit
504
Processing Unit
102
Account Database
Memory
508
510

FIG. 5

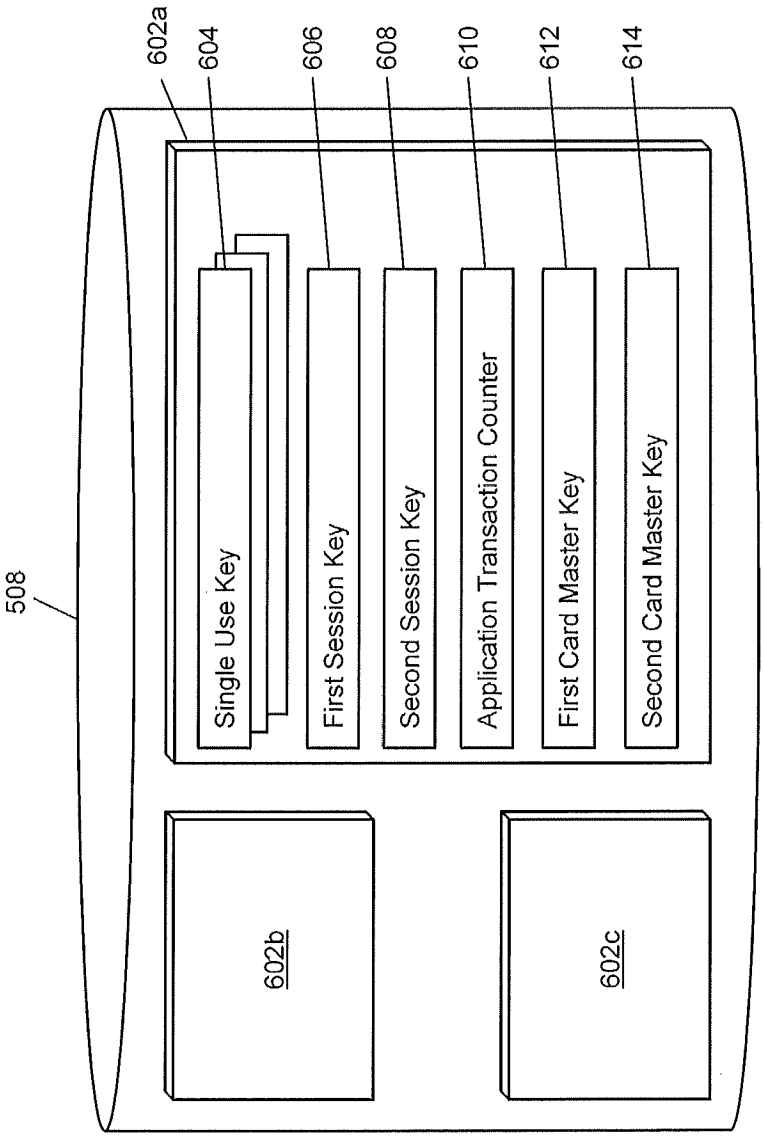

508
602a
604
606
608
610
612
614
Single Use Key
First Session Key
Second Session Key
Application Transaction Counter
First Card Master Key
Second Card Master Key
602b
602c

FIG. 6

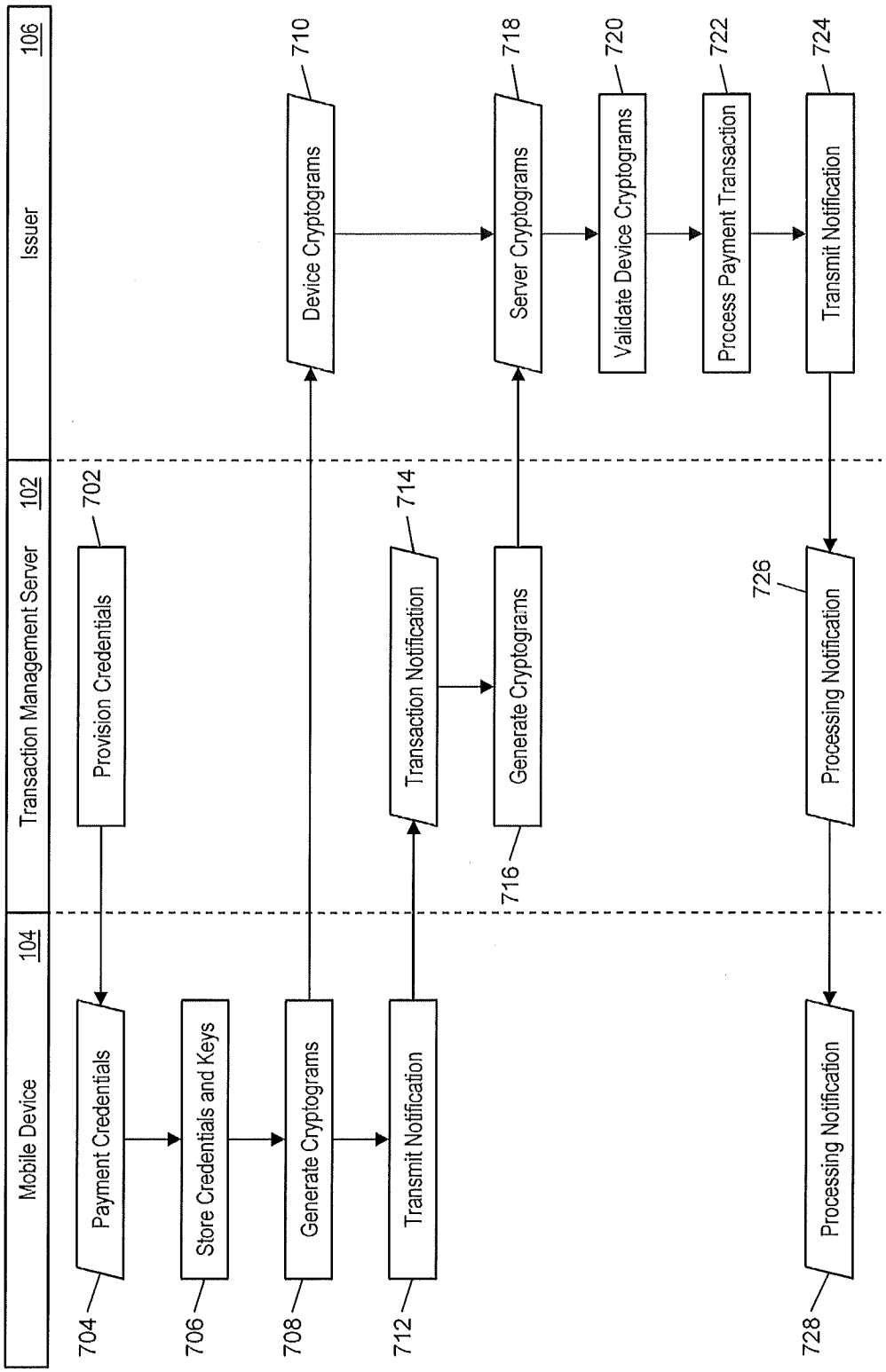

Mobile Device 104
Transaction Management Server 102
Issuer 106
Payment Credentials
Provision Credentials
Store Credentials and Keys
Generate Cryptograms
Transmit Notification
Device Cryptograms
Transaction Notification
Generate Cryptograms
Server Cryptograms
Validate Device Cryptograms
Process Payment Transaction
Transmit Notification
Processing Notification
Processing Notification
702
704
706
708
710
712
714
716
718
720
722
724
726
728

