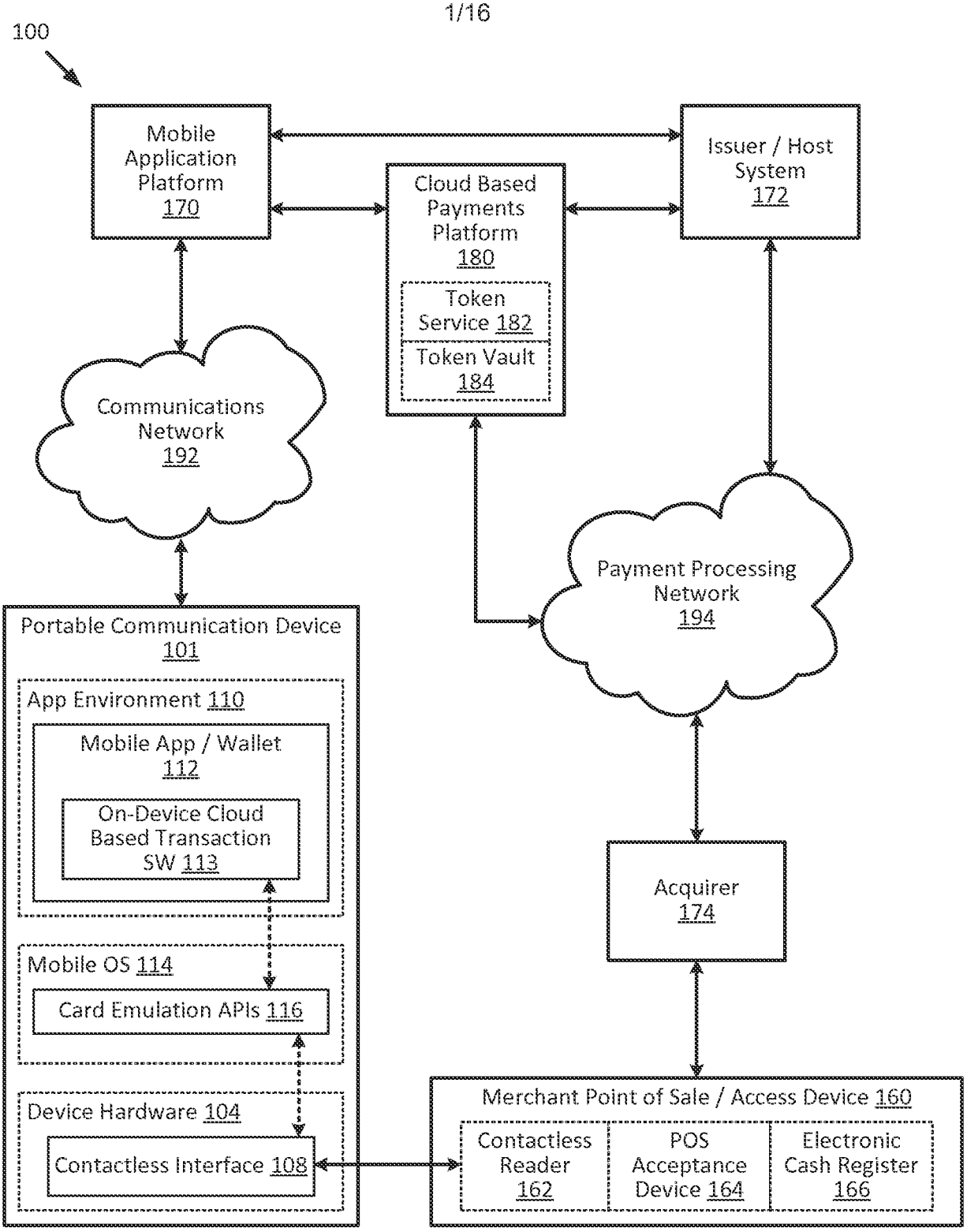

100
Mobile Application Platform 170
Issuer / Host System 172
Cloud Based Payments Platform 180
Token Service 182
Token Vault 184
Communications Network 192
Payment Processing Network 194
Portable Communication Device 101
App Environment 110
Mobile App / Wallet 112
On-Device Cloud Based Transaction SW 113
Mobile OS 114
Card Emulation APIs 116
Device Hardware 104
Contactless Interface 108
Acquirer 174
Merchant Point of Sale / Access Device 160
Contactless Reader 162
POS Acceptance Device 164
Electronic Cash Register 166

FIG. 1

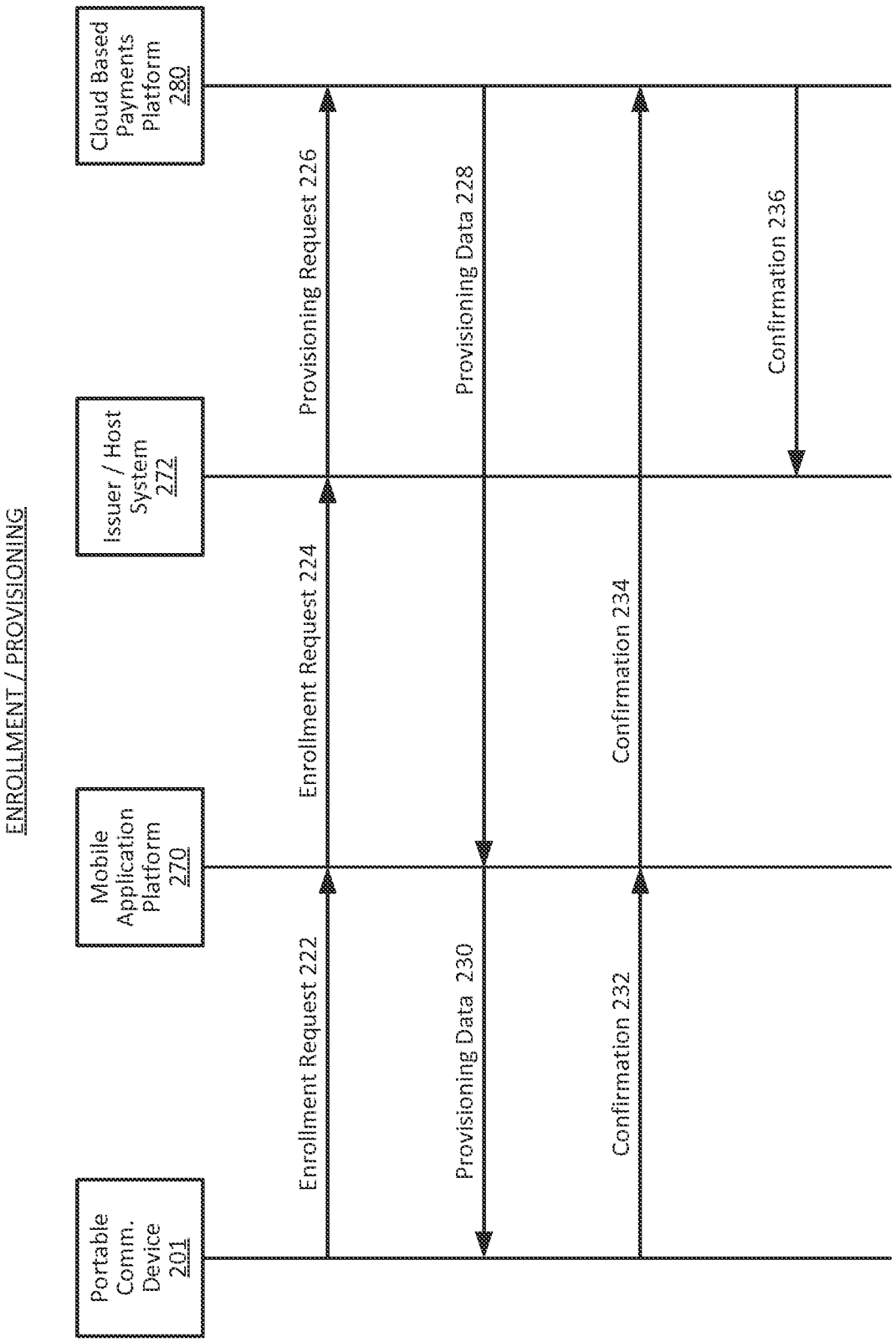

ENROLLMENT / PROVISIONING
Portable Comm. Device 201
Mobile Application Platform 270
Issuer / Host System 272
Cloud Based Payments Platform 280
Enrollment Request 222
Enrollment Request 224
Provisioning Request 226
Provisioning Data 230
Provisioning Data 228
Confirmation 232
Confirmation 234
Confirmation 236

