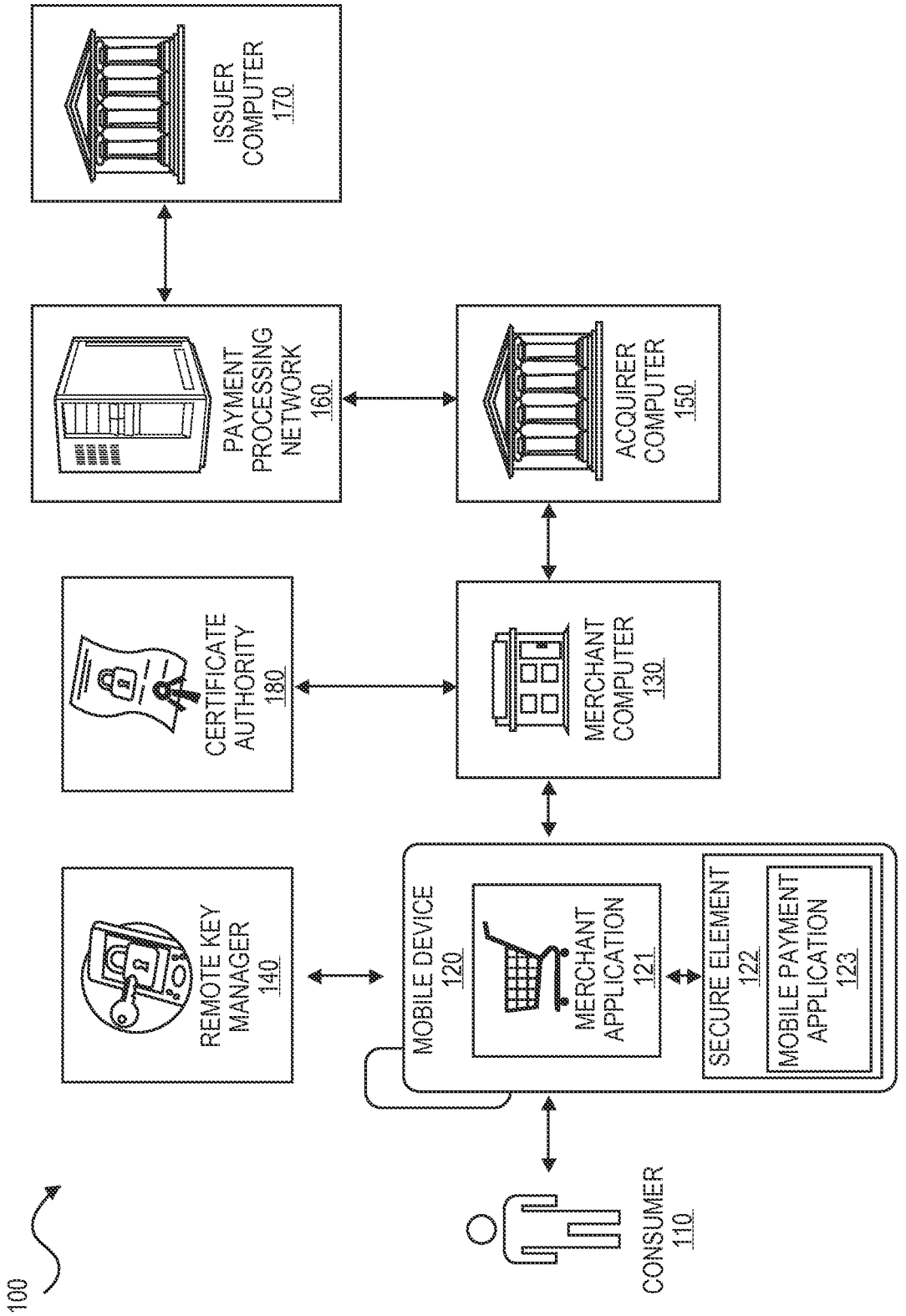

ISSUER COMPUTER 170
PAYMENT PROCESSING NETWORK 160
ACQUIRER COMPUTER 150
CERTIFICATE AUTHORITY 180
MERCHANT COMPUTER 130
REMOTE KEY MANAGER 140
MOBILE DEVICE 120
MERCHANT APPLICATION 121
SECURE ELEMENT 122
MOBILE PAYMENT APPLICATION 123
CONSUMER 110
100