FIG. 7

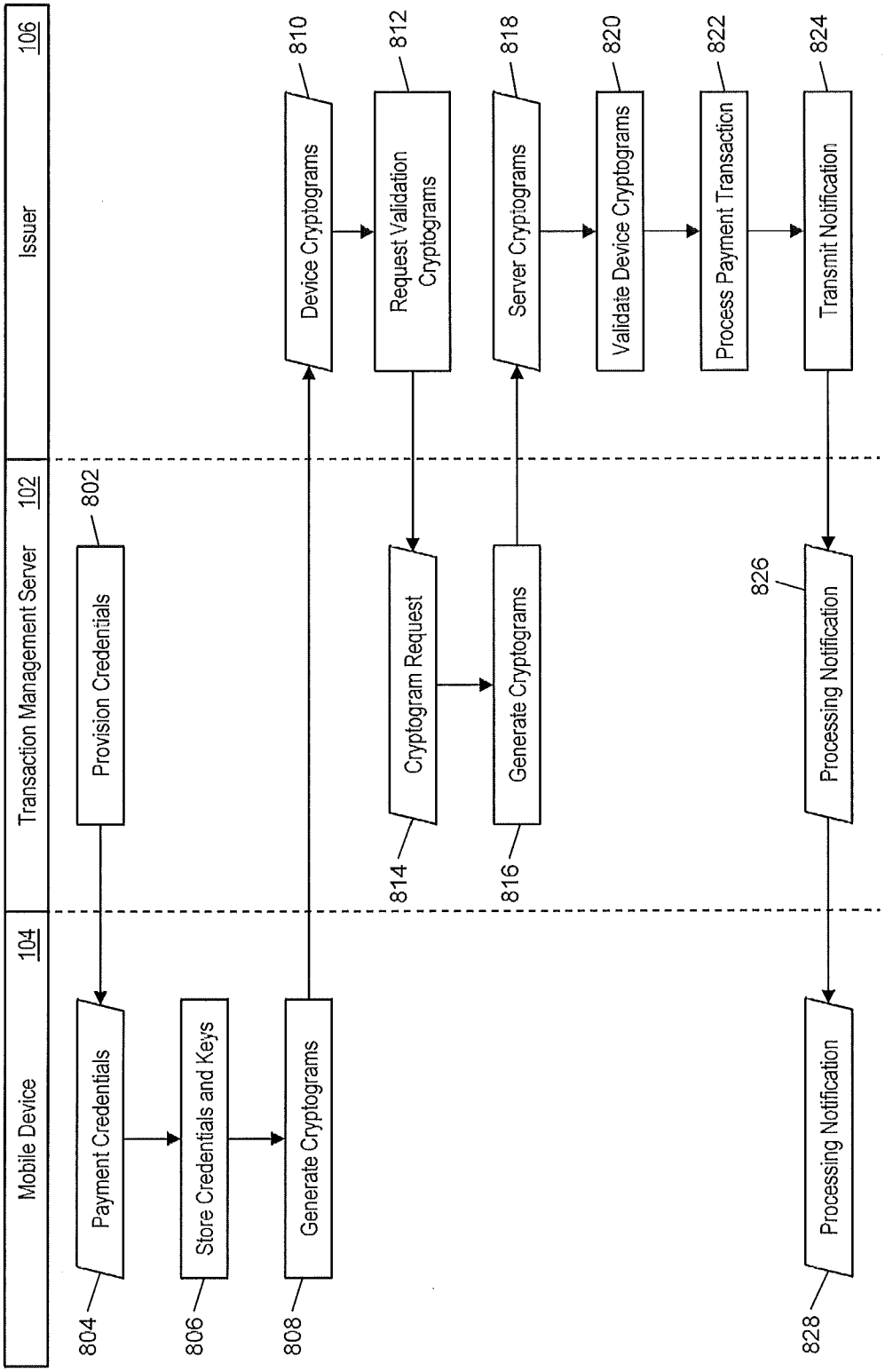

Mobile Device 104
Transaction Management Server 102
Issuer 106
Provision Credentials
802
Payment Credentials
804
Store Credentials and Keys
806
Generate Cryptograms
808
Device Cryptograms
810
Request Validation Cryptograms
812
Cryptogram Request
814
Generate Cryptograms
816
Server Cryptograms
818
Validate Device Cryptograms
820
Process Payment Transaction
822
Transmit Notification
824
Processing Notification
826
Processing Notification
828

