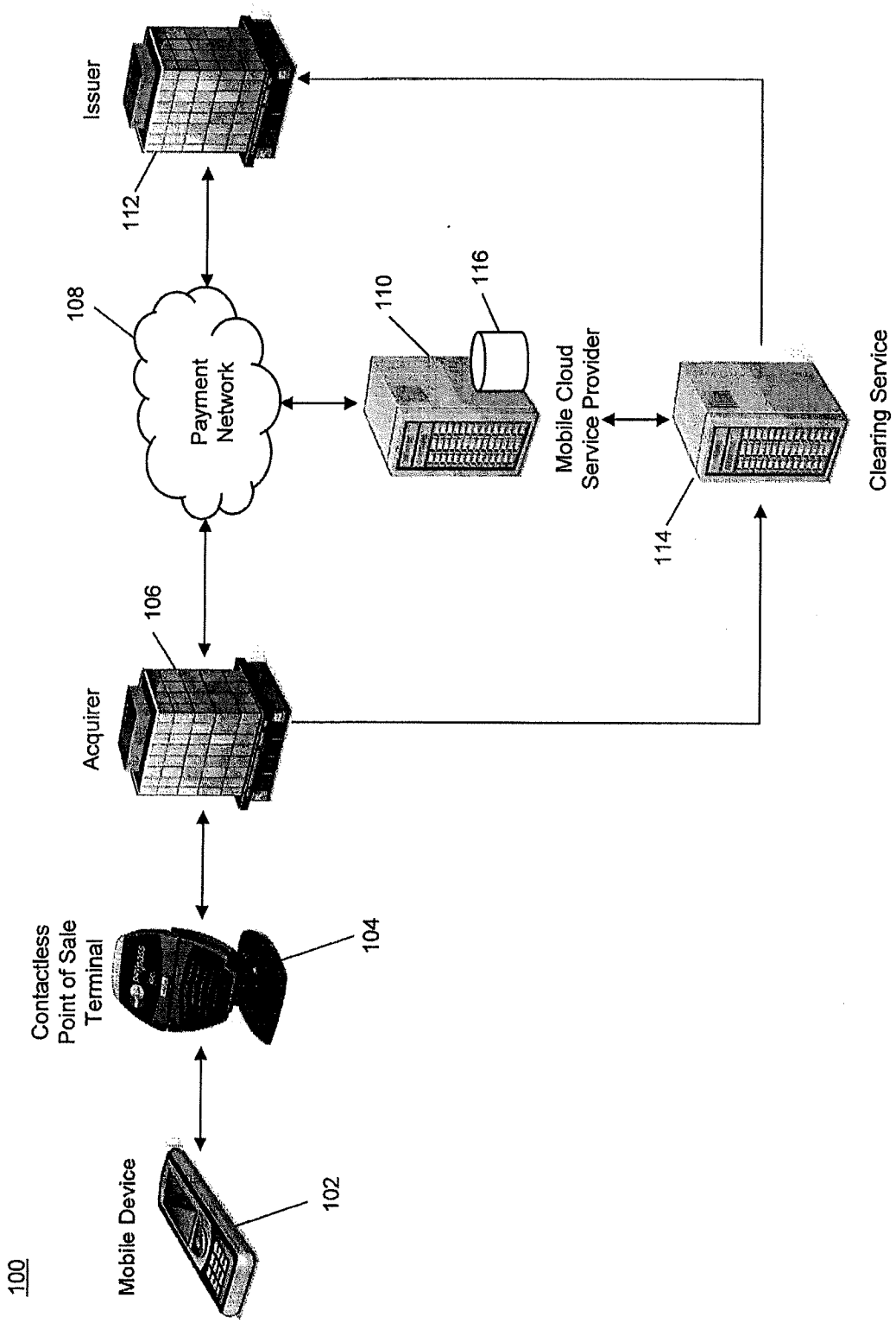

100
Mobile Device
102
Contactless Point of Sale Terminal
104
Acquirer
106
Payment Network
108
Issuer
112
110
116
Mobile Cloud Service Provider
114
Clearing Service

FIG. 1

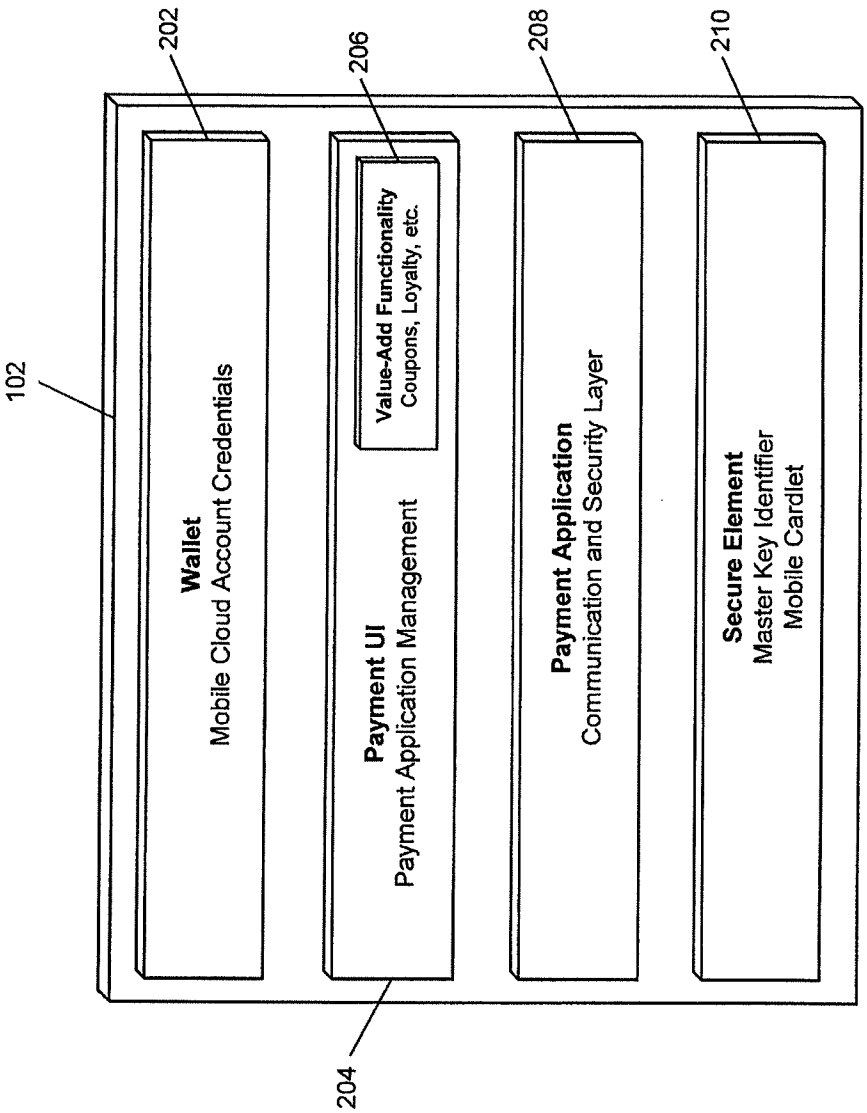

102
202
206
208
210
204
Wallet
Mobile Cloud Account Credentials
Payment UI
Payment Application Management
Value-Add Functionality
Coupons, Loyalty, etc.
Payment Application
Communication and Security Layer
Secure Element
Master Key Identifier
Mobile Cardlet