FIG. 1

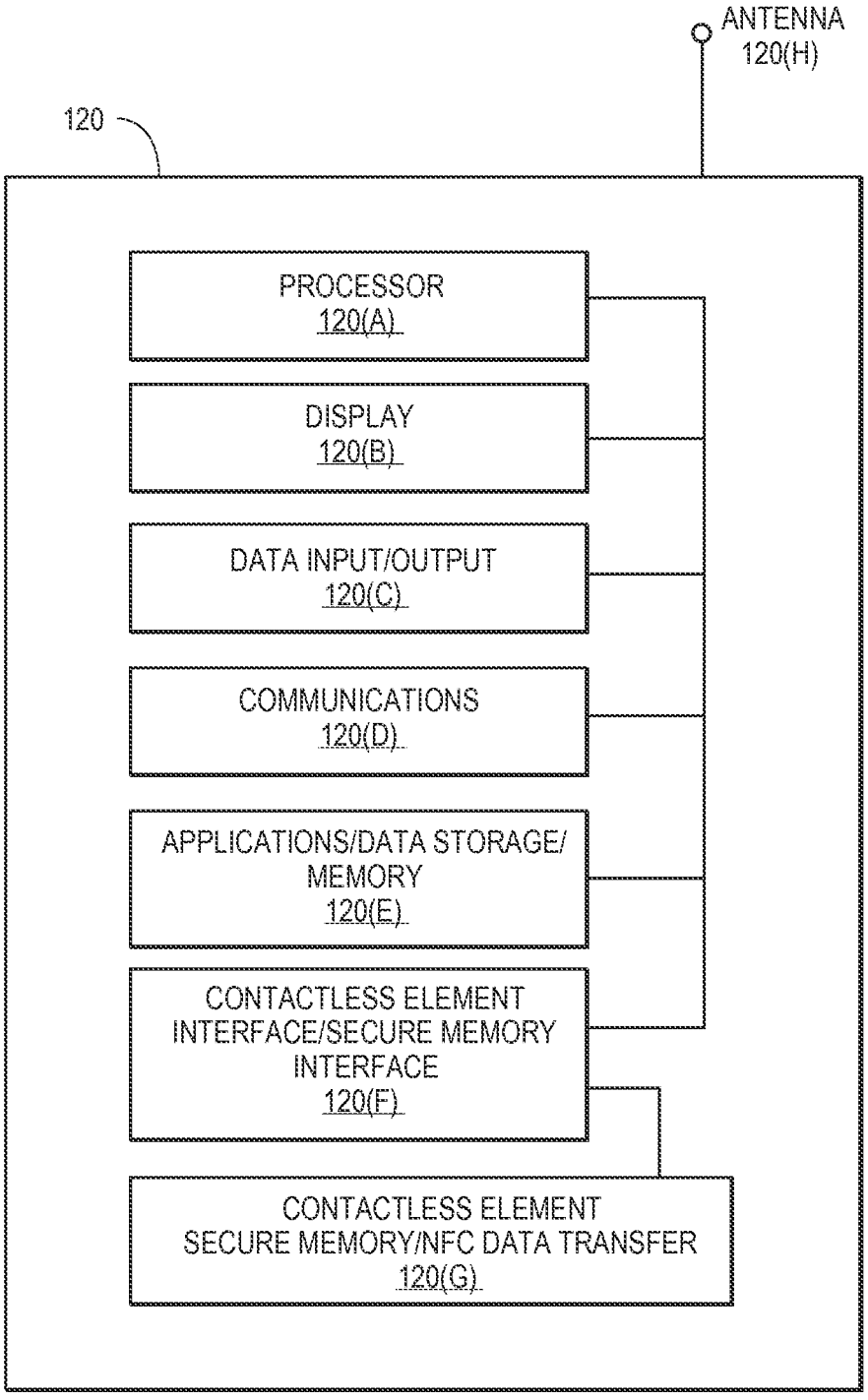

ANTENNA
120(H)
120
PROCESSOR
120(A)
DISPLAY
120(B)
DATA INPUT/OUTPUT
120(C)
COMMUNICATIONS
120(D)
APPLICATIONS/DATA STORAGE/
MEMORY
120(E)
CONTACTLESS ELEMENT
INTERFACE/SECURE MEMORY
INTERFACE
120(F)
CONTACTLESS ELEMENT
SECURE MEMORY/NFC DATA TRANSFER
120(G)