FIG. 8

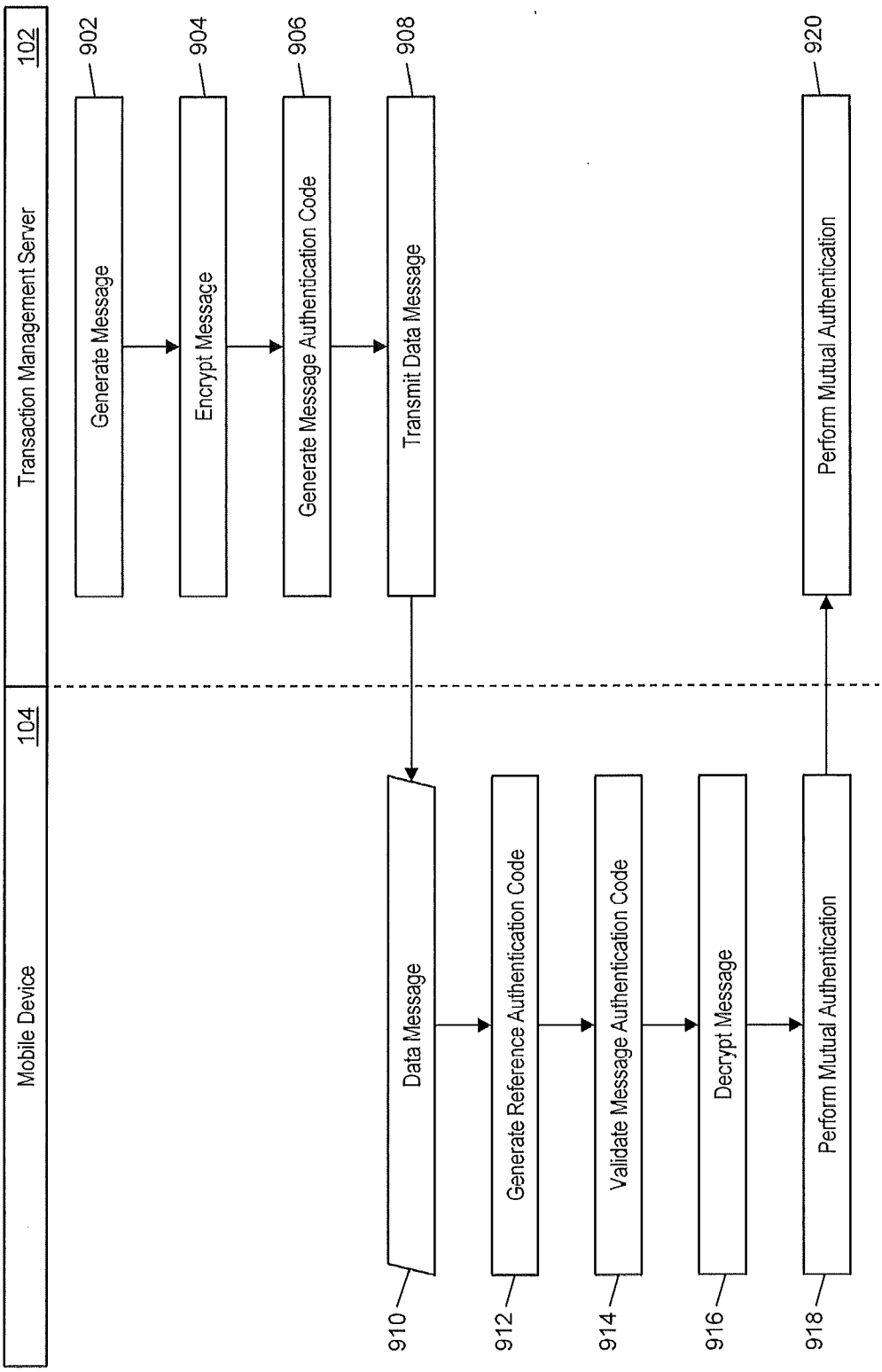

Transaction Management Server
102
Mobile Device
104
902
Generate Message
904
Encrypt Message
906
Generate Message Authentication Code
908
Transmit Data Message
920
Perform Mutual Authentication
910
Data Message
912
Generate Reference Authentication Code
914
Validate Message Authentication Code
916
Decrypt Message
918
Perform Mutual Authentication

FIG. 9

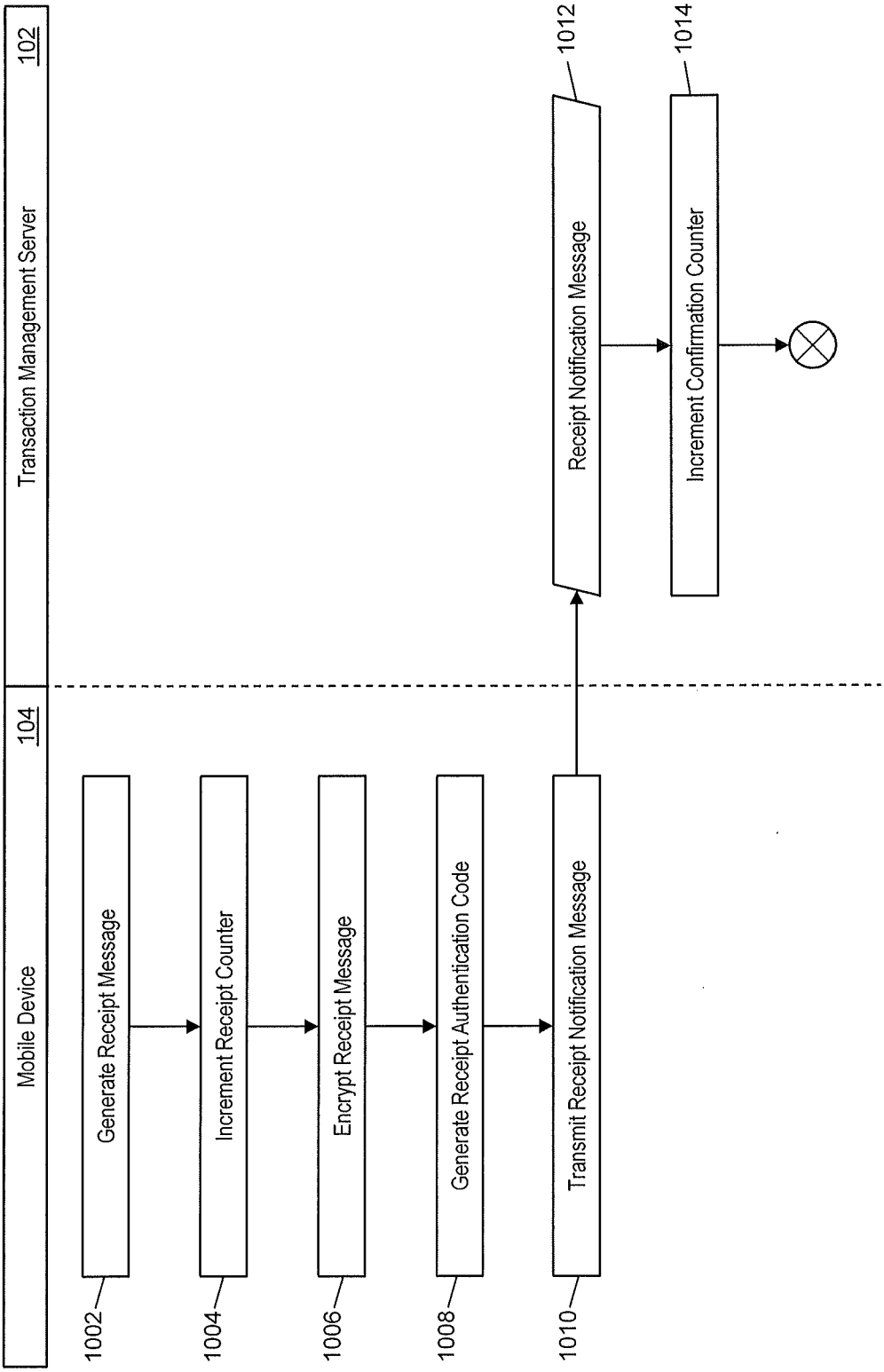

Mobile Device
104
Transaction Management Server
102
Generate Receipt Message
Increment Receipt Counter
Encrypt Receipt Message
Generate Receipt Authentication Code
Transmit Receipt Notification Message
Receipt Notification Message
Increment Confirmation Counter
1002
1004
1006
1008
1010
1012
1014