FIG. 2

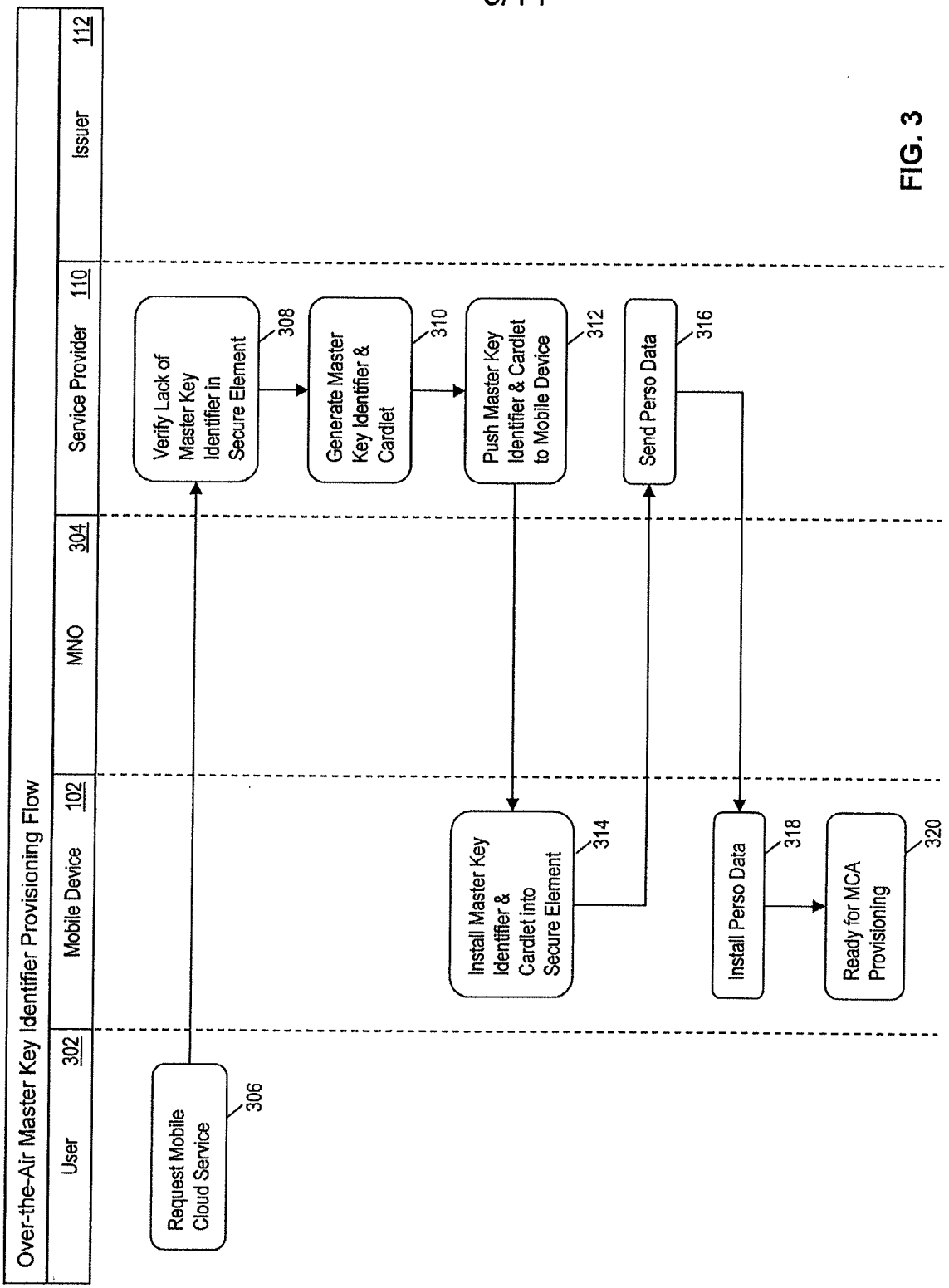

Over-the-Air Master Key Identifier Provisioning Flow
User 302
Mobile Device 102
MNO 304
Service Provider 110
Issuer 112
Request Mobile Cloud Service
306
Verify Lack of Master Key Identifier in Secure Element
308
Generate Master Key Identifier & Cardlet
310
Push Master Key Identifier & Cardlet to Mobile Device
312
Send Perso Data
316
Install Master Key Identifier & Cardlet into Secure Element
314
Install Perso Data
318
Ready for MCA Provisioning
320