FIG. 2

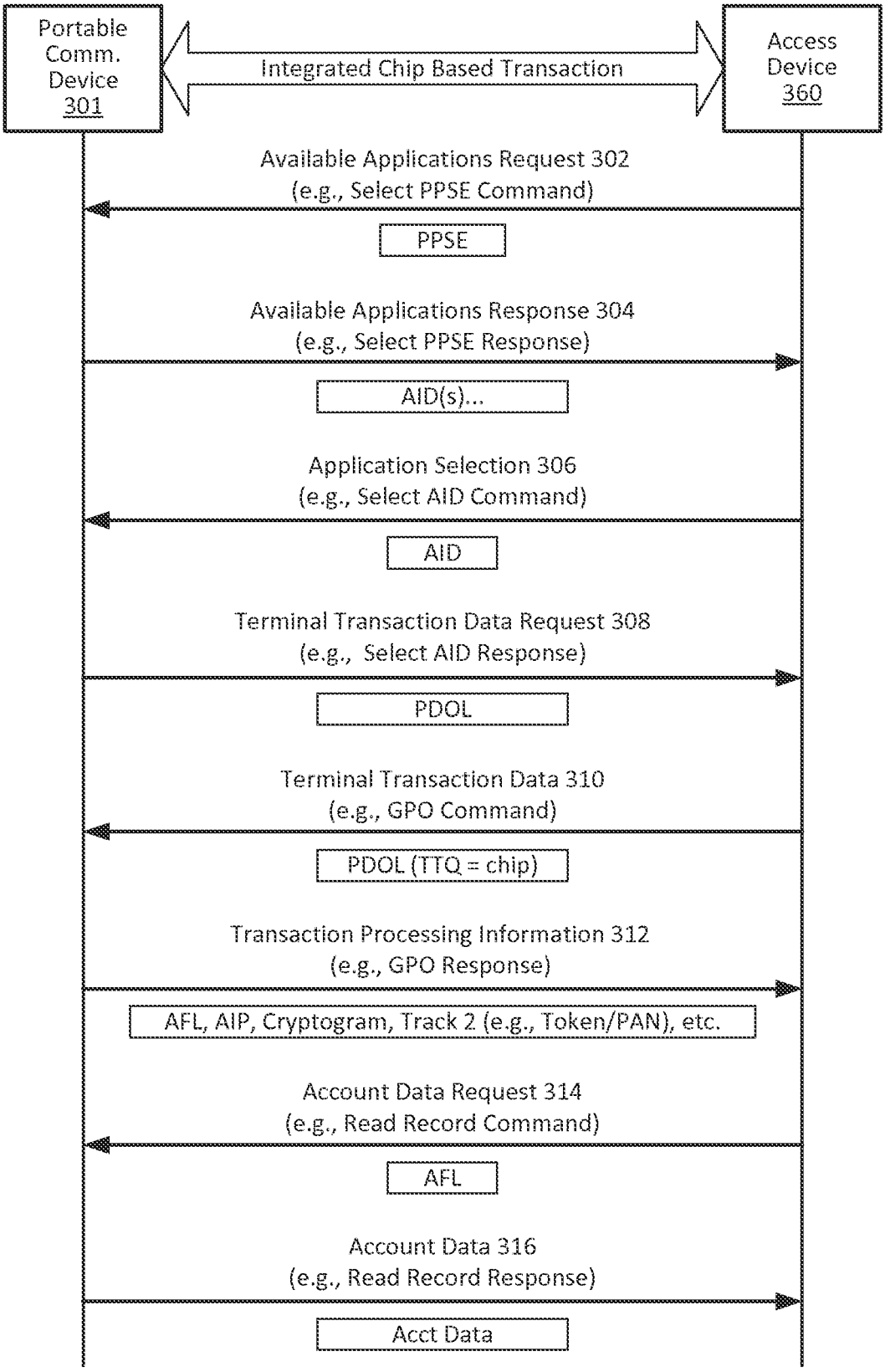

Portable Comm. Device 301
Integrated Chip Based Transaction
Access Device 360
Available Applications Request 302
(e.g., Select PPSE Command)
PPSE
Available Applications Response 304
(e.g., Select PPSE Response)
AID(s)...
Application Selection 306
(e.g., Select AID Command)
AID
Terminal Transaction Data Request 308
(e.g., Select AID Response)
PDOL
Terminal Transaction Data 310
(e.g., GPO Command)
PDOL (TTQ = chip)
Transaction Processing Information 312
(e.g., GPO Response)
AFL, AIP, Cryptogram, Track 2 (e.g., Token/PAN), etc.
Account Data Request 314
(e.g., Read Record Command)
AFL
Account Data 316
(e.g., Read Record Response)
Acct Data

FIG. 3

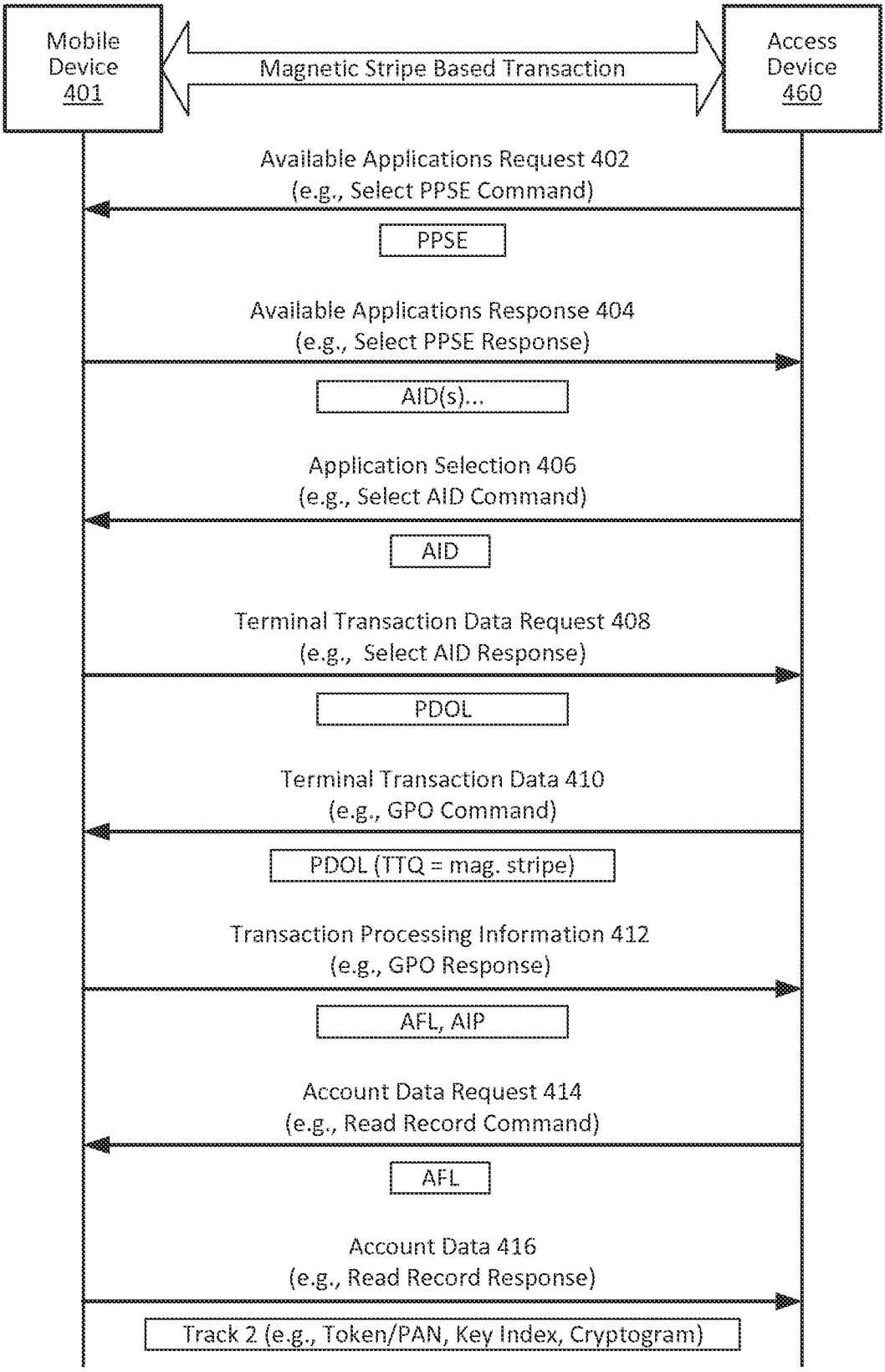

Mobile Device 401
Magnetic Stripe Based Transaction
Access Device 460
Available Applications Request 402
(e.g., Select PPSE Command)
PPSE
Available Applications Response 404
(e.g., Select PPSE Response)
AID(s)...
Application Selection 406
(e.g., Select AID Command)
AID
Terminal Transaction Data Request 408
(e.g., Select AID Response)
PDOL
Terminal Transaction Data 410
(e.g., GPO Command)
PDOL (TTQ = mag. stripe)
Transaction Processing Information 412
(e.g., GPO Response)
AFL, AIP
Account Data Request 414
(e.g., Read Record Command)
AFL
Account Data 416
(e.g., Read Record Response)
Track 2 (e.g., Token/PAN, Key Index, Cryptogram)