FIG. 10A

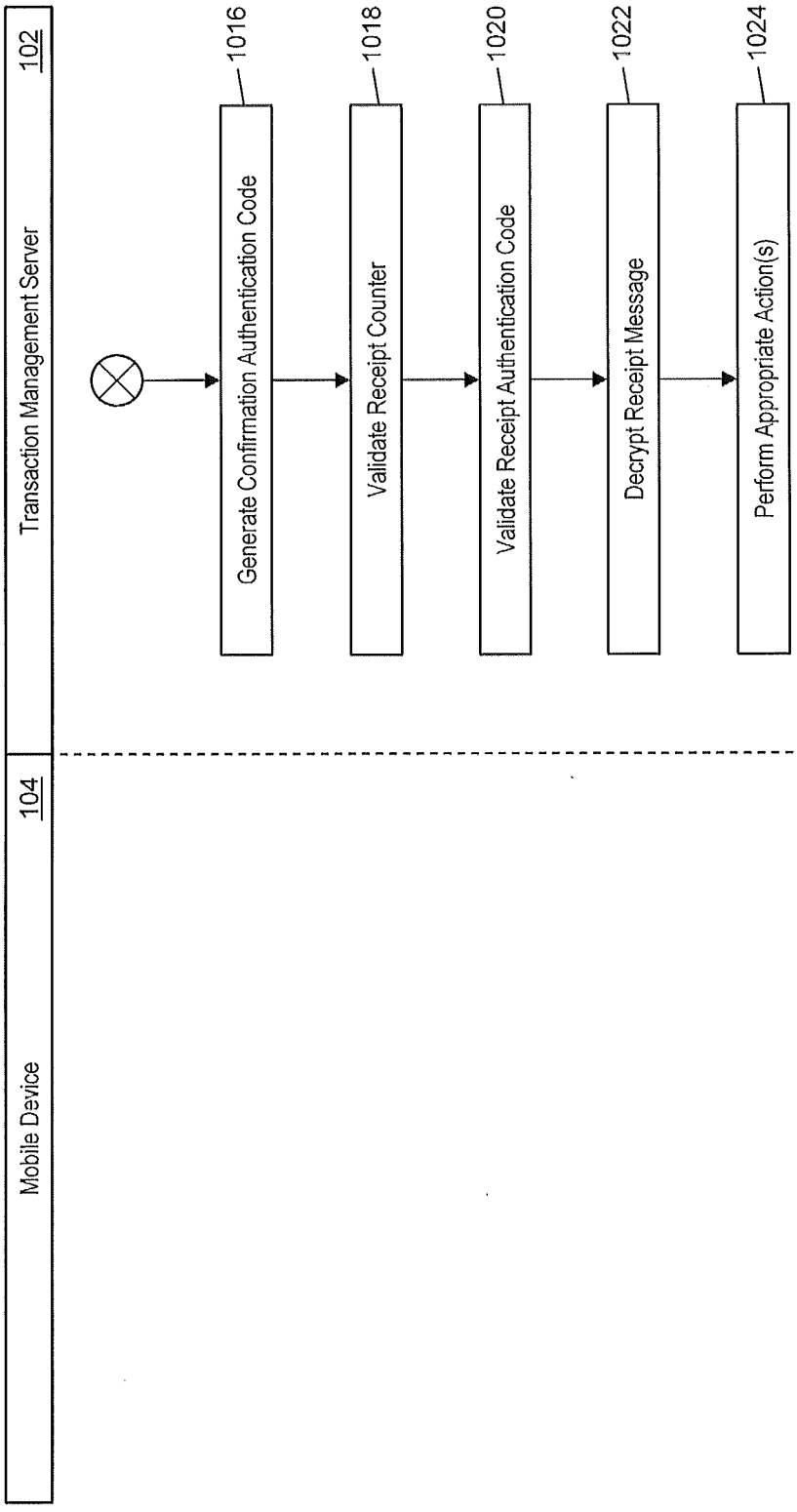

Mobile Device
104
Transaction Management Server
102
1016
Generate Confirmation Authentication Code
1018
Validate Receipt Counter
1020
Validate Receipt Authentication Code
1022
Decrypt Receipt Message
1024
Perform Appropriate Action(s)