FIG. 3

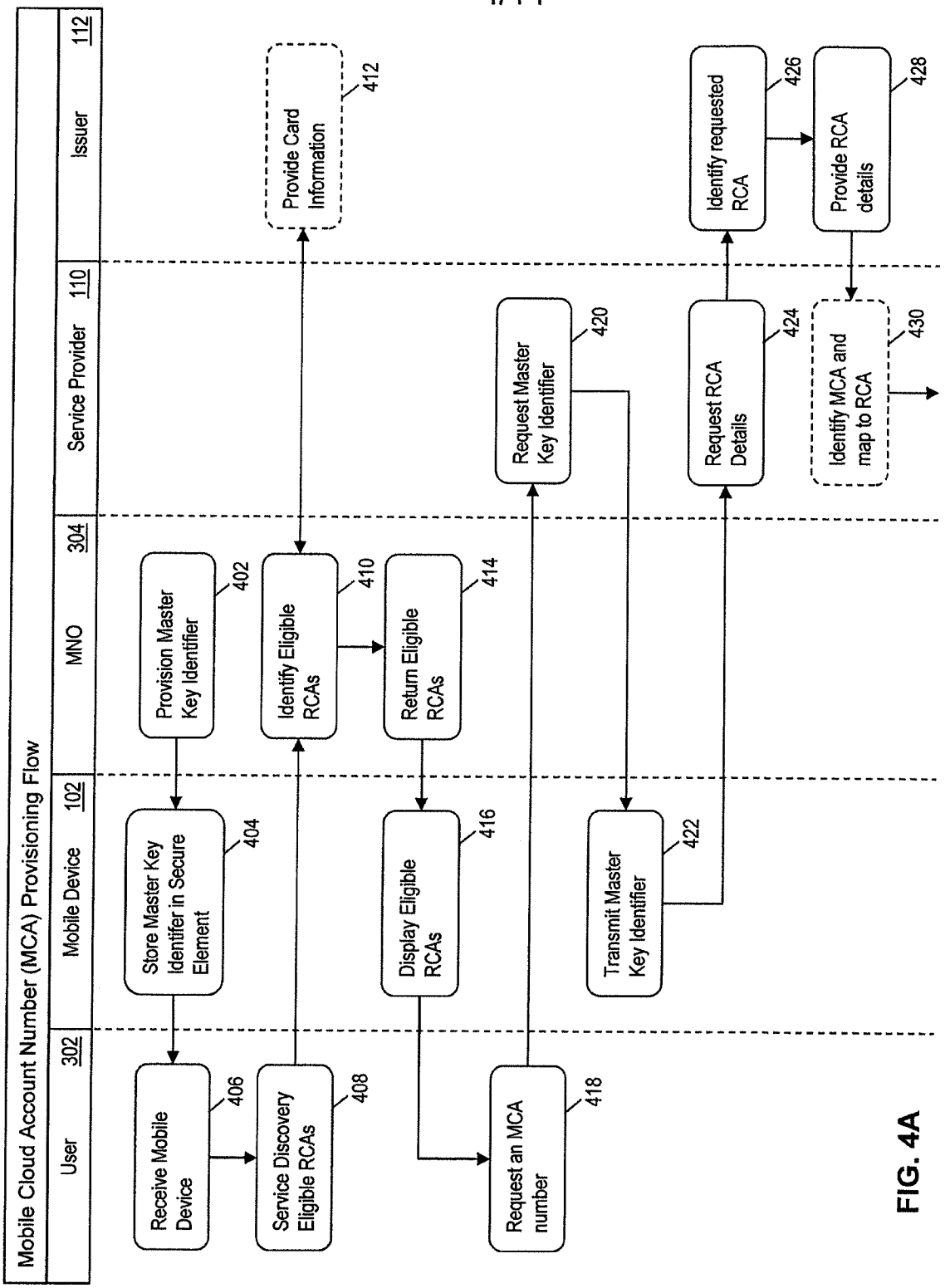

Mobile Cloud Account Number (MCA) Provisioning Flow
User 302
Mobile Device 102
MNO 304
Service Provider 110
Issuer 112
Provide Card Information
412
Provision Master Key Identifier
402
Identify Eligible RCAs
410
Return Eligible RCAs
414
Request Master Key Identifier
420
Identify requested RCA
426
Provide RCA details
428
Request RCA Details
424
Identify MCA and map to RCA
430
Store Master Key Identifer in Secure Element
404
Display Eligible RCAs
416
Transmit Master Key Identifier
422
Receive Mobile Device
406
Service Discovery Eligible RCAs
408
Request an MCA number
418

FIG. 4A

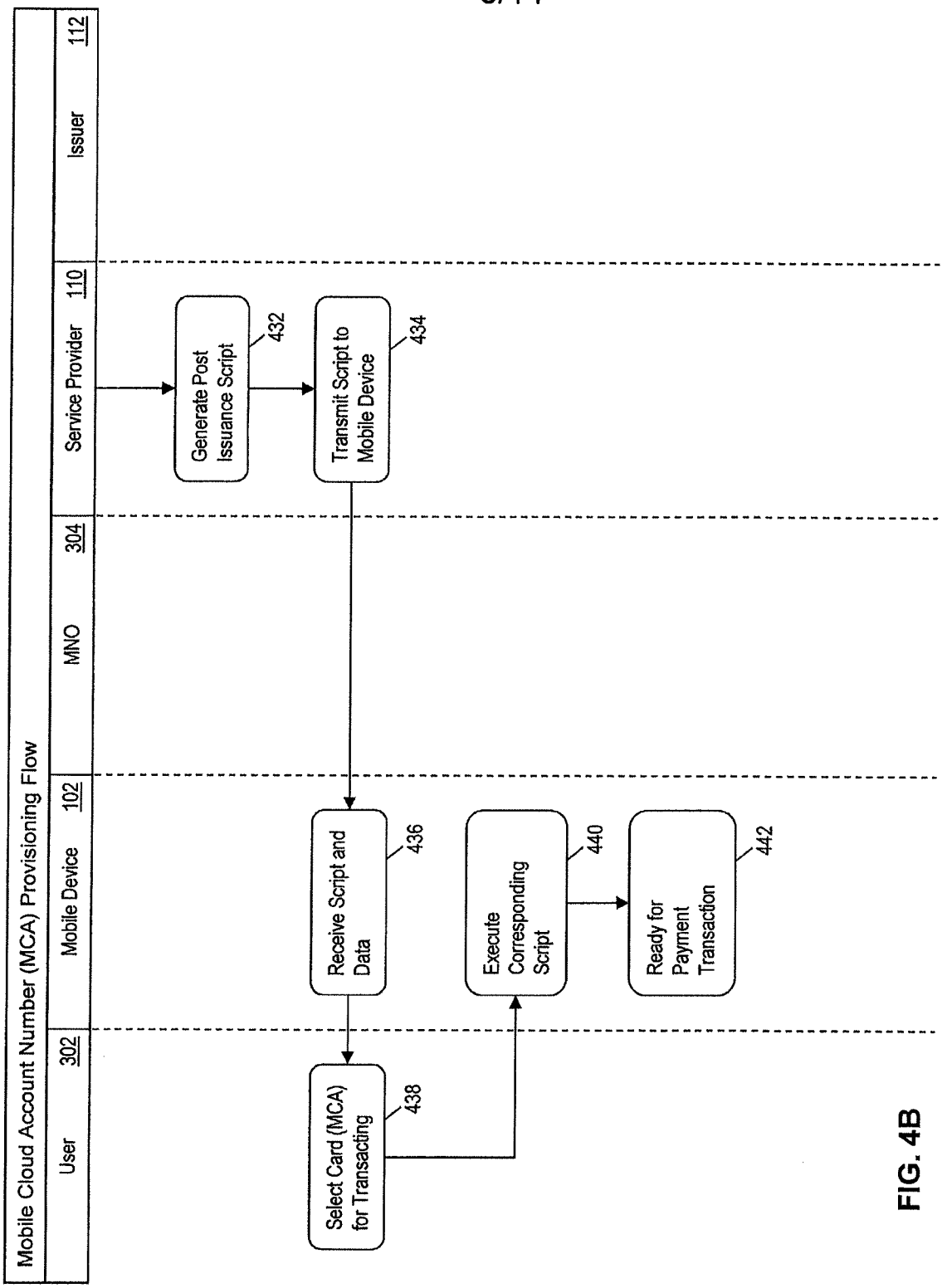

Mobile Cloud Account Number (MCA) Provisioning Flow
User 302
Mobile Device 102
MNO 304
Service Provider 110
Issuer 112
Generate Post Issuance Script
432
Transmit Script to Mobile Device
434
Receive Script and Data
436
Select Card (MCA) for Transacting
438
Execute Corresponding Script
440
Ready for Payment Transaction
442