FIG. 2

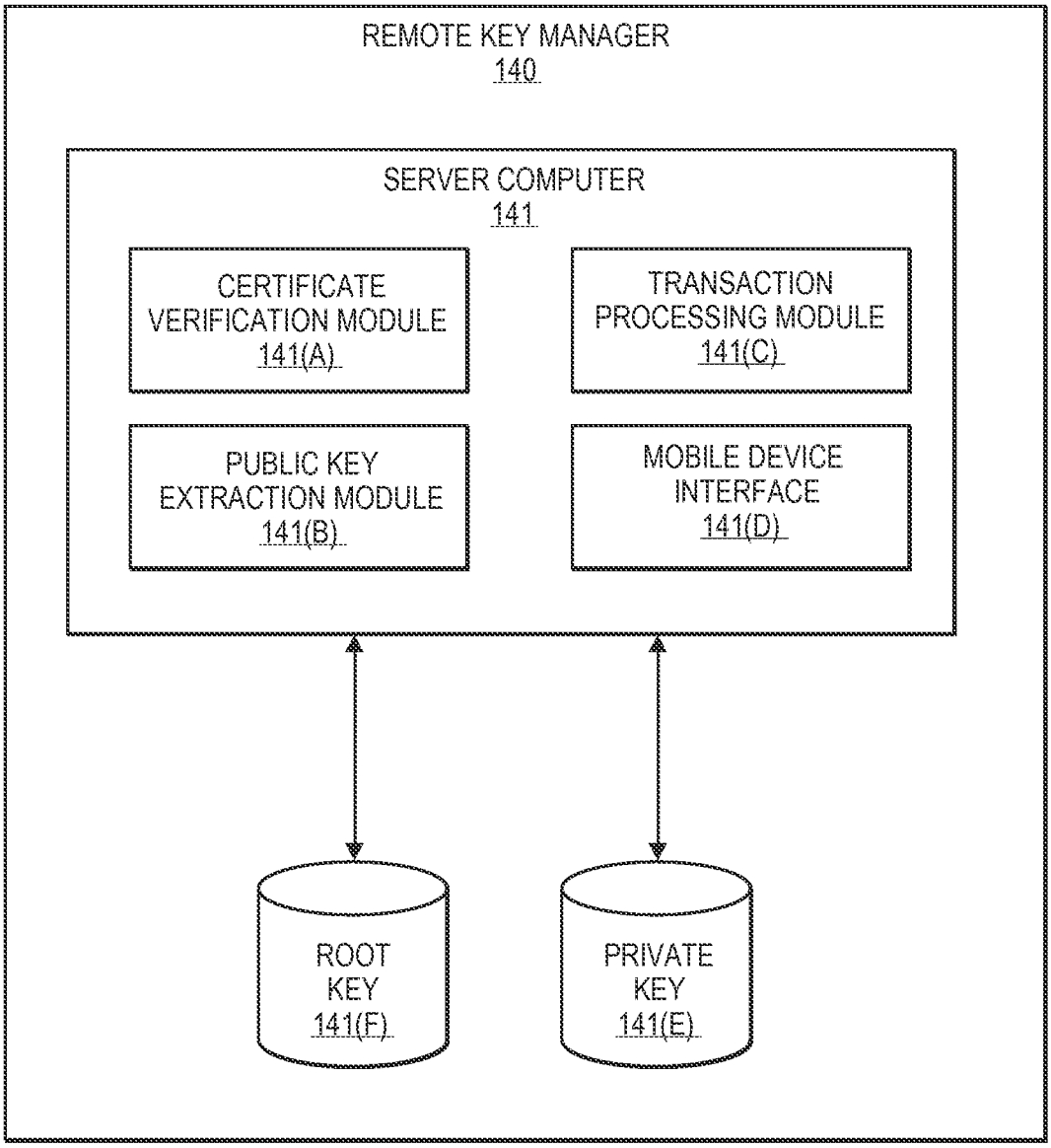

REMOTE KEY MANAGER
140
SERVER COMPUTER
141
CERTIFICATE VERIFICATION MODULE
141(A)
TRANSACTION PROCESSING MODULE
141(C)
PUBLIC KEY EXTRACTION MODULE
141(B)
MOBILE DEVICE INTERFACE
141(D)
ROOT KEY
141(F)
PRIVATE KEY
141(E)