FIG. 10B

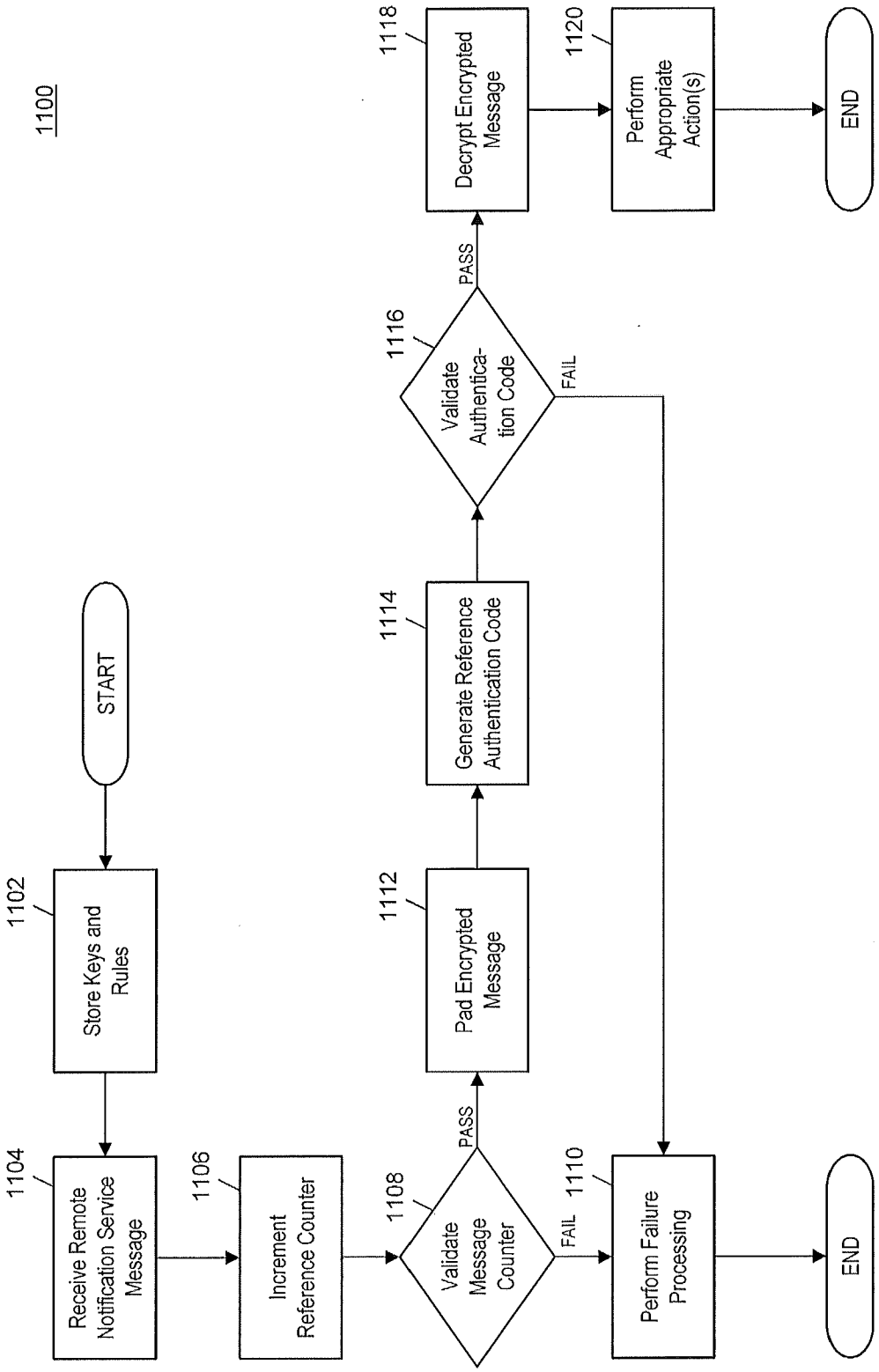

1100
START
1102
Store Keys and Rules
1104
Receive Remote Notification Service Message
1106
Increment Reference Counter
1108
Validate Message Counter
PASS
FAIL
1110
Perform Failure Processing
END
1112
Pad Encrypted Message
1114
Generate Reference Authentication Code
1116
Validate Authentication Code
PASS
FAIL
1118
Decrypt Encrypted Message
1120
Perform Appropriate Action(s)
END

FIG. 11

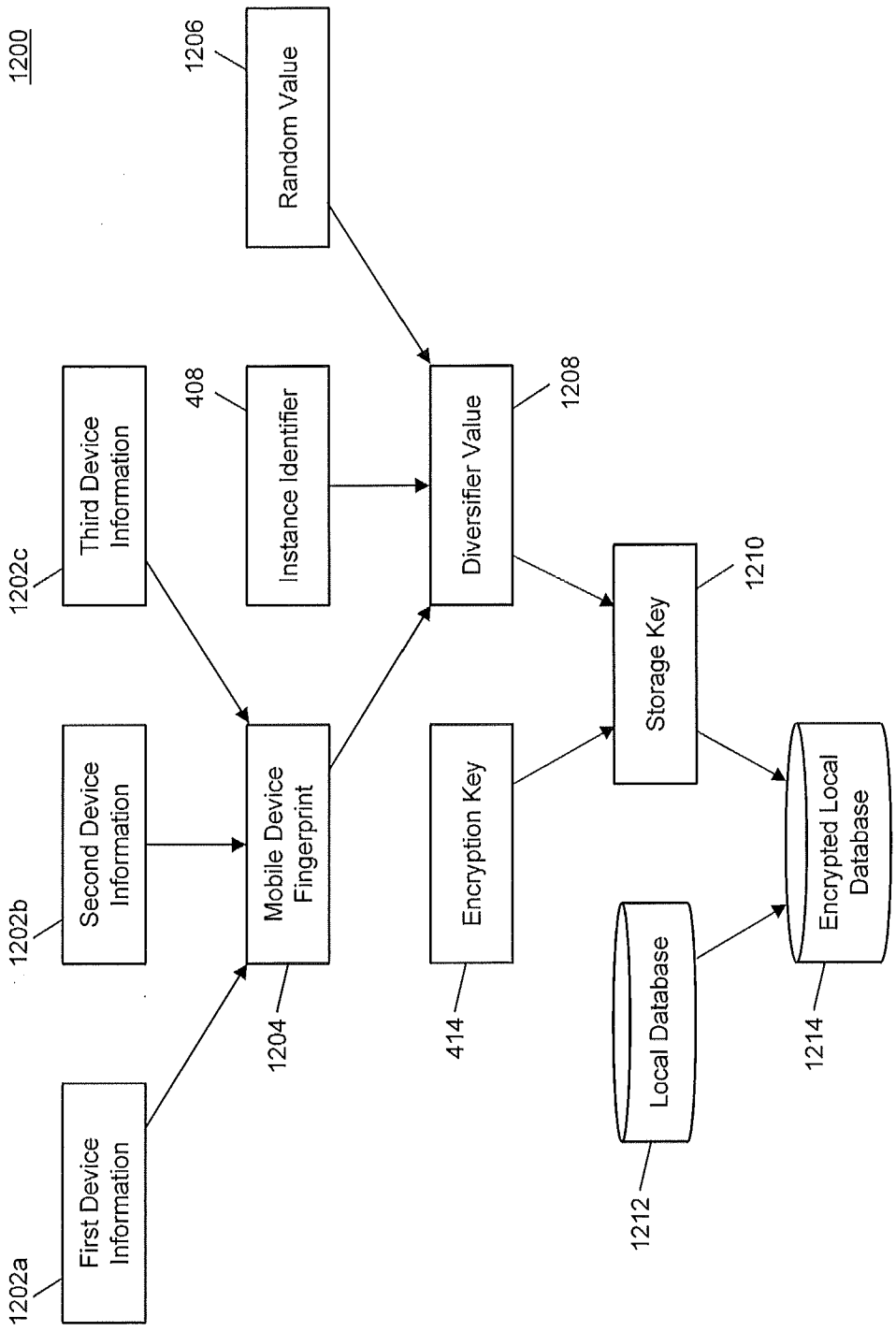

1200
1206
Random Value
408
Instance Identifier
1208
Diversifier Value
1202c
Third Device Information
1202b
Second Device Information
1202a
First Device Information
Mobile Device Fingerprint
1204
Encryption Key
414
Storage Key
1210
Local Database
1212
Encrypted Local Database
1214