FIG. 4B

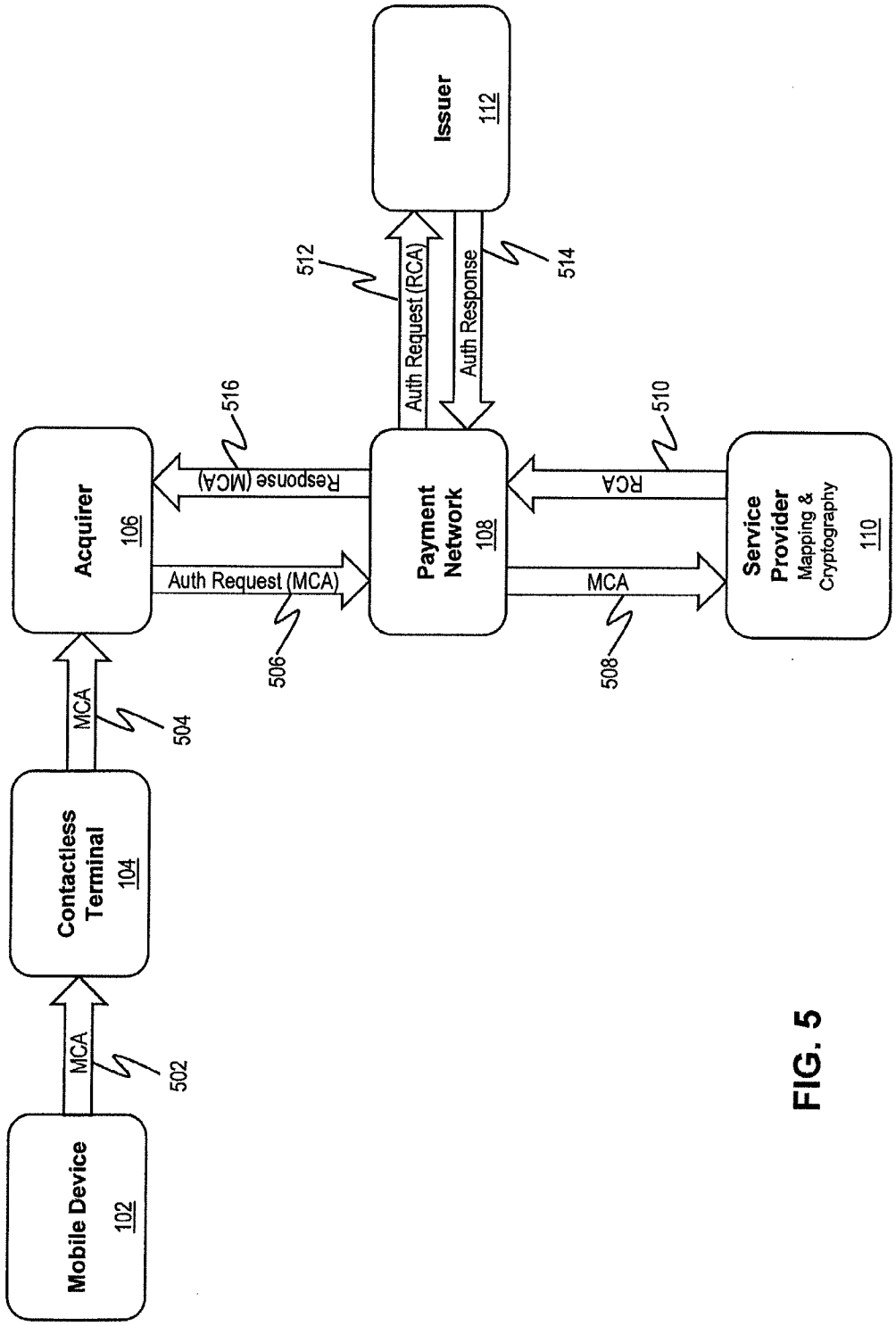

Mobile Device
102
Contactless Terminal
104
Acquirer
106
Payment Network
108
Service Provider
Mapping & Cryptography
110
Issuer
112
MCA
502
MCA
504
Auth Request (MCA)
506
MCA
508
RCA
510
Response (MCA)
516
Auth Request (RCA)
512
Auth Response
514

FIG. 5

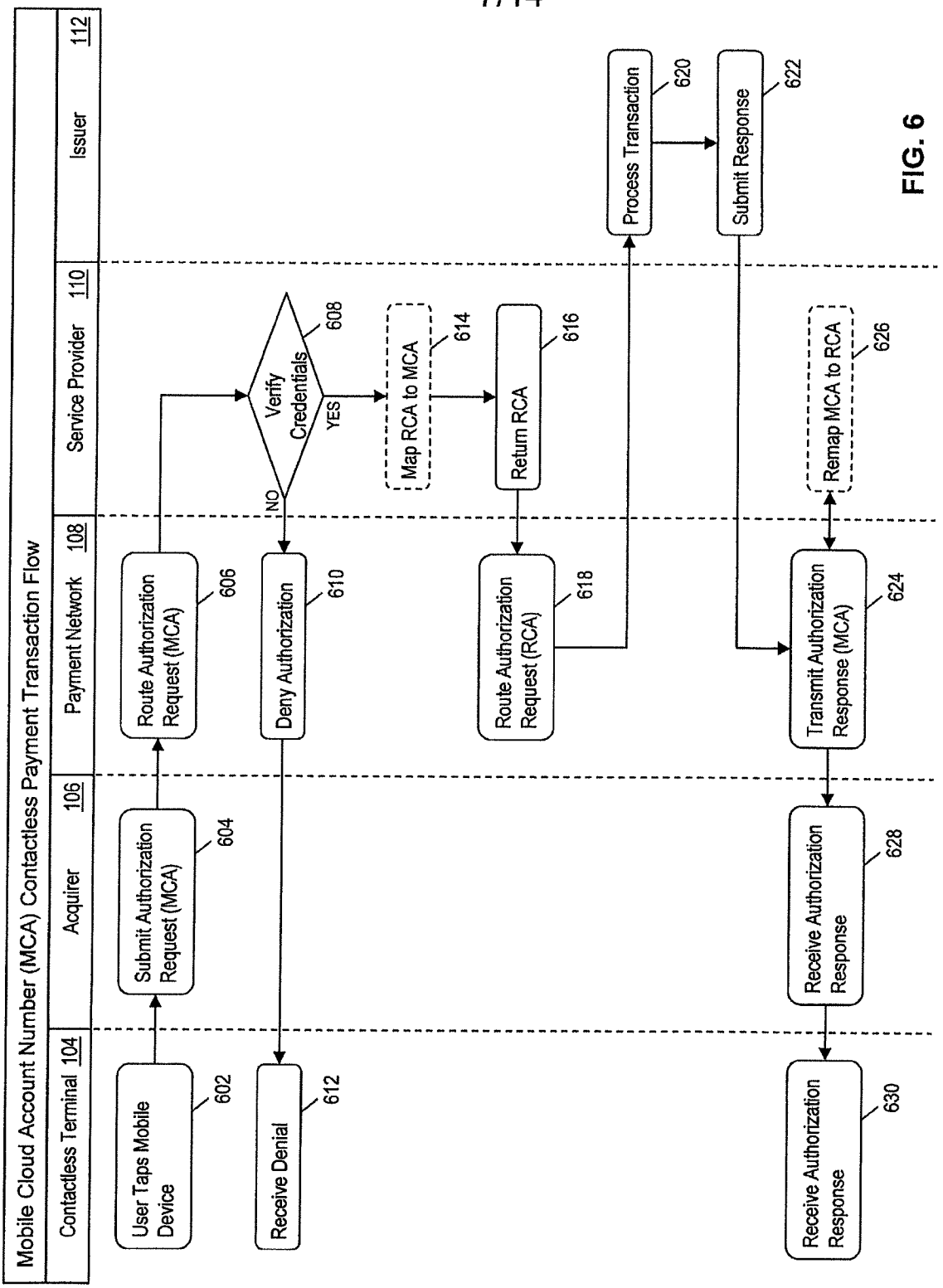

Mobile Cloud Account Number (MCA) Contactless Payment Transaction Flow
Contactless Terminal 104
Acquirer 106
Payment Network 108
Service Provider 110
Issuer 112
User Taps Mobile Device
602
Submit Authorization Request (MCA)
604
Route Authorization Request (MCA)
606
Verify Credentials
608
YES
NO
Map RCA to MCA
614
Return RCA
616
Route Authorization Request (RCA)
618
Process Transaction
620
Submit Response
622
Remap MCA to RCA
626
Transmit Authorization Response (MCA)
624
Receive Authorization Response
628
Receive Authorization Response
630
Deny Authorization
610
Receive Denial
612