FIG. 4

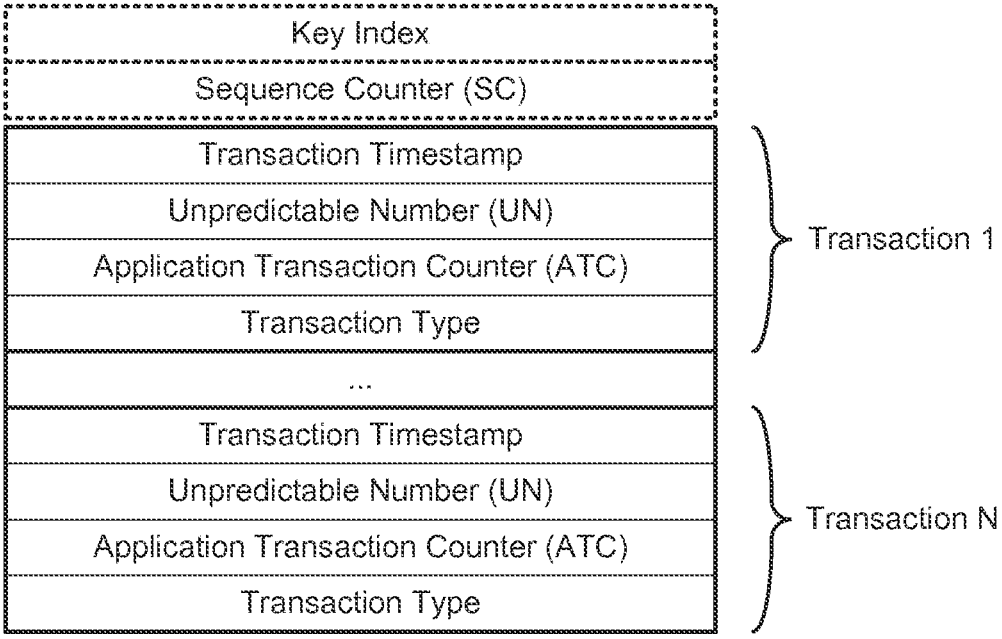

Key Index
Sequence Counter (SC)
Transaction Timestamp
Unpredictable Number (UN)
Application Transaction Counter (ATC)
Transaction Type
...
Transaction Timestamp
Unpredictable Number (UN)
Application Transaction Counter (ATC)
Transaction Type
Transaction 1
Transaction N

FIG. 5

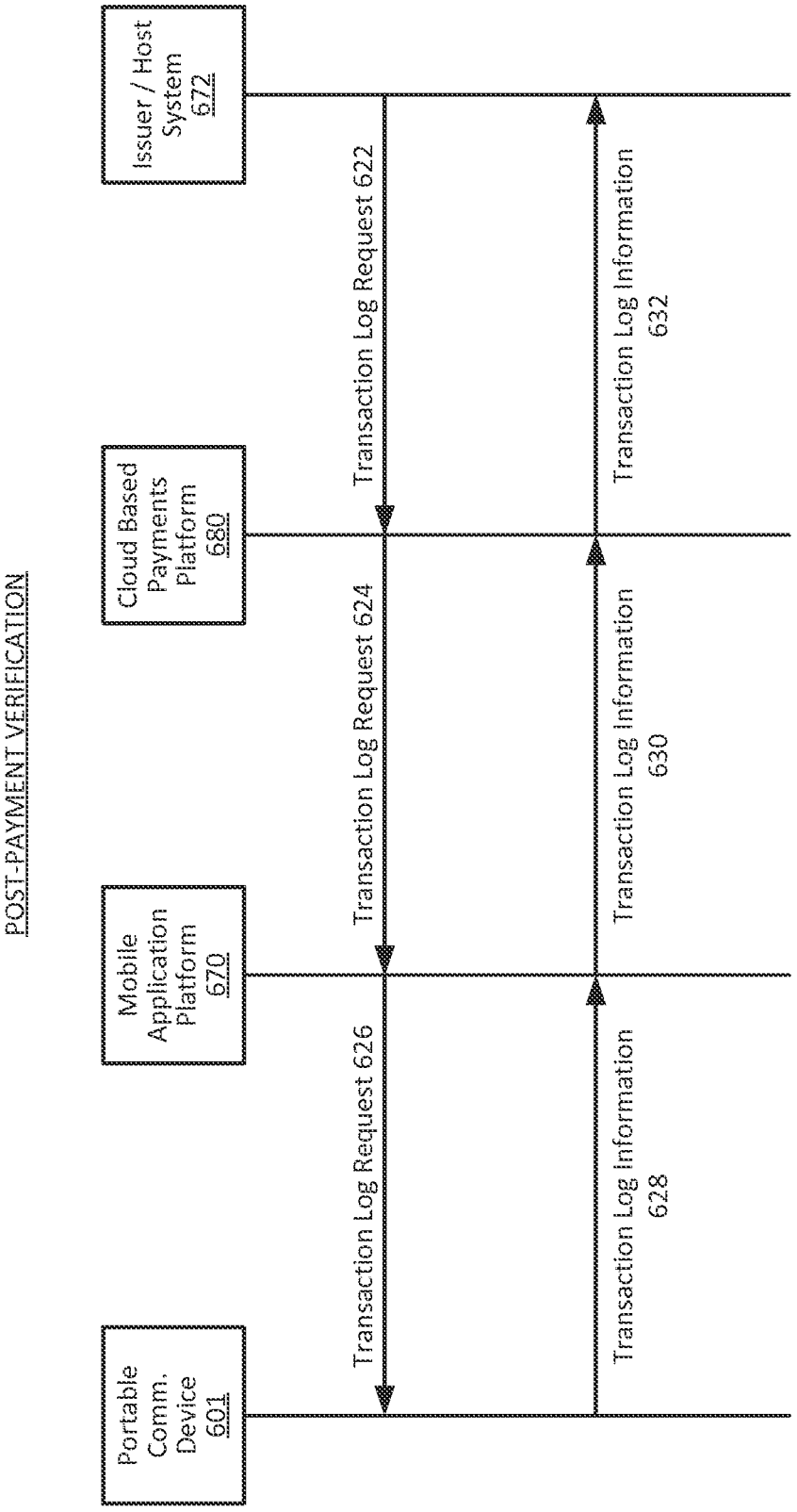

POST-PAYMENT VERIFICATION
Portable Comm. Device 601
Mobile Application Platform 670
Cloud Based Payments Platform 680
Issuer / Host System 672
Transaction Log Request 626
Transaction Log Request 624
Transaction Log Request 622
Transaction Log Information 628
Transaction Log Information 630
Transaction Log Information 632