FIG. 12

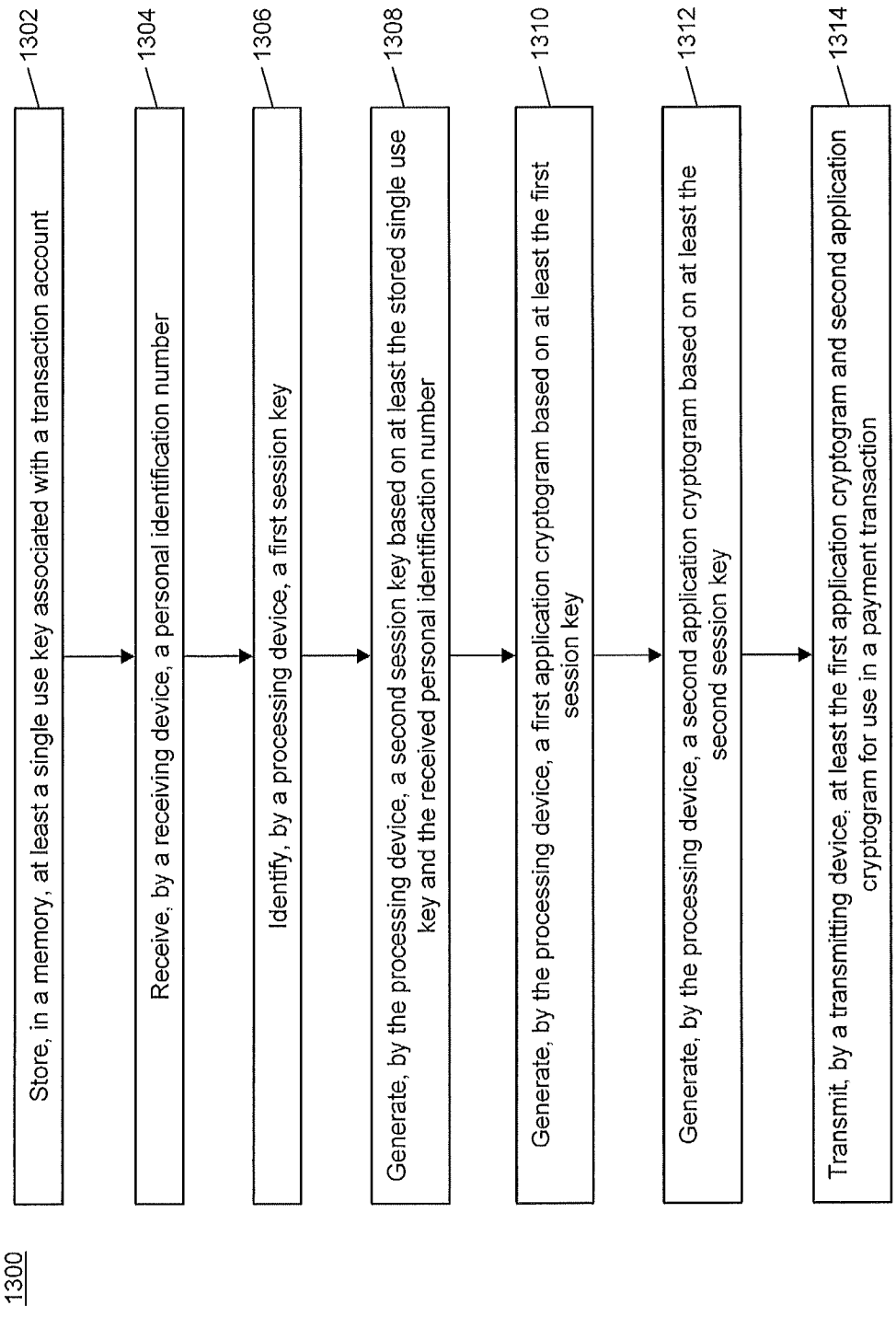

1300
1302
Store, in a memory, at least a single use key associated with a transaction account
1304
Receive, by a receiving device, a personal identification number
1306
Identify, by a processing device, a first session key
1308
Generate, by the processing device, a second session key based on at least the stored single use key and the received personal identification number
1310
Generate, by the processing device, a first application cryptogram based on at least the first session key
1312
Generate, by the processing device, a second application cryptogram based on at least the second session key
1314
Transmit, by a transmitting device, at least the first application cryptogram and second application cryptogram for use in a payment transaction

FIG. 13

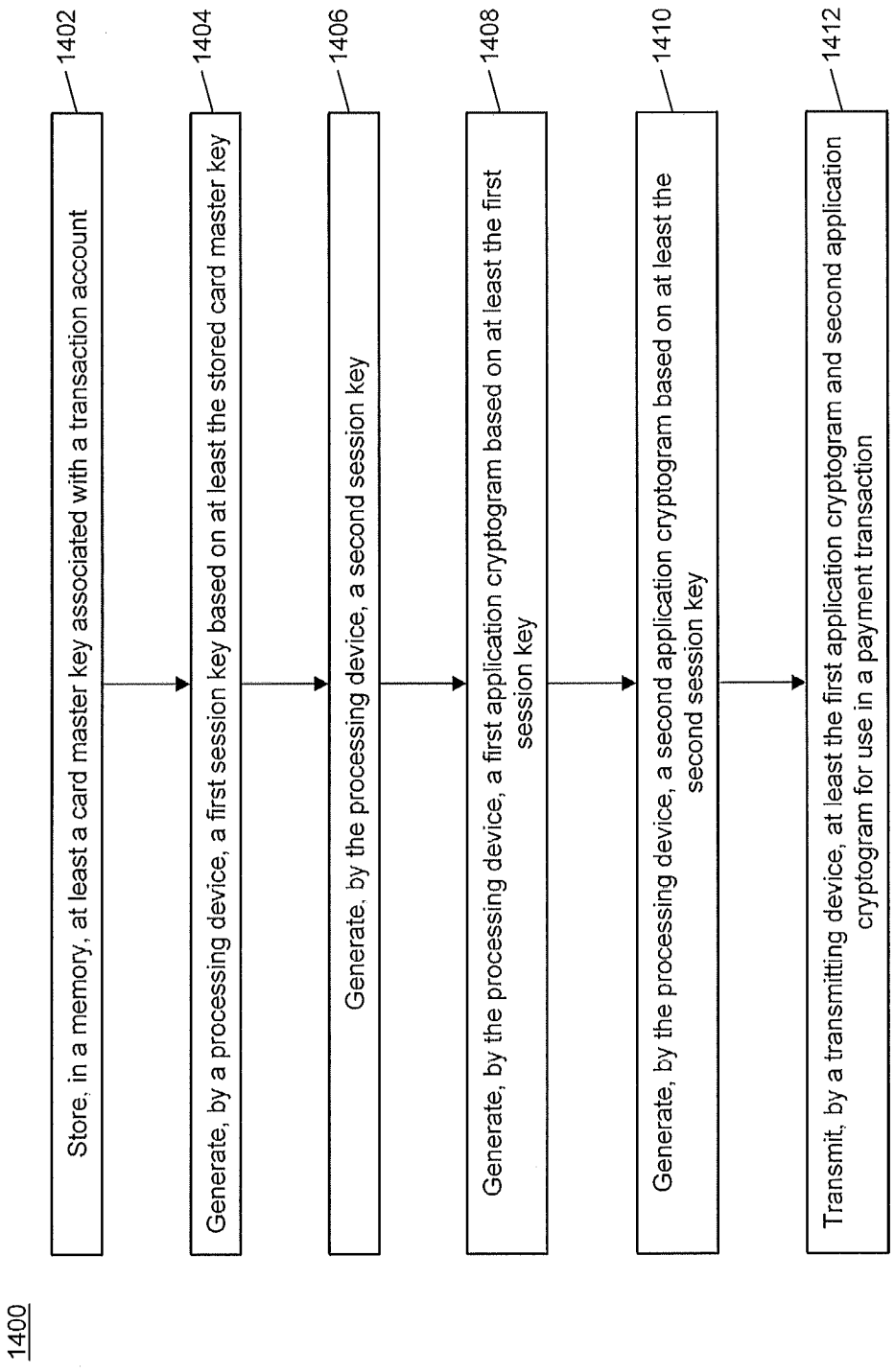

1400
1402
Store, in a memory, at least a card master key associated with a transaction account
1404
Generate, by a processing device, a first session key based on at least the stored card master key
1406
Generate, by the processing device, a second session key
1408
Generate, by the processing device, a first application cryptogram based on at least the first session key
1410
Generate, by the processing device, a second application cryptogram based on at least the second session key
1412
Transmit, by a transmitting device, at least the first application cryptogram and second application cryptogram for use in a payment transaction