FIG. 6

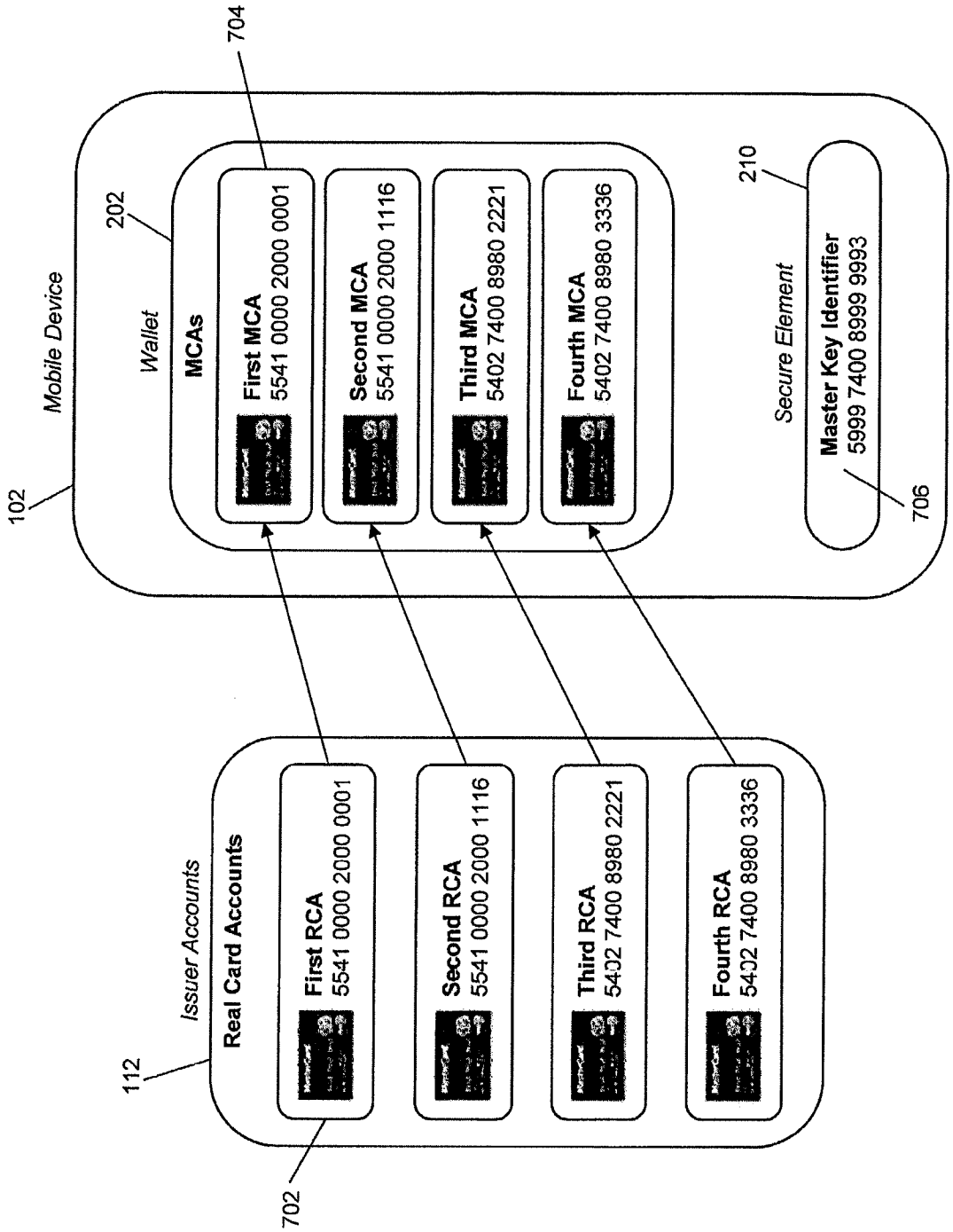

Issuer Accounts
112
Real Card Accounts
First RCA
5541 0000 2000 0001
Second RCA
5541 0000 2000 1116
Third RCA
5402 7400 8980 2221
Fourth RCA
5402 7400 8980 3336
702
Mobile Device
102
Wallet
202
MCAs
First MCA
5541 0000 2000 0001
Second MCA
5541 0000 2000 1116
Third MCA
5402 7400 8980 2221
Fourth MCA
5402 7400 8980 3336
704
Secure Element
210
Master Key Identifier
5999 7400 8999 9993
706