FIG. 6

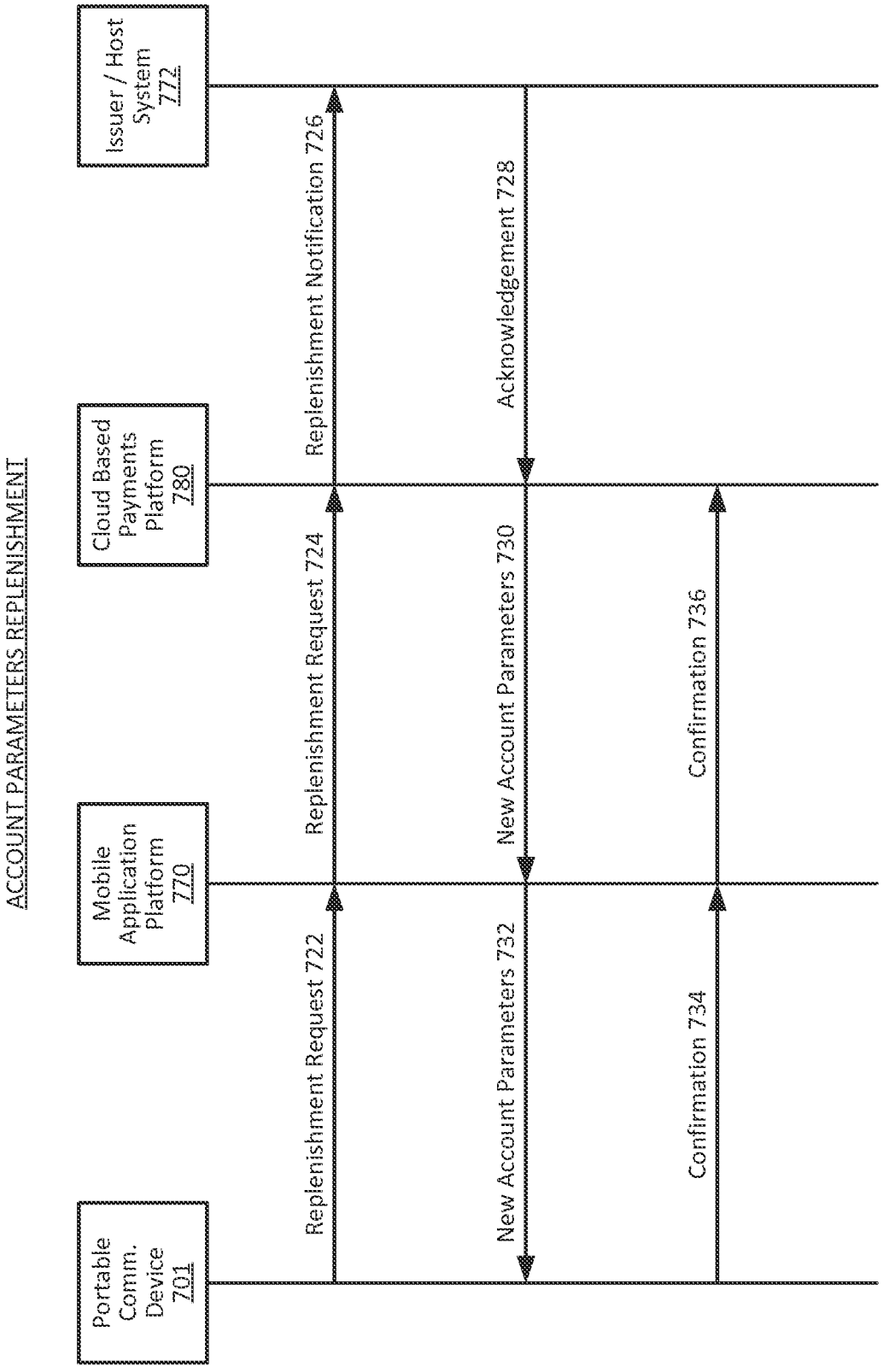

ACCOUNT PARAMETERS REPLENISHMENT
Portable Comm. Device 701
Mobile Application Platform 770
Cloud Based Payments Platform 780
Issuer / Host System 772
Replenishment Request 722
Replenishment Request 724
Replenishment Notification 726
Acknowledgement 728
New Account Parameters 730
New Account Parameters 732
Confirmation 734
Confirmation 736

FIG. 7

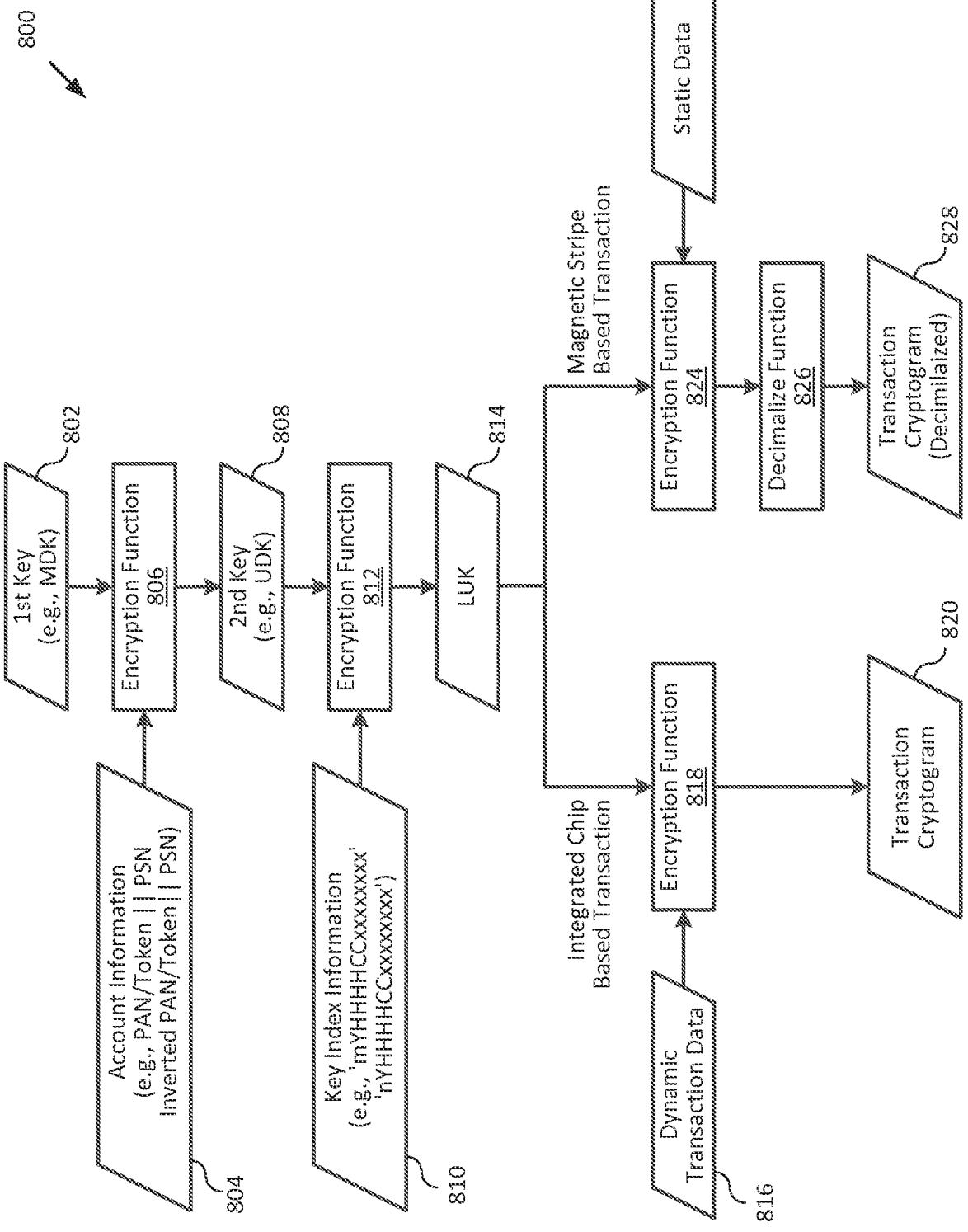

800
1st Key (e.g., MDK)
802
Encryption Function 806
2nd Key (e.g., UDK)
808
Encryption Function 812
LUK
814
Account Information (e.g., PAN/Token || PSN Inverted PAN/Token || PSN)
804
Key Index Information (e.g., 'mYHHHHCCxxxxxxx' 'nYHHHHCCxxxxxxx')
810
Magnetic Stripe Based Transaction
Integrated Chip Based Transaction
Static Data
822
Encryption Function 824
Decimalize Function 826
Transaction Cryptogram (Decimilaized)
828
Encryption Function 818
Dynamic Transaction Data
816
Transaction Cryptogram
820