FIG. 3

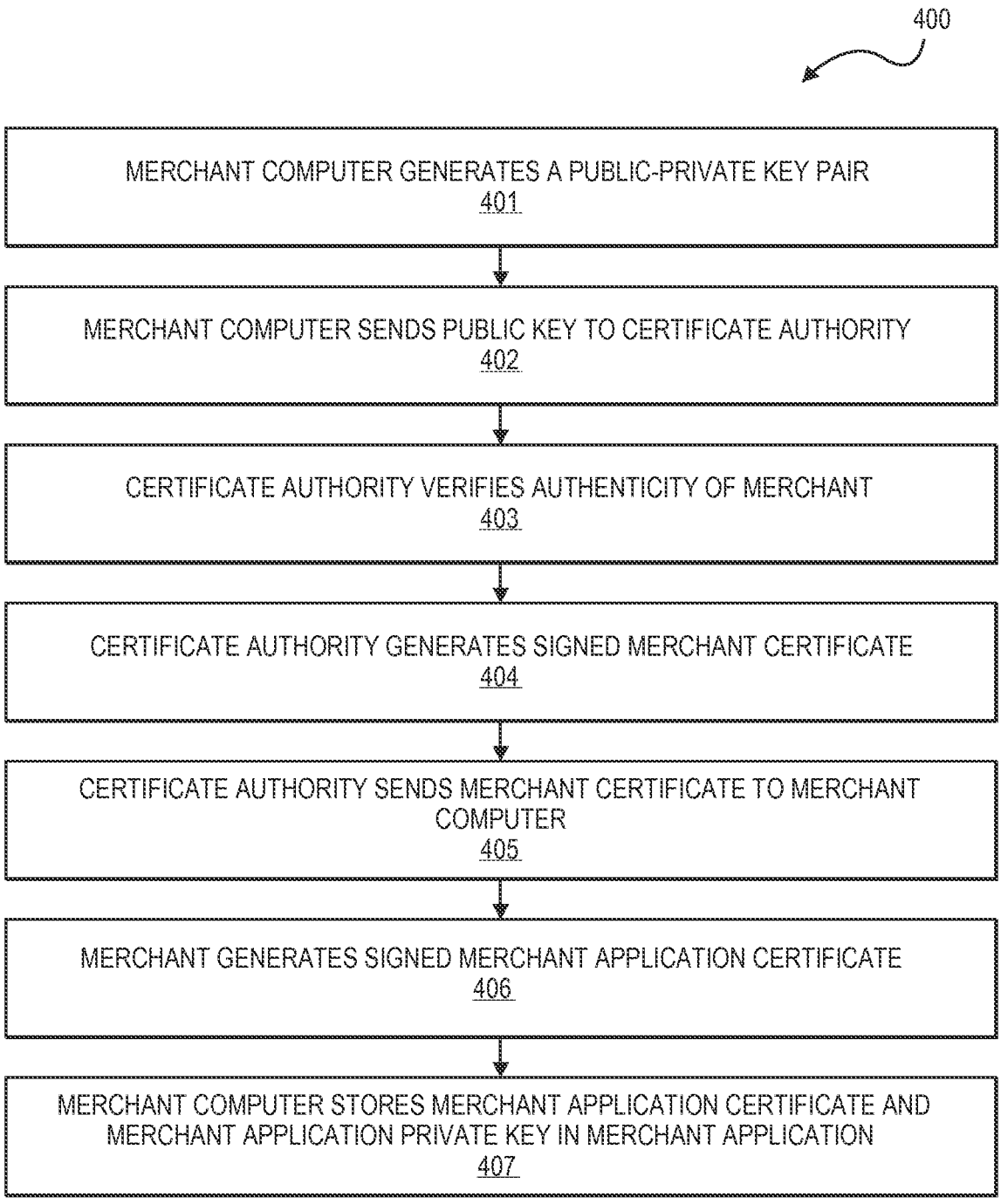