FIG. 7

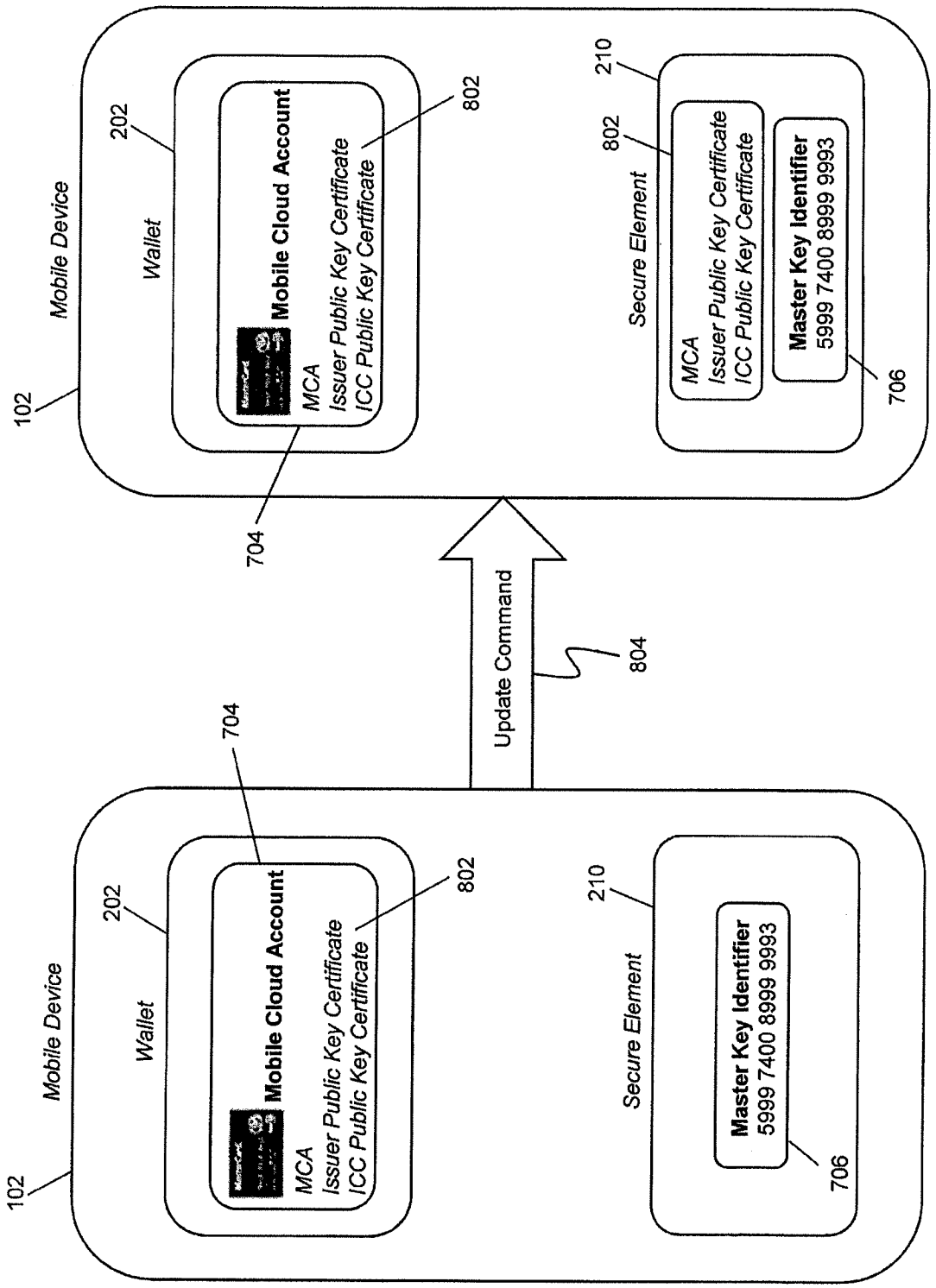

102
Mobile Device
202
Wallet
Mobile Cloud Account
MCA
Issuer Public Key Certificate
ICC Public Key Certificate
802
704
210
Secure Element
MCA
Issuer Public Key Certificate
ICC Public Key Certificate
Master Key Identifier
5999 7400 8999 9993
706
Update Command
804

FIG. 8

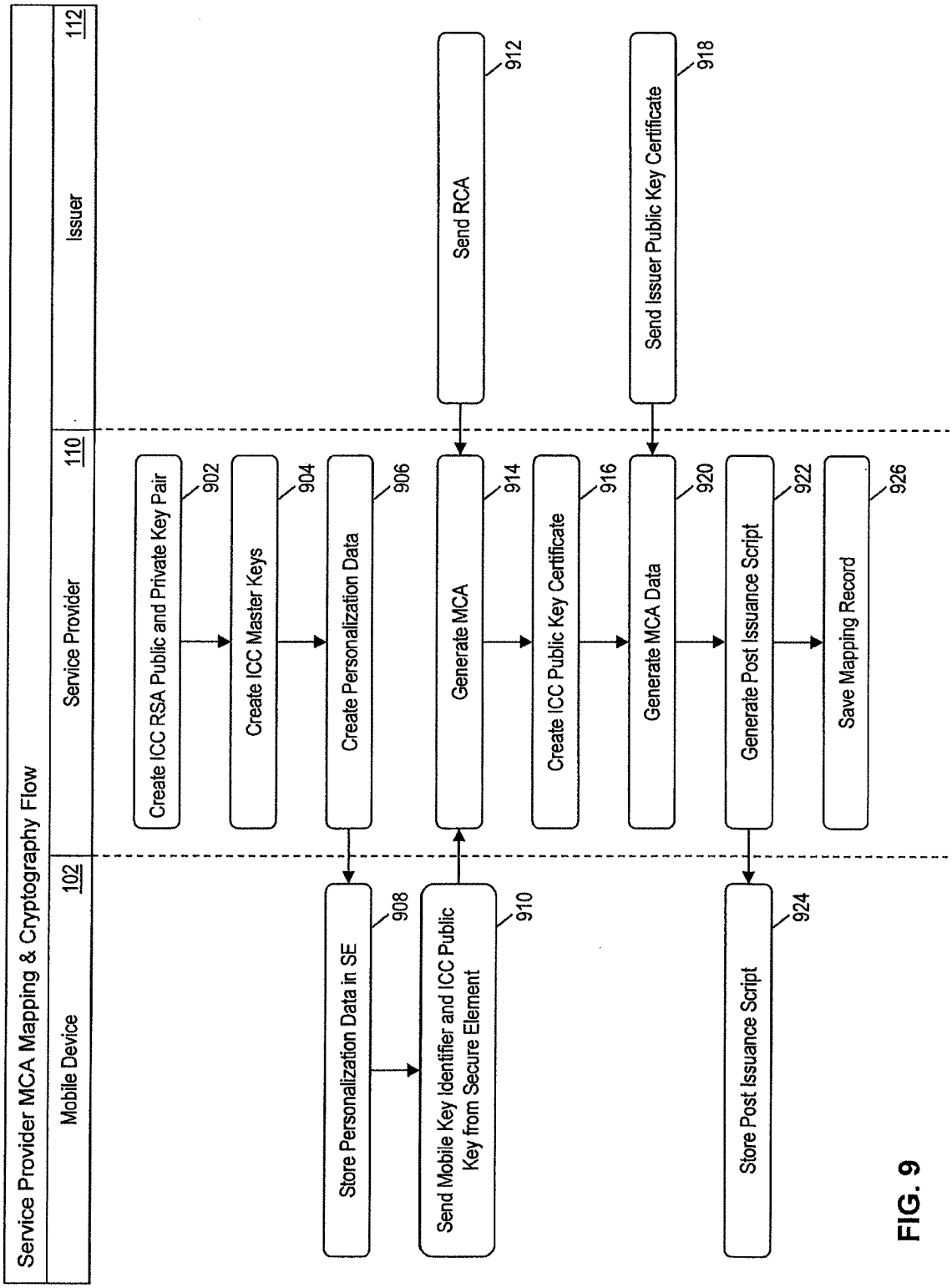

Service Provider MCA Mapping & Cryptography Flow
Mobile Device 102
Service Provider 110
Issuer 112
Create ICC RSA Public and Private Key Pair 902
Create ICC Master Keys 904
Create Personalization Data 906
Store Personalization Data in SE 908
Send Mobile Key Identifier and ICC Public Key from Secure Element 910
Send RCA 912
Generate MCA 914
Create ICC Public Key Certificate 916
Send Issuer Public Key Certificate 918
Generate MCA Data 920
Generate Post Issuance Script 922
Store Post Issuance Script 924
Save Mapping Record 926