FIG. 8

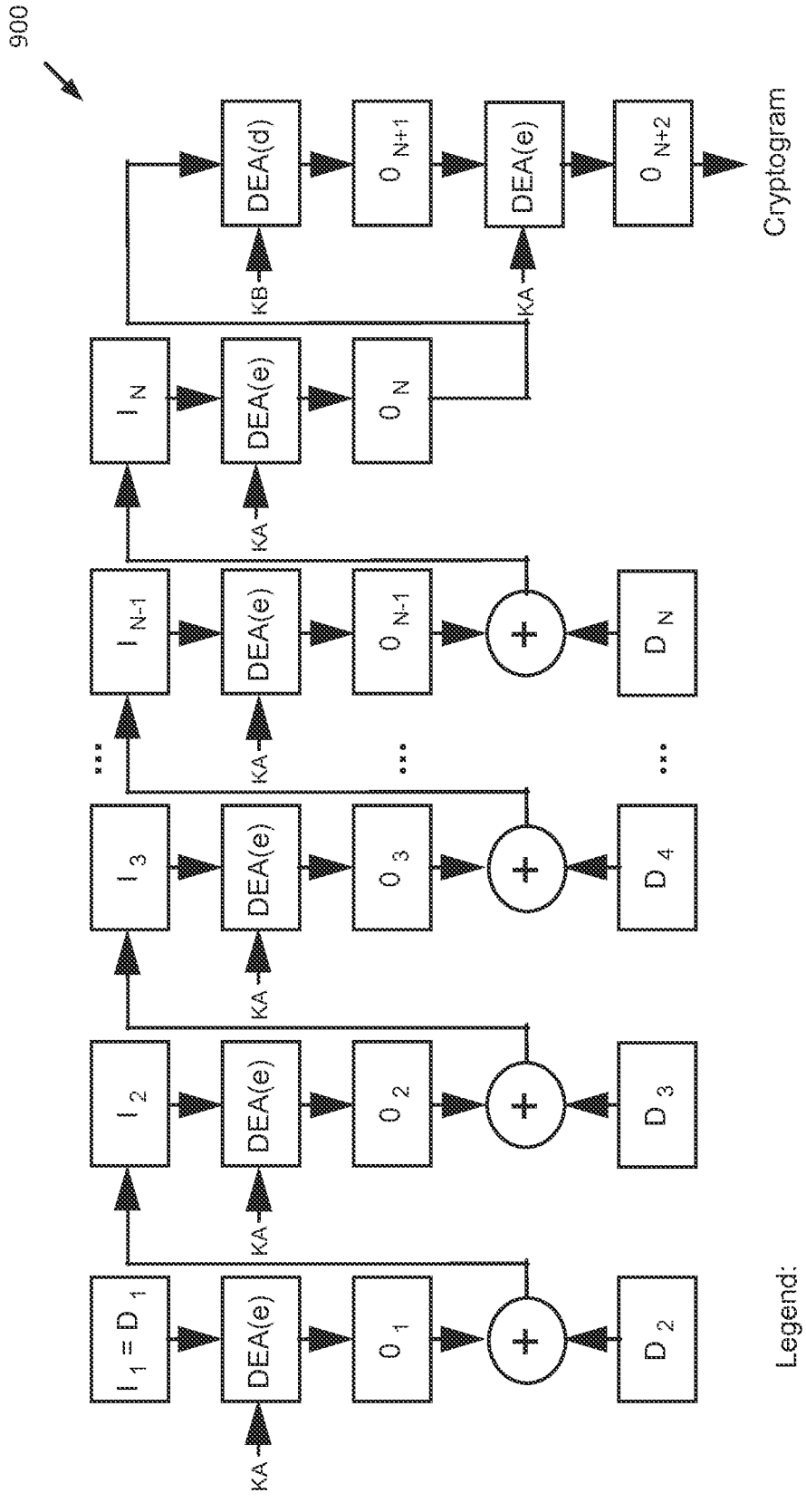

900
I 1 = D 1
DEA(e)
KA
O 1
I 2
O 2
I 3
O 3
I N-1
O N-1
I N
O N
DEA(d)
KB
O N+1
DEA(e)
O N+2
Cryptogram
D 2
D 3
D 4
D N
Legend:
I = Input
DEA(e) = Data Encryption Algorithm (encipherment mode)
DEA(d) = Data Encryption Algorithm (decipherment mode)
O = Output
D Data block
KA = Key A
KB = Key B
+ = Exclusive-OR

FIG. 9

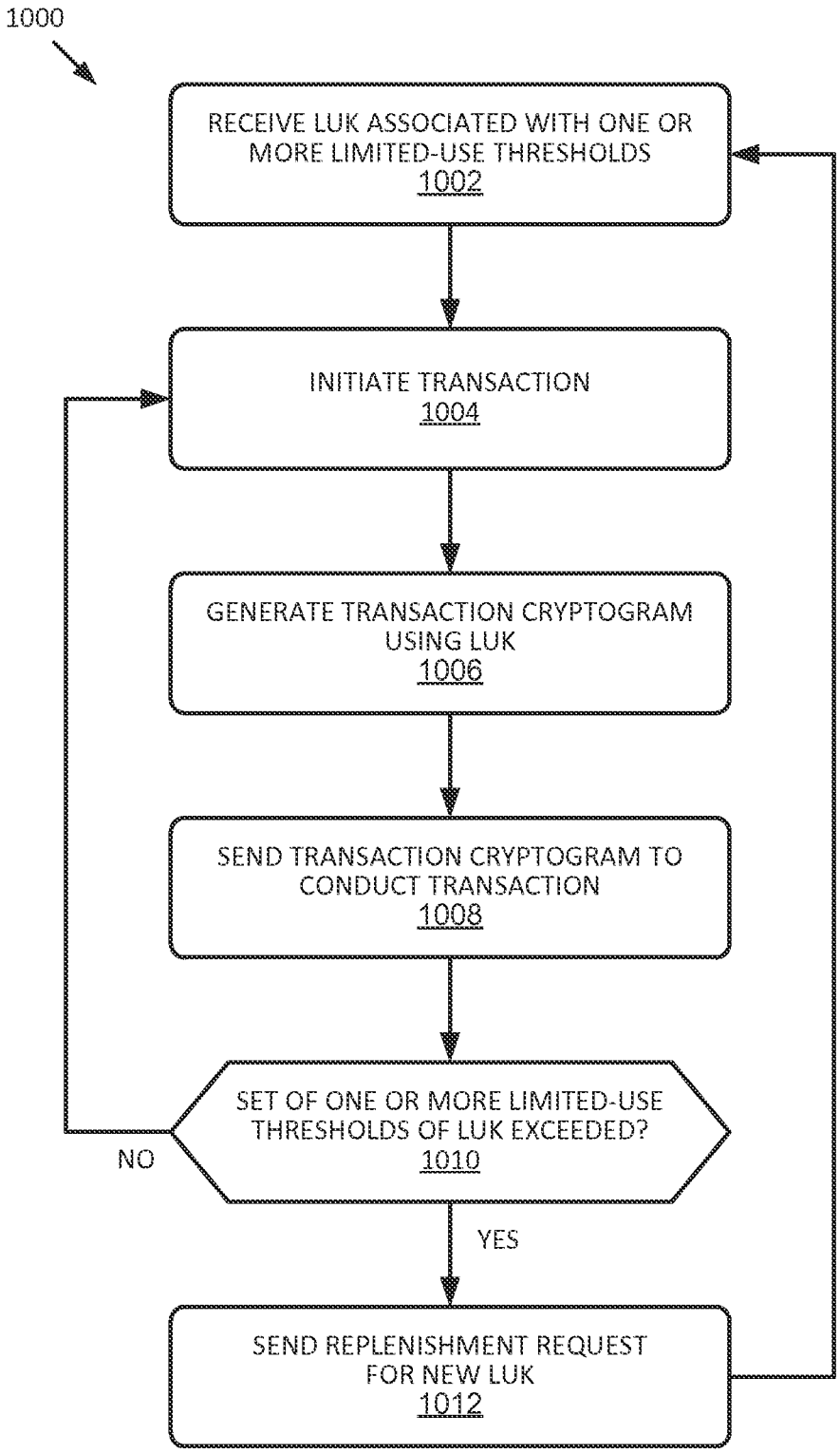

1000
RECEIVE LUK ASSOCIATED WITH ONE OR MORE LIMITED-USE THRESHOLDS
1002
INITIATE TRANSACTION
1004
GENERATE TRANSACTION CRYPTOGRAM USING LUK
1006
SEND TRANSACTION CRYPTOGRAM TO CONDUCT TRANSACTION
1008
SET OF ONE OR MORE LIMITED-USE THRESHOLDS OF LUK EXCEEDED?
1010
NO
YES
SEND REPLENISHMENT REQUEST FOR NEW LUK
1012