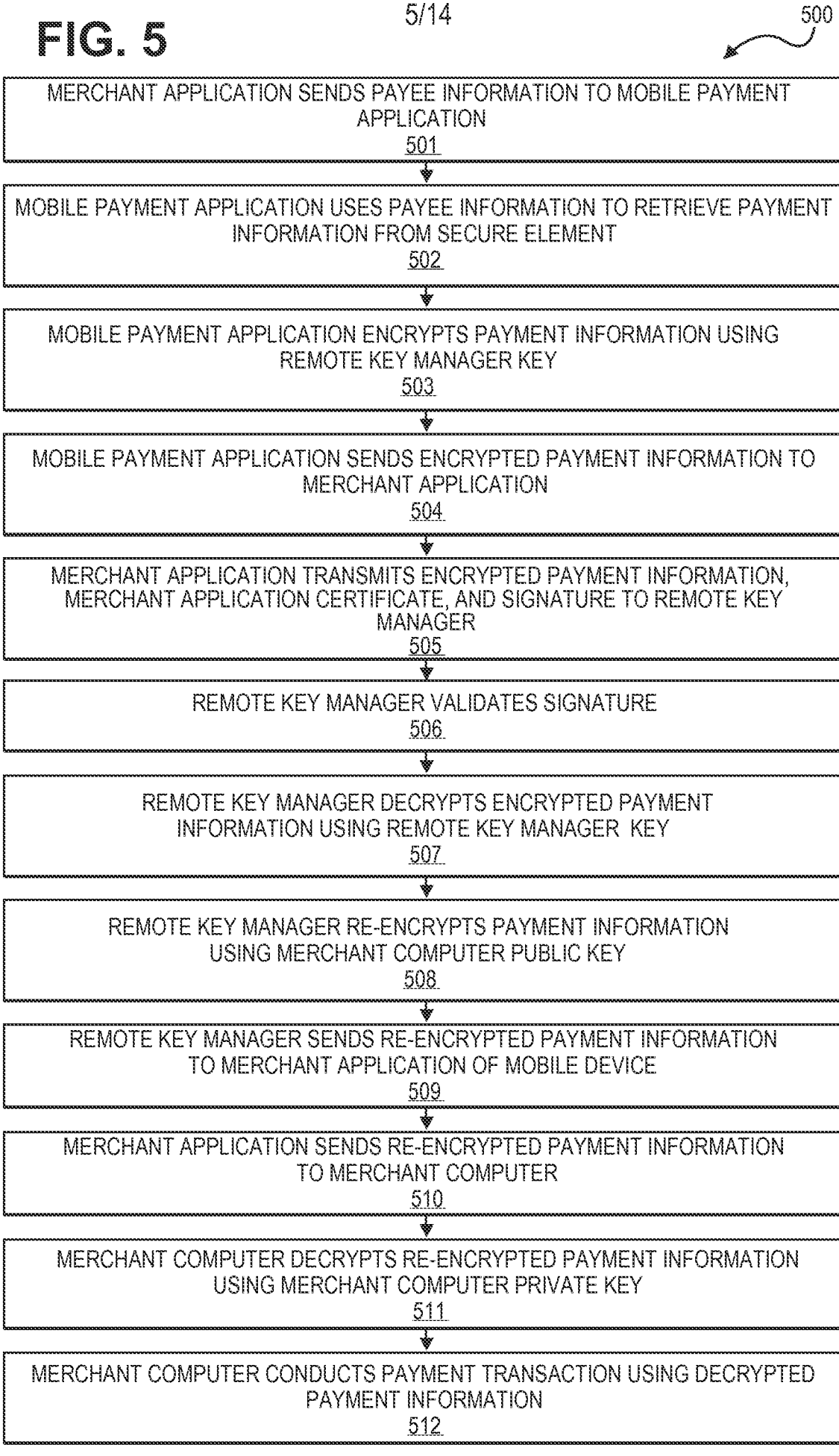