FIG. 14

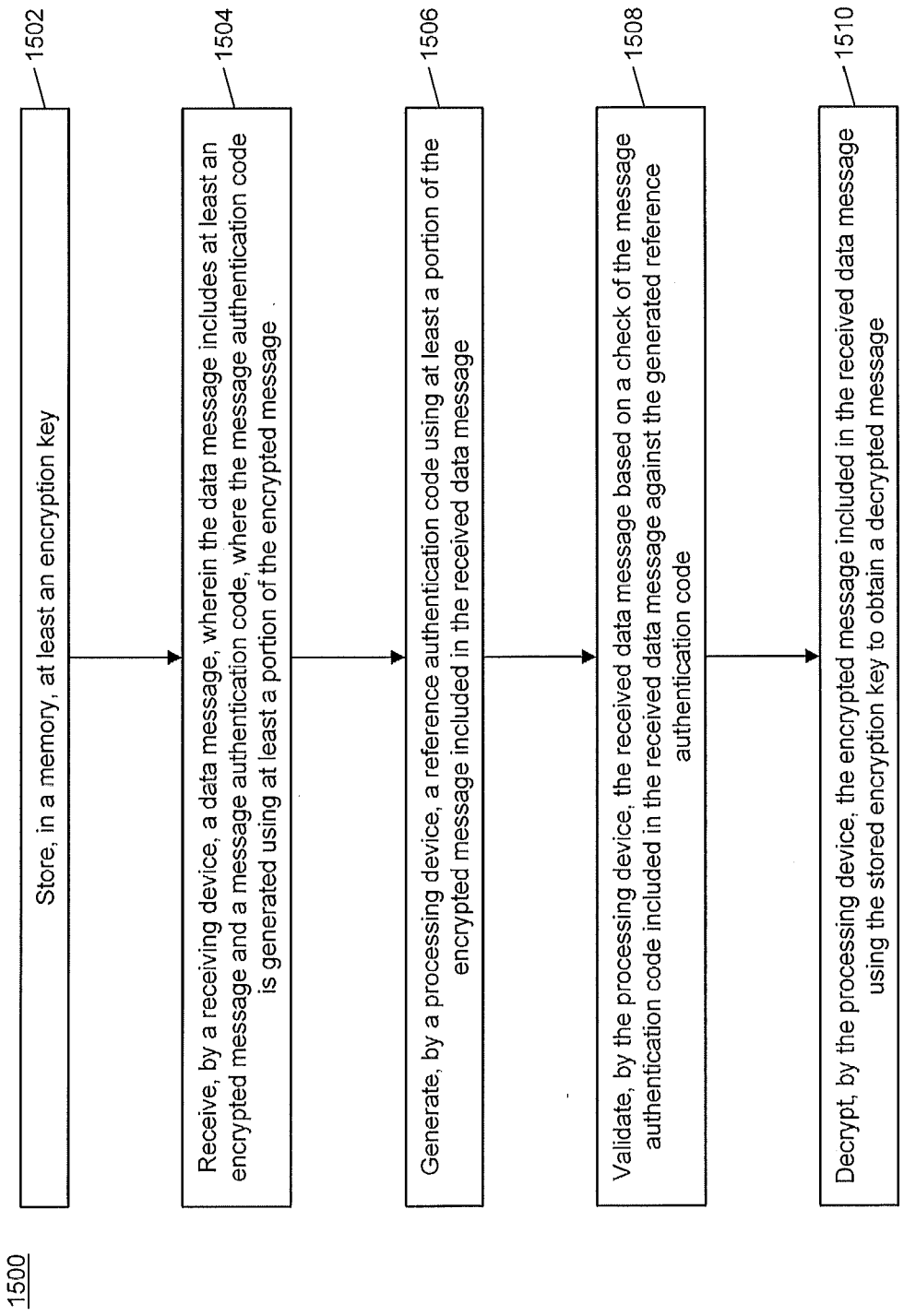

1500
1502
Store, in a memory, at least an encryption key
1504
Receive, by a receiving device, a data message, wherein the data message includes at least an encrypted message and a message authentication code, where the message authentication code is generated using at least a portion of the encrypted message
1506
Generate, by a processing device, a reference authentication code using at least a portion of the encrypted message included in the received data message
1508
Validate, by the processing device, the received data message based on a check of the message authentication code included in the received data message against the generated reference authentication code
1510
Decrypt, by the processing device, the encrypted message included in the received data message using the stored encryption key to obtain a decrypted message