FIG. 10

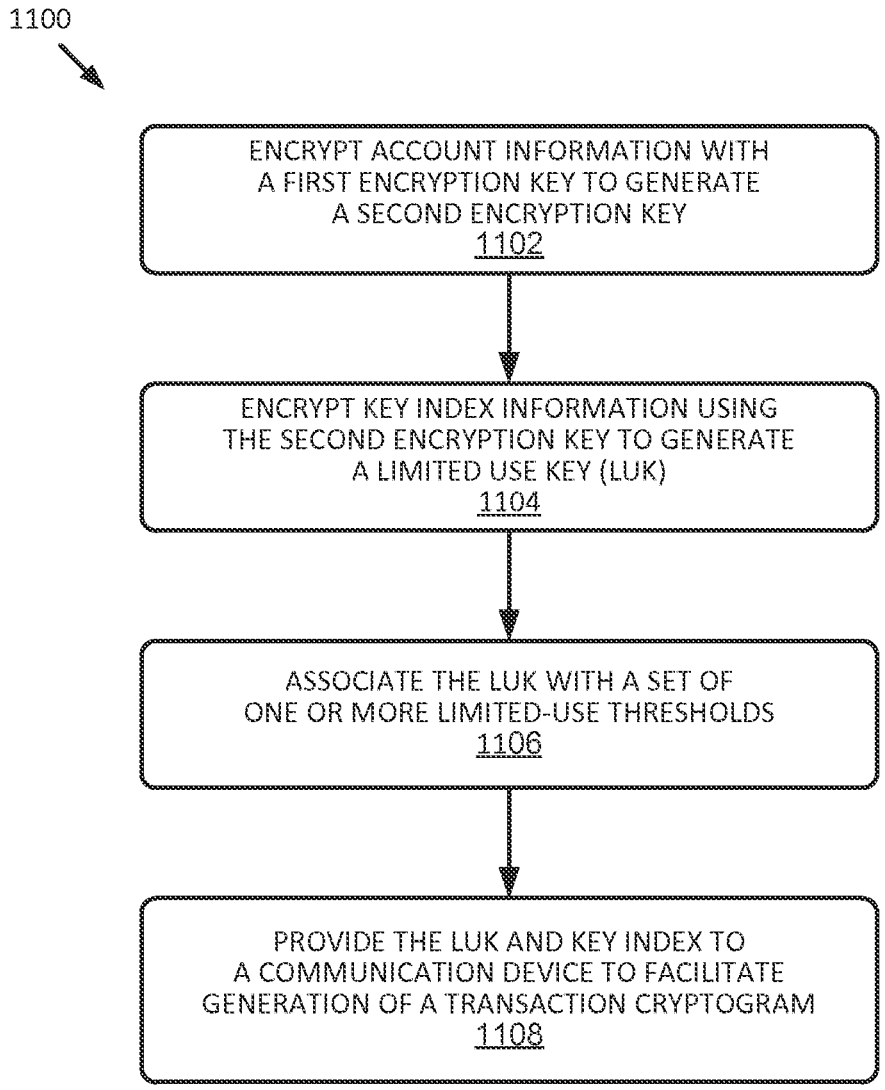

1100
ENCRYPT ACCOUNT INFORMATION WITH A FIRST ENCRYPTION KEY TO GENERATE A SECOND ENCRYPTION KEY
1102
ENCRYPT KEY INDEX INFORMATION USING THE SECOND ENCRYPTION KEY TO GENERATE A LIMITED USE KEY (LUK)
1104
ASSOCIATE THE LUK WITH A SET OF ONE OR MORE LIMITED-USE THRESHOLDS
1106
PROVIDE THE LUK AND KEY INDEX TO A COMMUNICATION DEVICE TO FACILITATE GENERATION OF A TRANSACTION CRYPTOGRAM
1108

FIG. 11

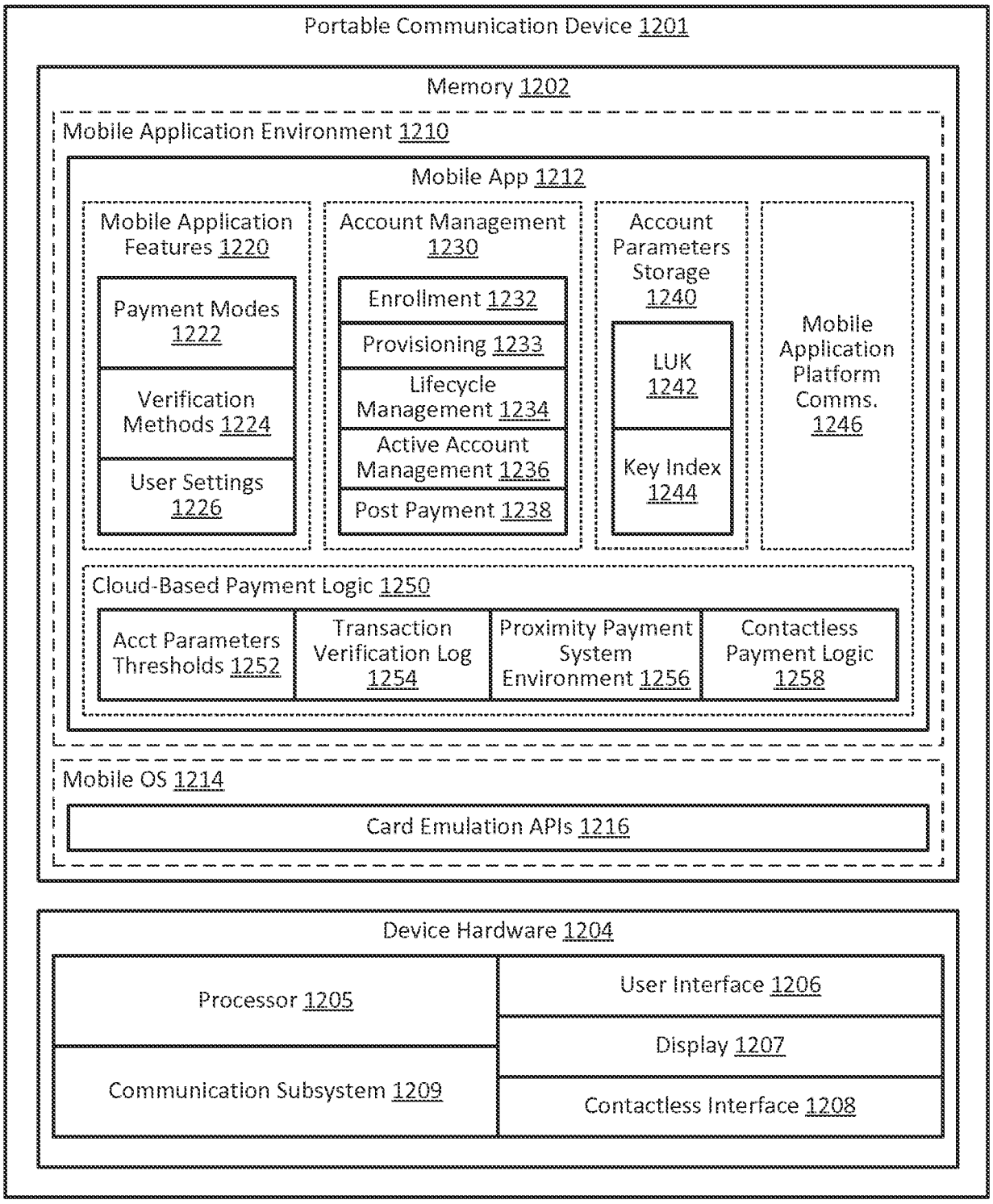

Portable Communication Device 1201
Memory 1202
Mobile Application Environment 1210
Mobile App 1212
Mobile Application Features 1220
Payment Modes 1222
Verification Methods 1224
User Settings 1226
Account Management 1230
Enrollment 1232
Provisioning 1233
Lifecycle Management 1234
Active Account Management 1236
Post Payment 1238
Account Parameters Storage 1240
LUK 1242
Key Index 1244
Mobile Application Platform Comms. 1246
Cloud-Based Payment Logic 1250
Acct Parameters Thresholds 1252
Transaction Verification Log 1254
Proximity Payment System Environment 1256
Contactless Payment Logic 1258
Mobile OS 1214
Card Emulation APIs 1216
Device Hardware 1204
Processor 1205
User Interface 1206
Display 1207
Communication Subsystem 1209
Contactless Interface 1208