400
MERCHANT COMPUTER GENERATES A PUBLIC-PRIVATE KEY PAIR
401
MERCHANT COMPUTER SENDS PUBLIC KEY TO CERTIFICATE AUTHORITY
402
CERTIFICATE AUTHORITY VERIFIES AUTHENTICITY OF MERCHANT
403
CERTIFICATE AUTHORITY GENERATES SIGNED MERCHANT CERTIFICATE
404
CERTIFICATE AUTHORITY SENDS MERCHANT CERTIFICATE TO MERCHANT COMPUTER
405
MERCHANT GENERATES SIGNED MERCHANT APPLICATION CERTIFICATE
406
MERCHANT COMPUTER STORES MERCHANT APPLICATION CERTIFICATE AND MERCHANT APPLICATION PRIVATE KEY IN MERCHANT APPLICATION
407

FIG. 4

FIG. 5


500
MERCHANT APPLICATION SENDS PAYEE INFORMATION TO MOBILE PAYMENT APPLICATION
501
MOBILE PAYMENT APPLICATION USES PAYEE INFORMATION TO RETRIEVE PAYMENT INFORMATION FROM SECURE ELEMENT
502
MOBILE PAYMENT APPLICATION ENCRYPTS PAYMENT INFORMATION USING REMOTE KEY MANAGER KEY
503
MOBILE PAYMENT APPLICATION SENDS ENCRYPTED PAYMENT INFORMATION TO MERCHANT APPLICATION
504
MERCHANT APPLICATION TRANSMITS ENCRYPTED PAYMENT INFORMATION, MERCHANT APPLICATION CERTIFICATE, AND SIGNATURE TO REMOTE KEY MANAGER
505
REMOTE KEY MANAGER VALIDATES SIGNATURE
506
REMOTE KEY MANAGER DECRYPTS ENCRYPTED PAYMENT INFORMATION USING REMOTE KEY MANAGER KEY
507
REMOTE KEY MANAGER RE-ENCRYPTS PAYMENT INFORMATION USING MERCHANT COMPUTER PUBLIC KEY
508
REMOTE KEY MANAGER SENDS RE-ENCRYPTED PAYMENT INFORMATION TO MERCHANT APPLICATION OF MOBILE DEVICE
509
MERCHANT APPLICATION SENDS RE-ENCRYPTED PAYMENT INFORMATION TO MERCHANT COMPUTER
510
MERCHANT COMPUTER DECRYPTS RE-ENCRYPTED PAYMENT INFORMATION USING MERCHANT COMPUTER PRIVATE KEY
511
MERCHANT COMPUTER CONDUCTS PAYMENT TRANSACTION USING DECRYPTED PAYMENT INFORMATION
512