FIG. 9

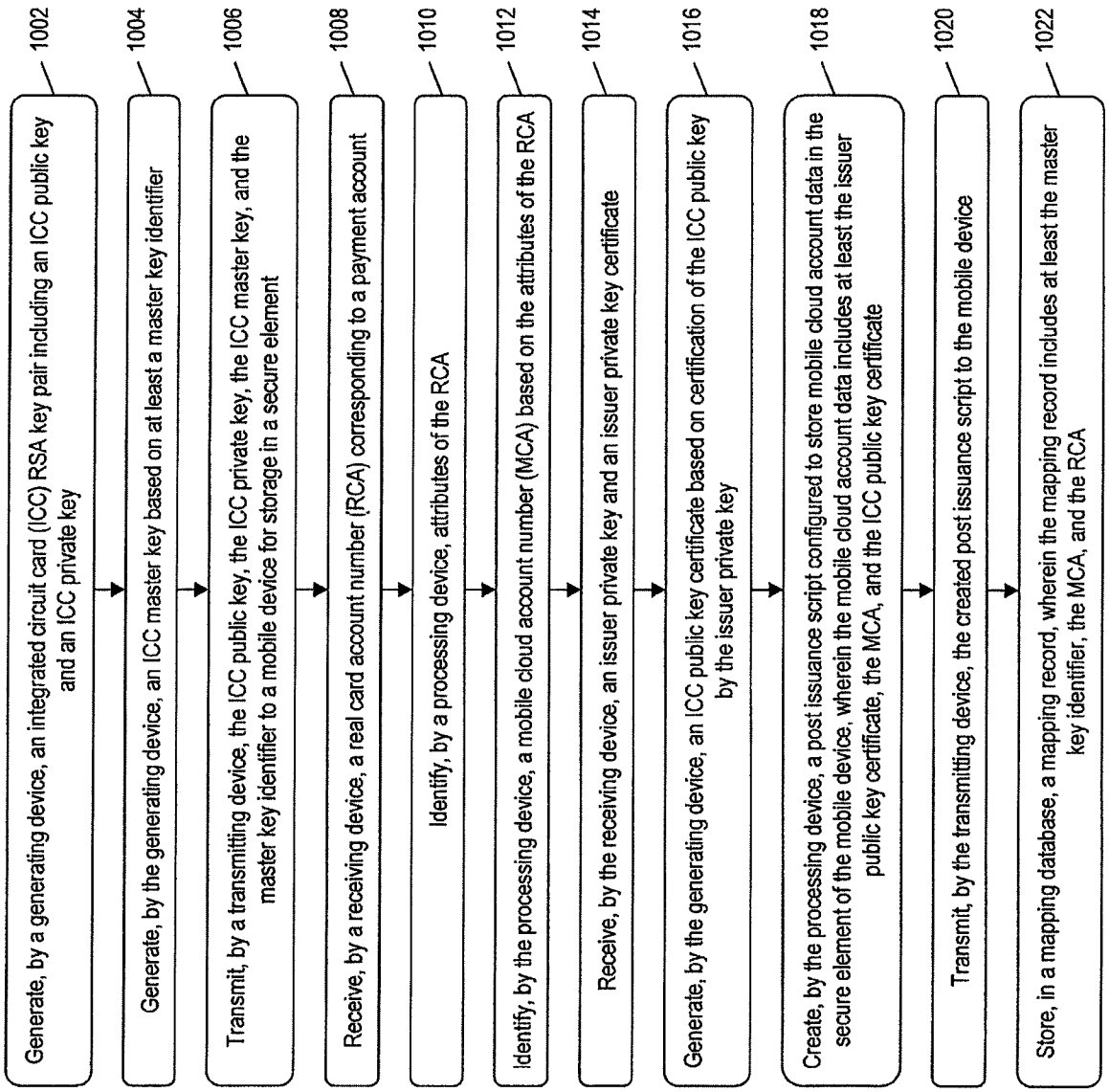

1000
Generate, by a generating device, an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key
1002
Generate, by the generating device, an ICC master key based on at least a master key identifier
1004
Transmit, by a transmitting device, the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element
1006
Receive, by a receiving device, a real card account number (RCA) corresponding to a payment account
1008
Identify, by a processing device, attributes of the RCA
1010
Identify, by the processing device, a mobile cloud account number (MCA) based on the attributes of the RCA
1012
Receive, by the receiving device, an issuer private key and an issuer private key certificate
1014
Generate, by the generating device, an ICC public key certificate based on certification of the ICC public key by the issuer private key
1016
Create, by the processing device, a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, wherein the mobile cloud account data includes at least the issuer public key certificate, the MCA, and the ICC public key certificate
1018
Transmit, by the transmitting device, the created post issuance script to the mobile device
1020
Store, in a mapping database, a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA
1022

FIG. 10

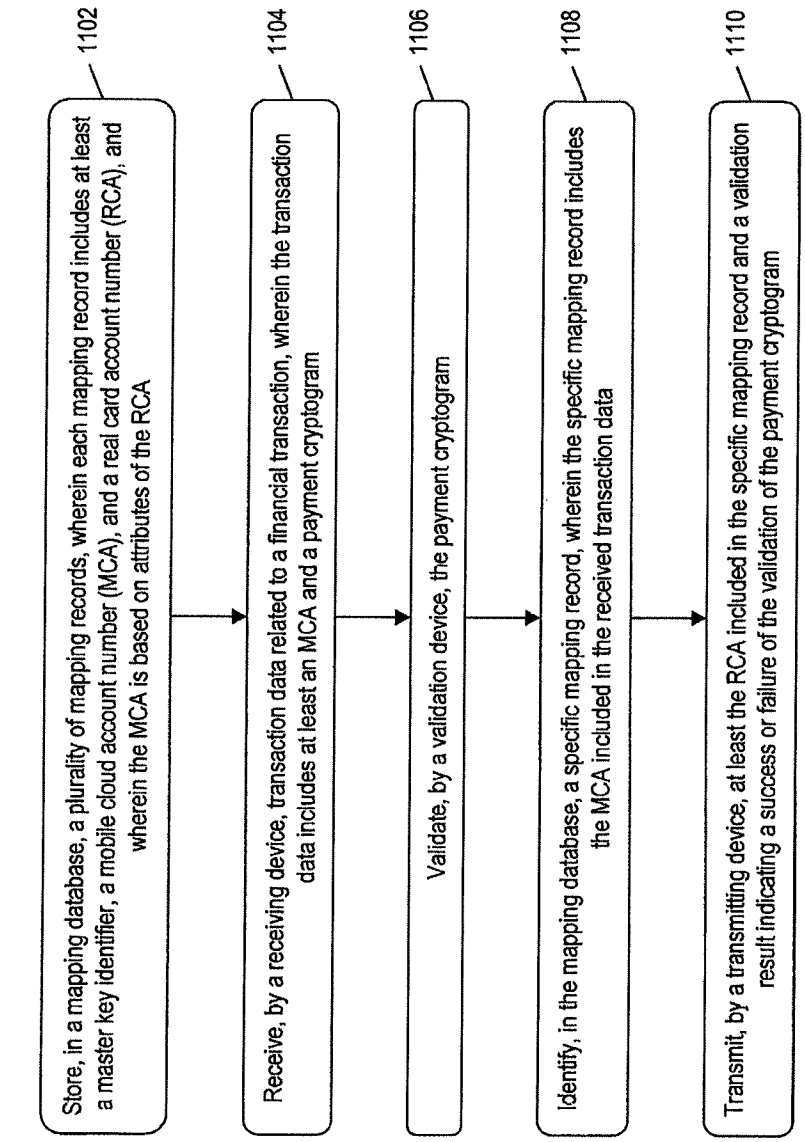

1100
1102
Store, in a mapping database, a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), and wherein the MCA is based on attributes of the RCA
1104
Receive, by a receiving device, transaction data related to a financial transaction, wherein the transaction data includes at least an MCA and a payment cryptogram
1106
Validate, by a validation device, the payment cryptogram
1108
Identify, in the mapping database, a specific mapping record, wherein the specific mapping record includes the MCA included in the received transaction data
1110
Transmit, by a transmitting device, at least the RCA included in the specific mapping record and a validation result indicating a success or failure of the validation of the payment cryptogram