FIG. 15

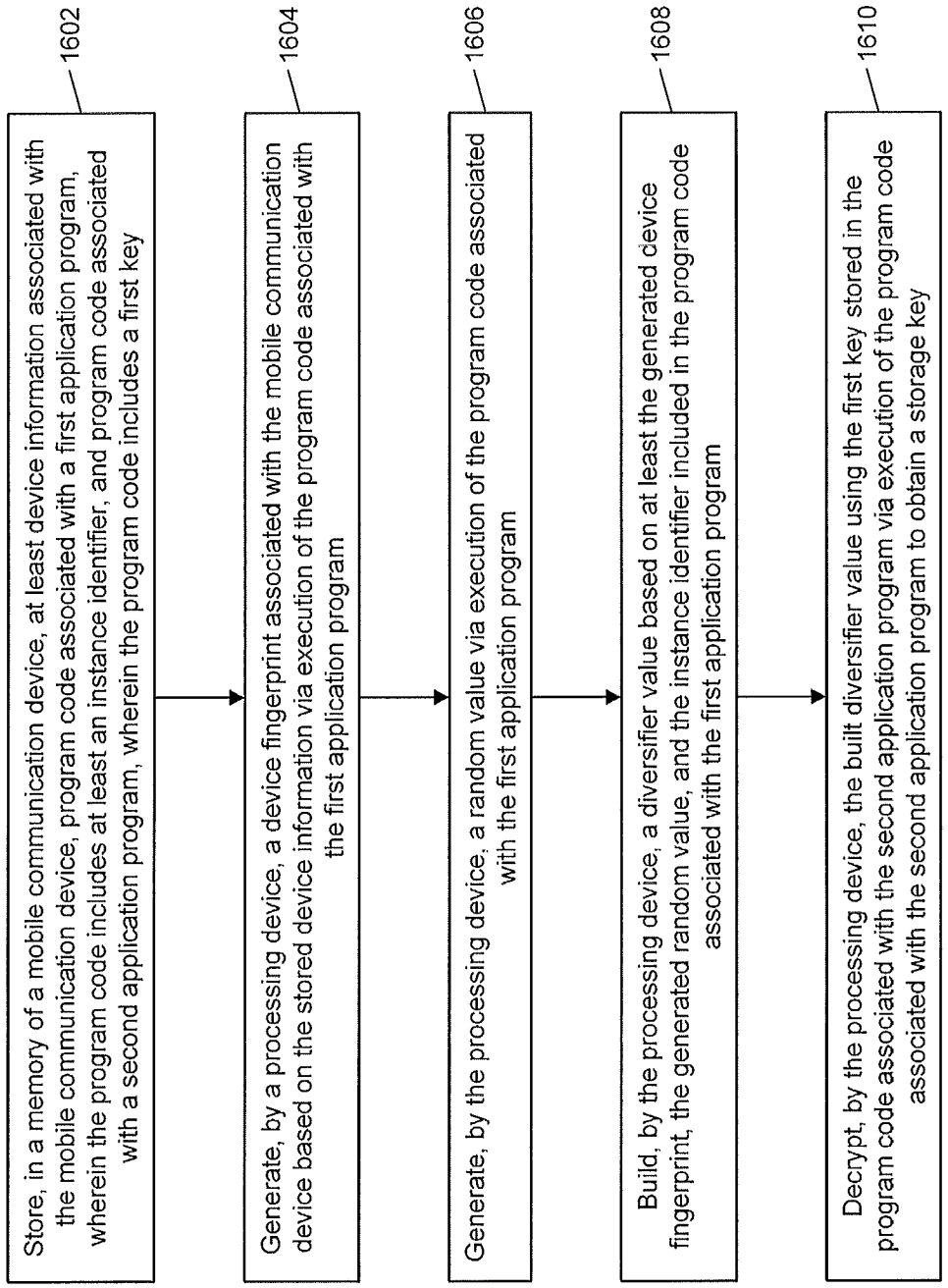

1600
Store, in a memory of a mobile communication device, at least device information associated with the mobile communication device, program code associated with a first application program, wherein the program code includes at least an instance identifier, and program code associated with a second application program, wherein the program code includes a first key
1602
Generate, by a processing device, a device fingerprint associated with the mobile communication device based on the stored device information via execution of the program code associated with the first application program
1604
Generate, by the processing device, a random value via execution of the program code associated with the first application program
1606
Build, by the processing device, a diversifier value based on at least the generated device fingerprint, the generated random value, and the instance identifier included in the program code associated with the first application program
1608
Decrypt, by the processing device, the built diversifier value using the first key stored in the program code associated with the second application program via execution of the program code associated with the second application program to obtain a storage key
1610

FIG. 16

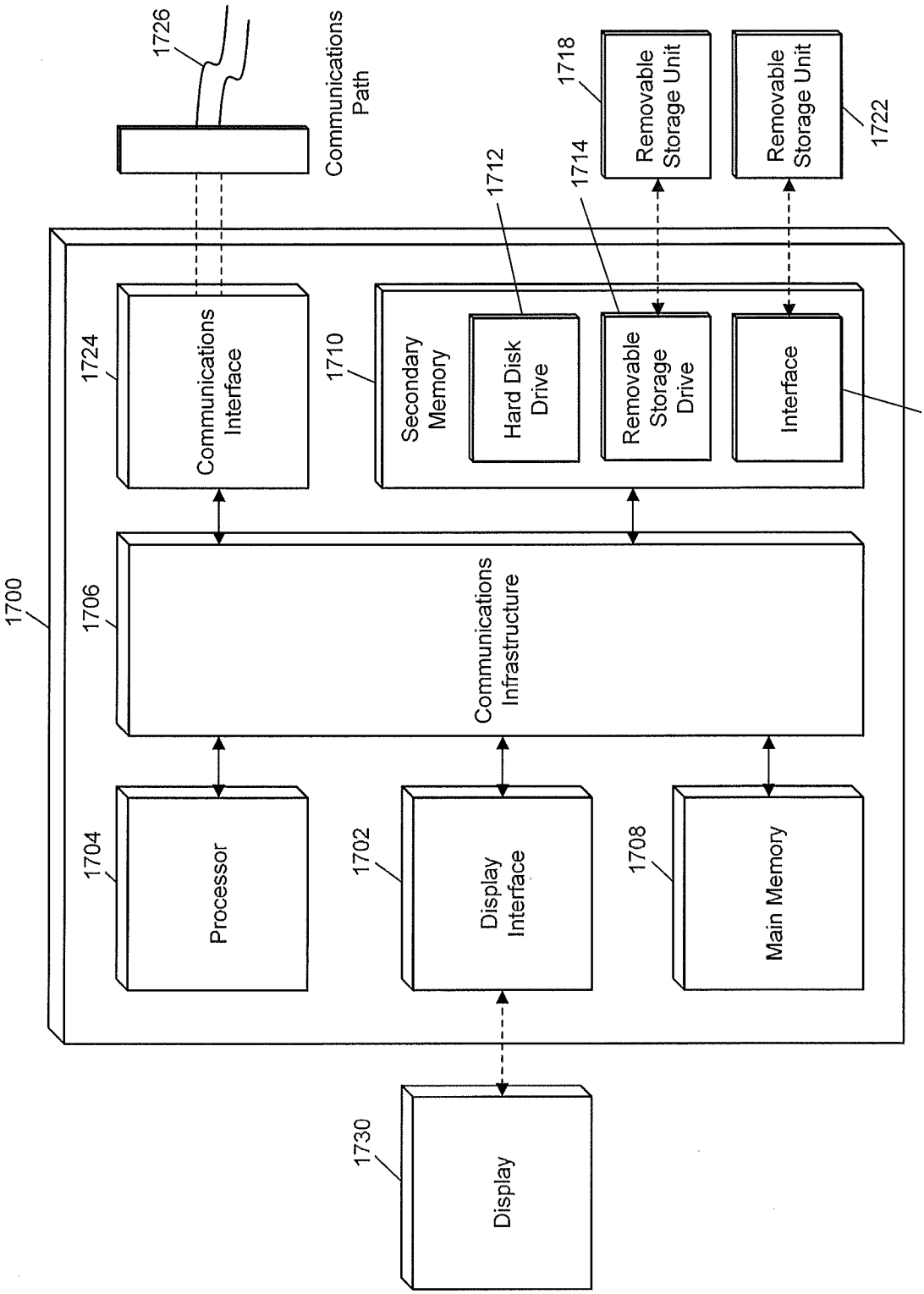

1726
Communications Path
1718
Removable Storage Unit
Removable Storage Unit
1722
1712
1714
1724
Communications Interface
1710
Secondary Memory
Hard Disk Drive
Removable Storage Drive
Interface
1720
1700
1706
Communications Infrastructure
1704
Processor
1702
Display Interface
1708
Main Memory
1730
Display

FIG. 17