FIG. 12

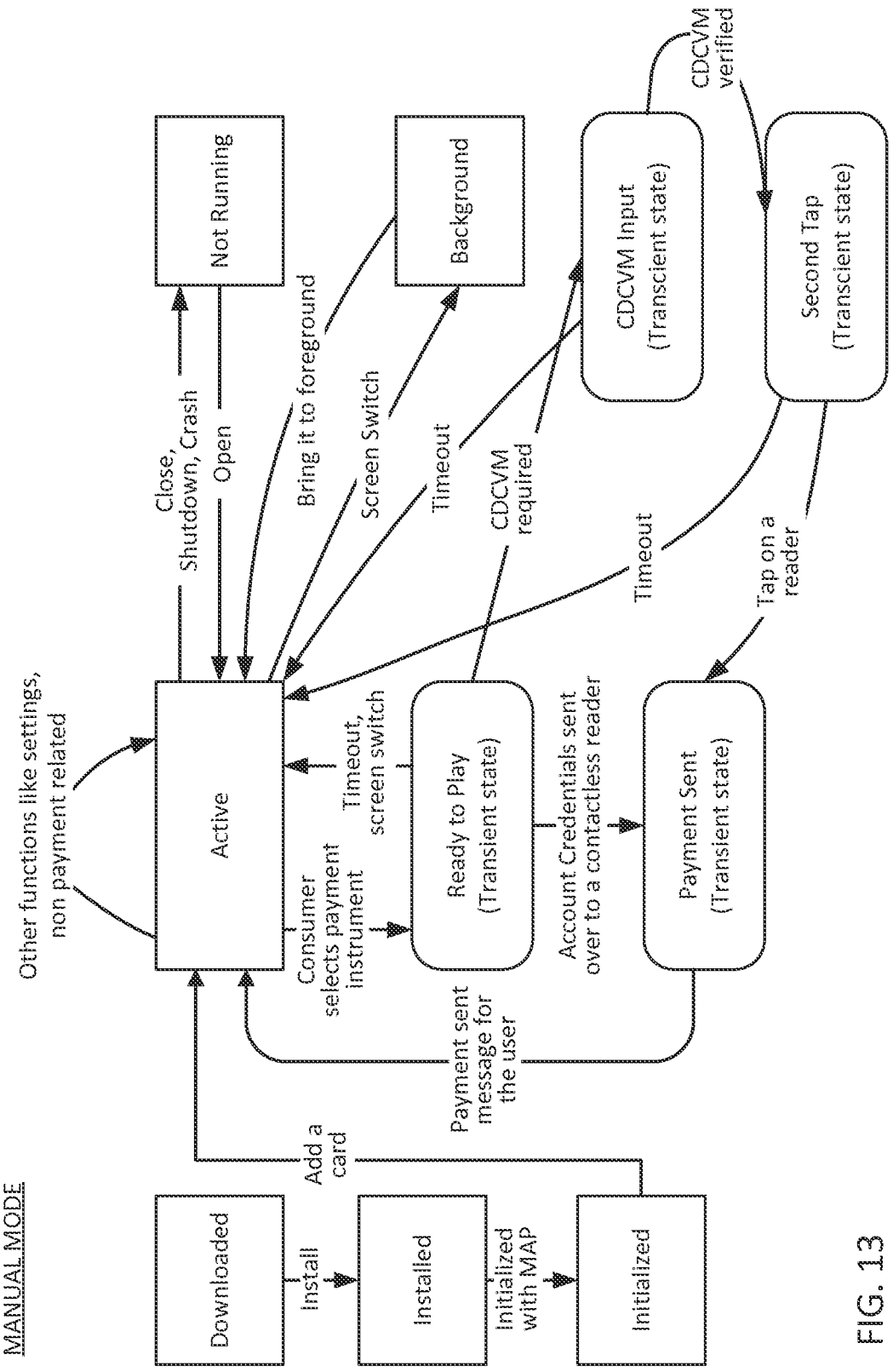

MANUAL MODE
Downloaded
Install
Installed
Initialized with MAP
Initialized
Add a card
Payment sent message for the user
Other functions like settings, non payment related
Active
Consumer selects payment instrument
Timeout, screen switch
Ready to Play (Transient state)
Account Credentials sent over to a contactless reader
Payment Sent (Transient state)
Tap on a reader
Timeout
CDCVM required
Timeout
Screen Switch
Bring it to foreground
Close, Shutdown, Crash
Open
Not Running
Background
CDCVM Input (Transcient state)
CDCVM verified
Second Tap (Transcient state)

FIG. 13

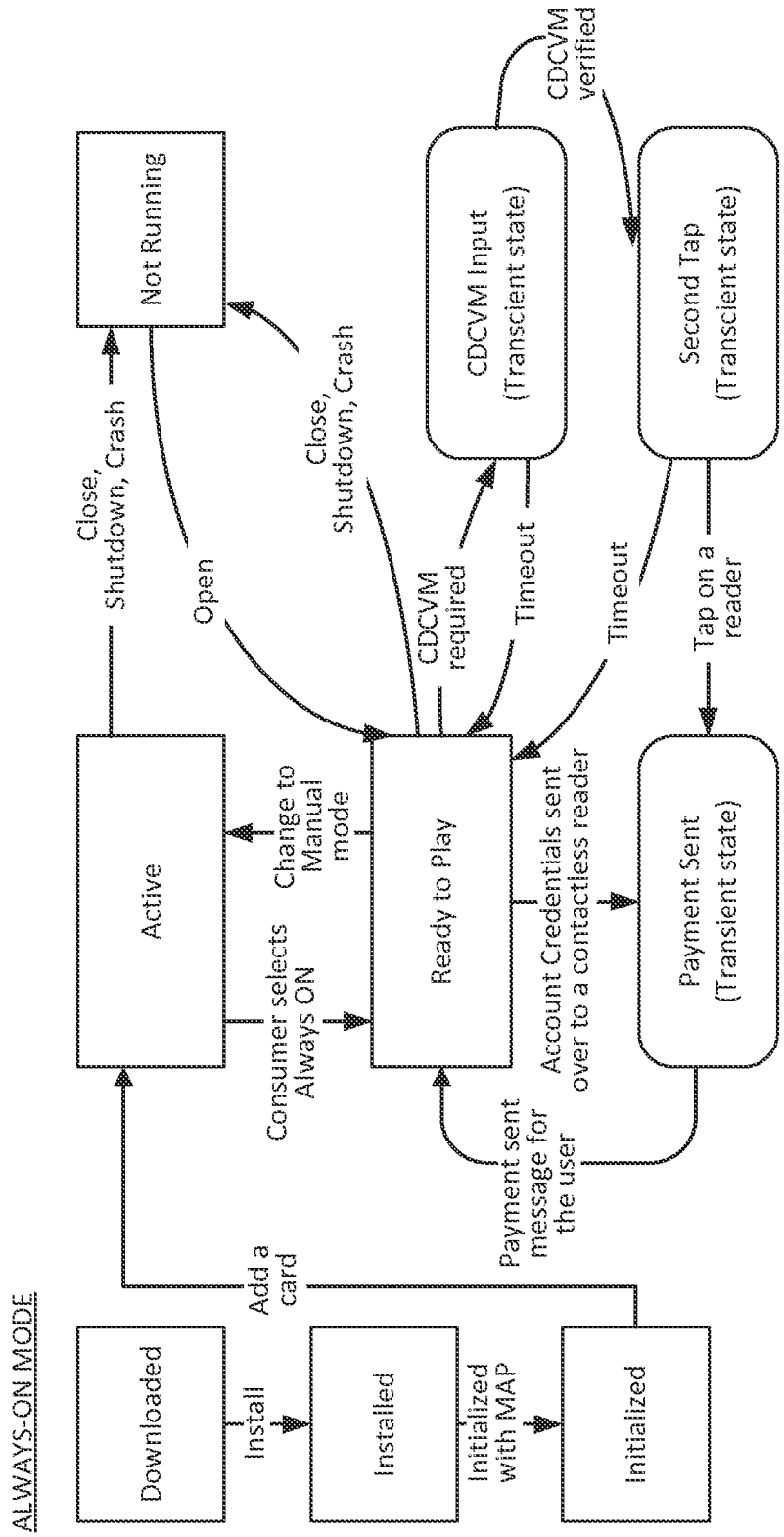

ALWAYS-ON MODE
Downloaded
Install
Installed
Initialized with MAP
Initialized
Add a card
Active
Not Running
Close, Shutdown, Crash
Open
Change to Manual mode
Consumer selects Always ON
Ready to Play
Close, Shutdown, Crash
CDCVM required
CDCVM Input (Transcient state)
Timeout
CDCVM verified
Second Tap (Transcient state)
Timeout
Tap on a reader
Account Credentials sent over to a contactless reader
Payment Sent (Transient state)
Payment sent message for the user