FIG. 11

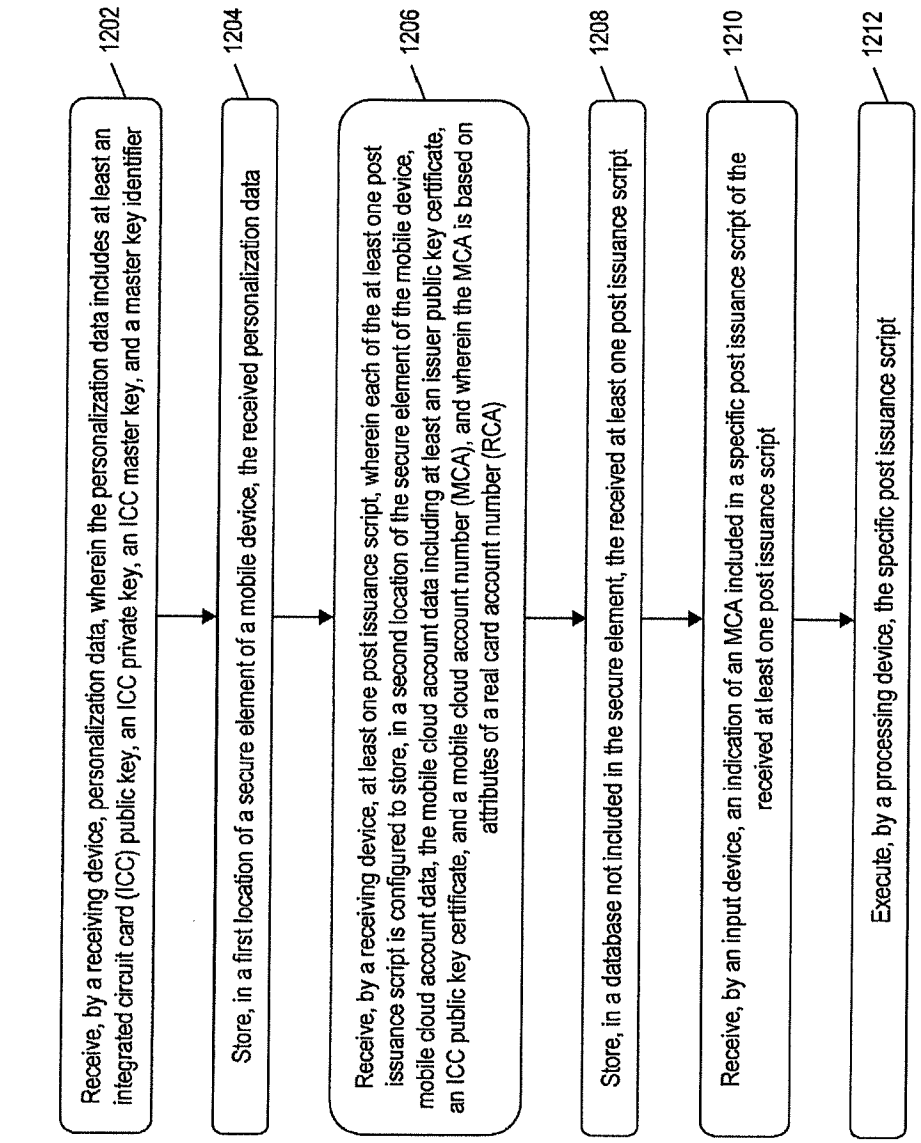

1200
1202
Receive, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier
1204
Store, in a first location of a secure element of a mobile device, the received personalization data
1206
Receive, by a receiving device, at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA), and wherein the MCA is based on attributes of a real card account number (RCA)
1208
Store, in a database not included in the secure element, the received at least one post issuance script
1210
Receive, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script
1212
Execute, by a processing device, the specific post issuance script

FIG. 12

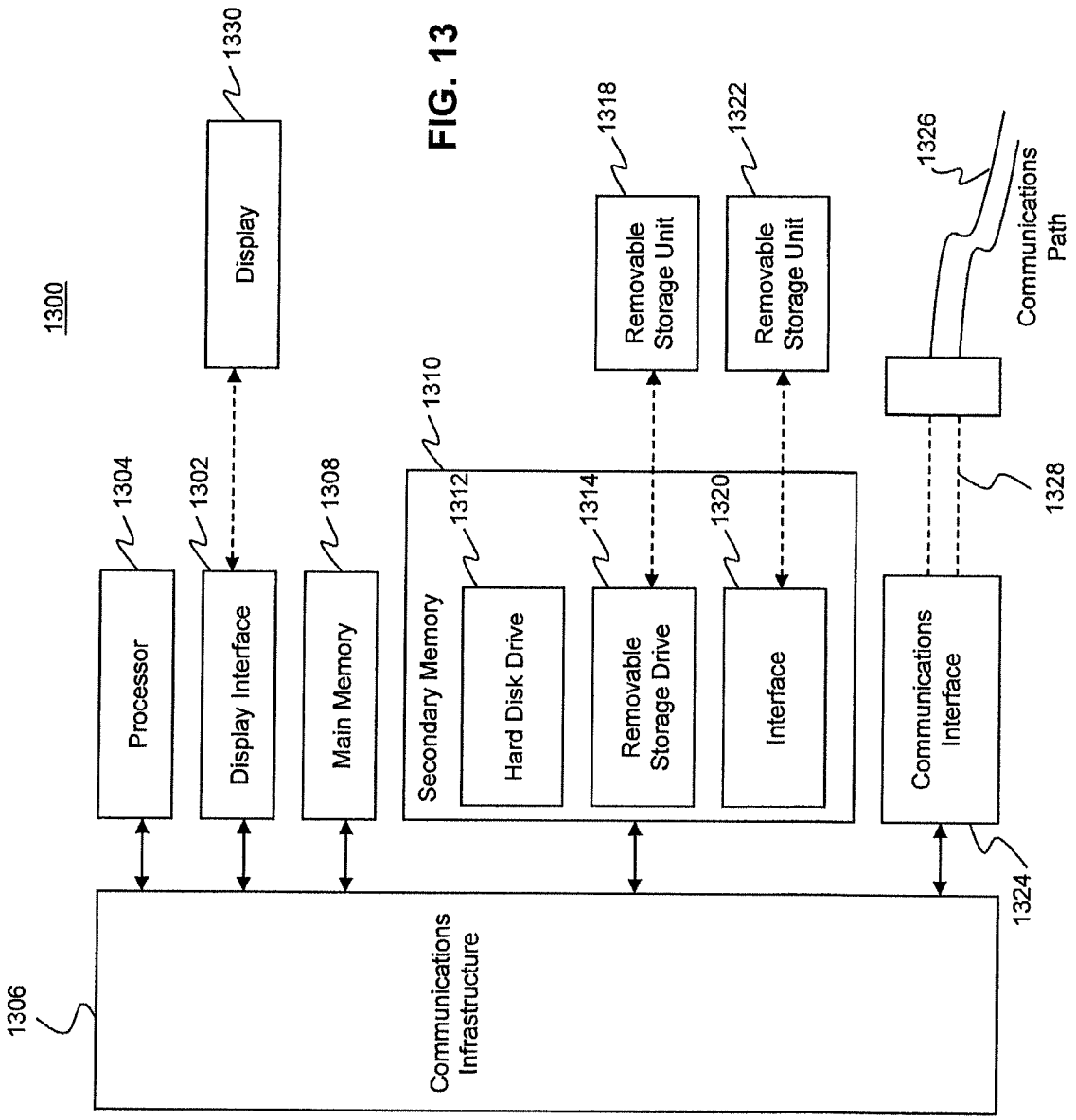

1300
1330
Display
1318
Removable Storage Unit
1322
Removable Storage Unit
1326
Communications Path
1310
1304
1302
1308
1312
1314
1320
1328
Processor
Display Interface
Main Memory
Secondary Memory
Hard Disk Drive
Removable Storage Drive
Interface
Communications Interface
1306
Communications Infrastructure
1324

FIG. 13