FIG. 14

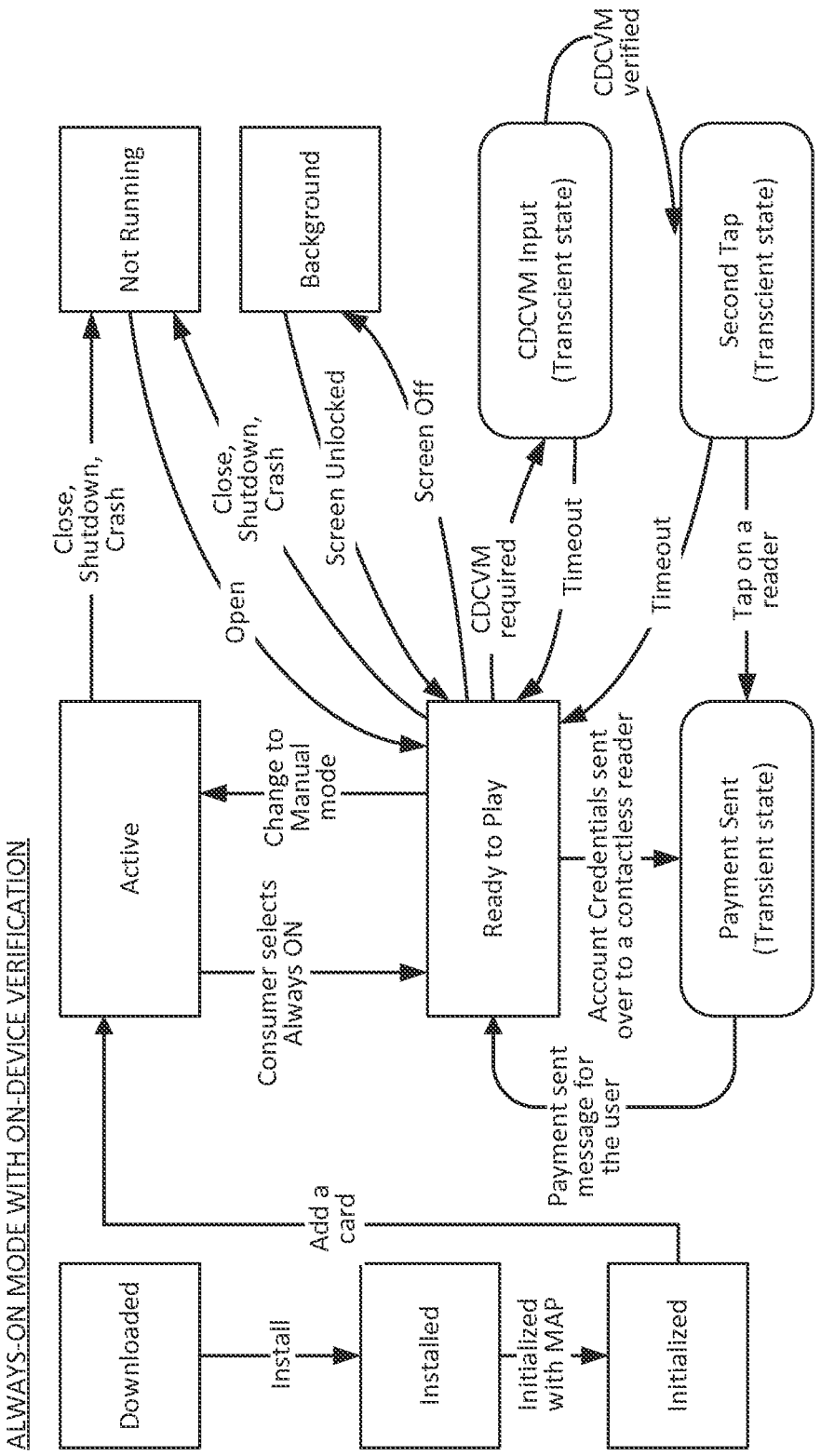

ALWAYS-ON MODE WITH ON-DEVICE VERIFICATION
Downloaded
Install
Installed
Initialized with MAP
Initialized
Add a card
Payment sent message for the user
Active
Consumer selects Always ON
Change to Manual mode
Ready to Play
Account Credentials sent over to a contactless reader
Payment Sent (Transient state)
Close, Shutdown, Crash
Not Running
Open
Close, Shutdown, Crash
Background
Screen Unlocked
Screen Off
CDCVM required
CDCVM Input (Transcient state)
Timeout
CDCVM verified
Second Tap (Transcient state)
Timeout
Tap on a reader

FIG. 15

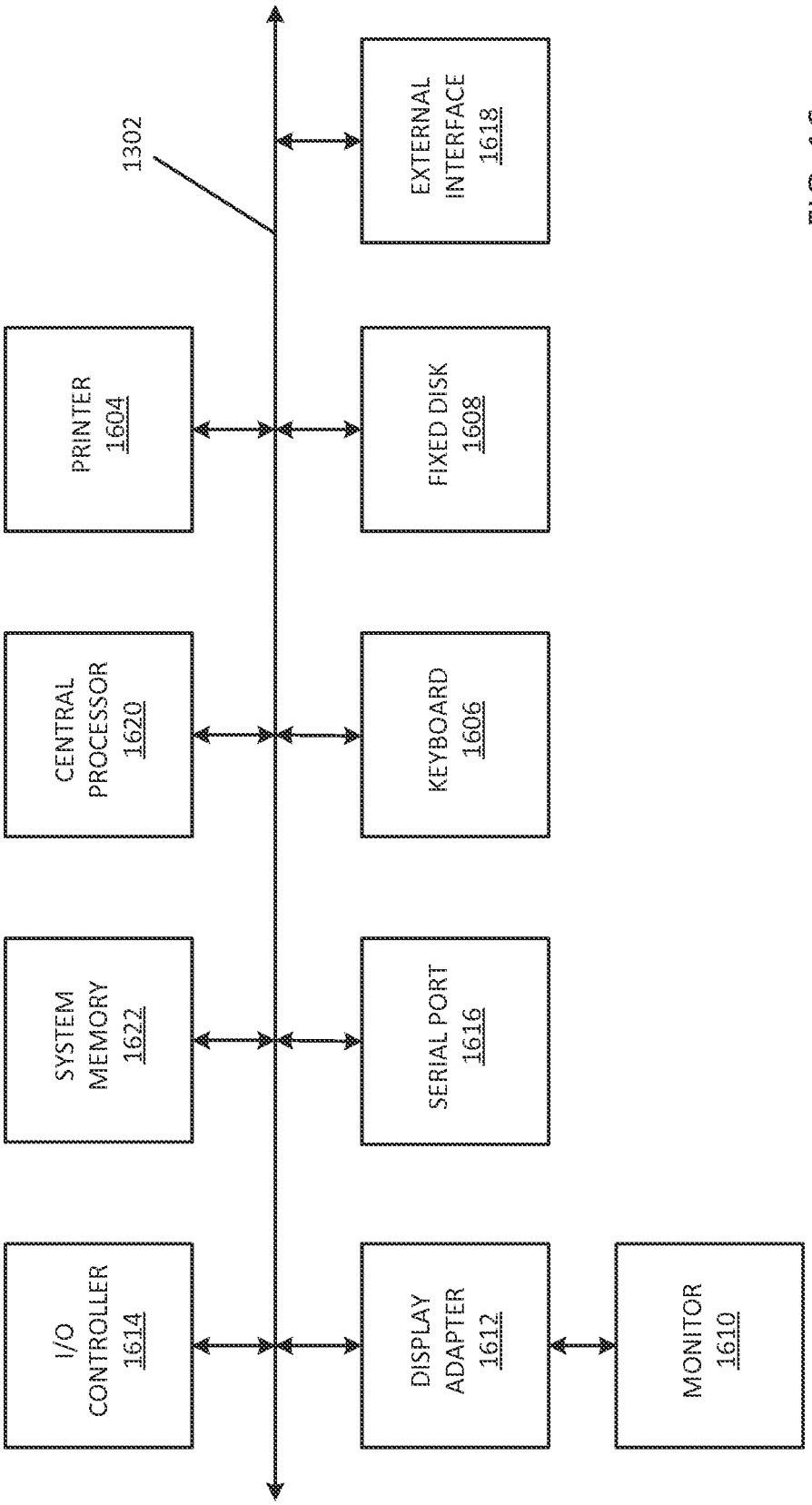

1302
EXTERNAL INTERFACE 1618
PRINTER 1604
FIXED DISK 1608
CENTRAL PROCESSOR 1620
KEYBOARD 1606
SYSTEM MEMORY 1622
SERIAL PORT 1616
I/O CONTROLLER 1614
DISPLAY ADAPTER 1612
MONITOR 1610

FIG. 16