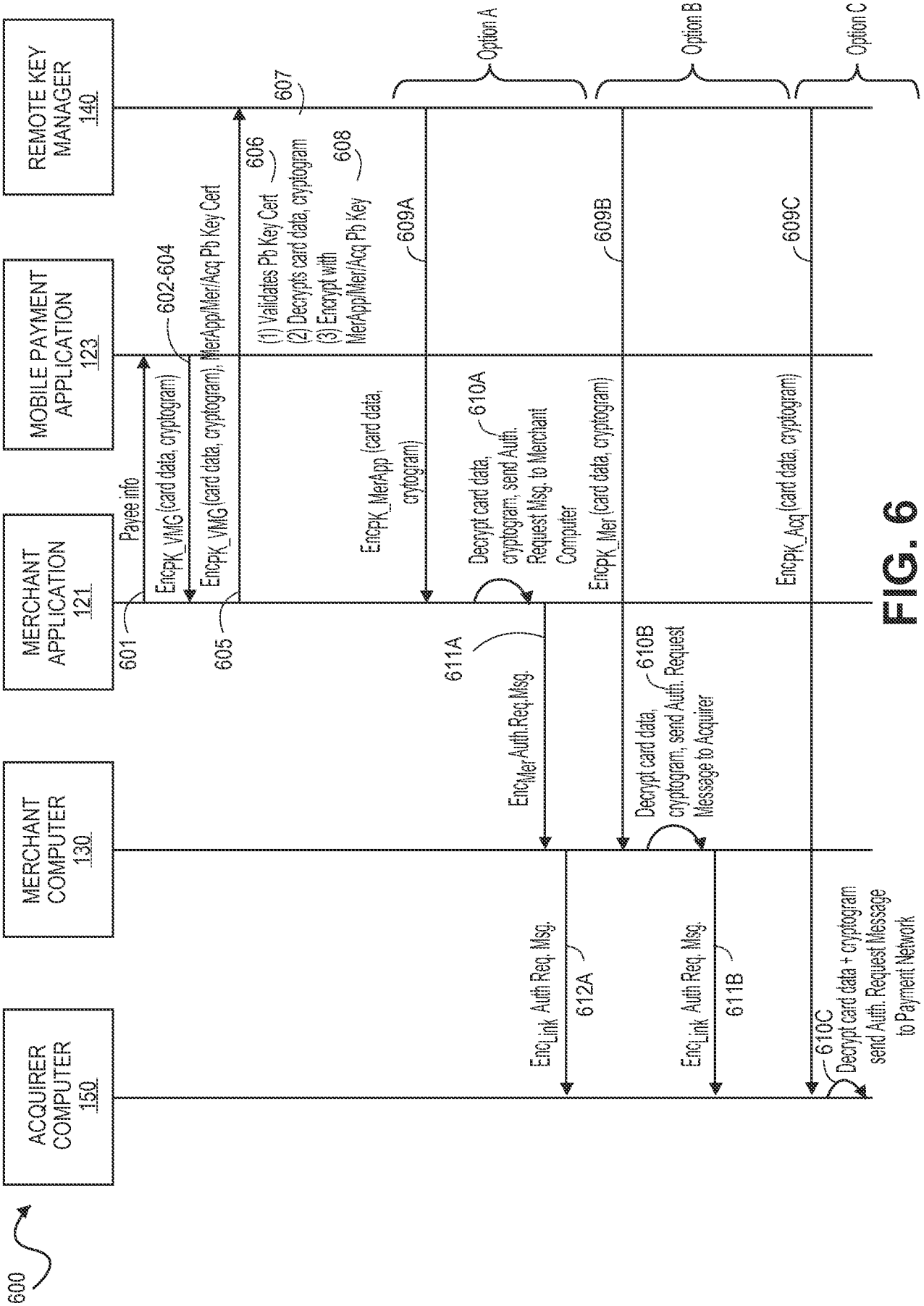

600
ACQUIRER COMPUTER 150
MERCHANT COMPUTER 130
MERCHANT APPLICATION 121
MOBILE PAYMENT APPLICATION 123
REMOTE KEY MANAGER 140
Option A
Option B
Option C
601
Payee info
Enc_PK_VMC (card data, cryptogram)
605
Enc_PK_VMC (card data, cryptogram), MerApp/Mer/Acq Pb Key Cert
602-604
606
(1) Validates Pb Key Cert
(2) Decrypts card data, cryptogram
(3) Encrypt with MerApp/Mer/Acq Pb Key
607
608
609A
Enc_PK_MerApp (card data, cryptogram)
610A
Decrypt card data, cryptogram, send Auth. Request Msg. to Merchant Computer
609B
Enc_PK_Mer (card data, cryptogram)
609C
Enc_PK_Acq (card data, cryptogram)
611A
Enc_Mer Auth.Req.Msg.
610B
Decrypt card data, cryptogram, send Auth. Request Message to Acquirer
612A
Enc_Link Auth Req. Msg.
611B
Enc_Link Auth Req. Msg.
610C
Decrypt card data + cryptogram send Auth. Request Message to Payment Network

FIG. 6

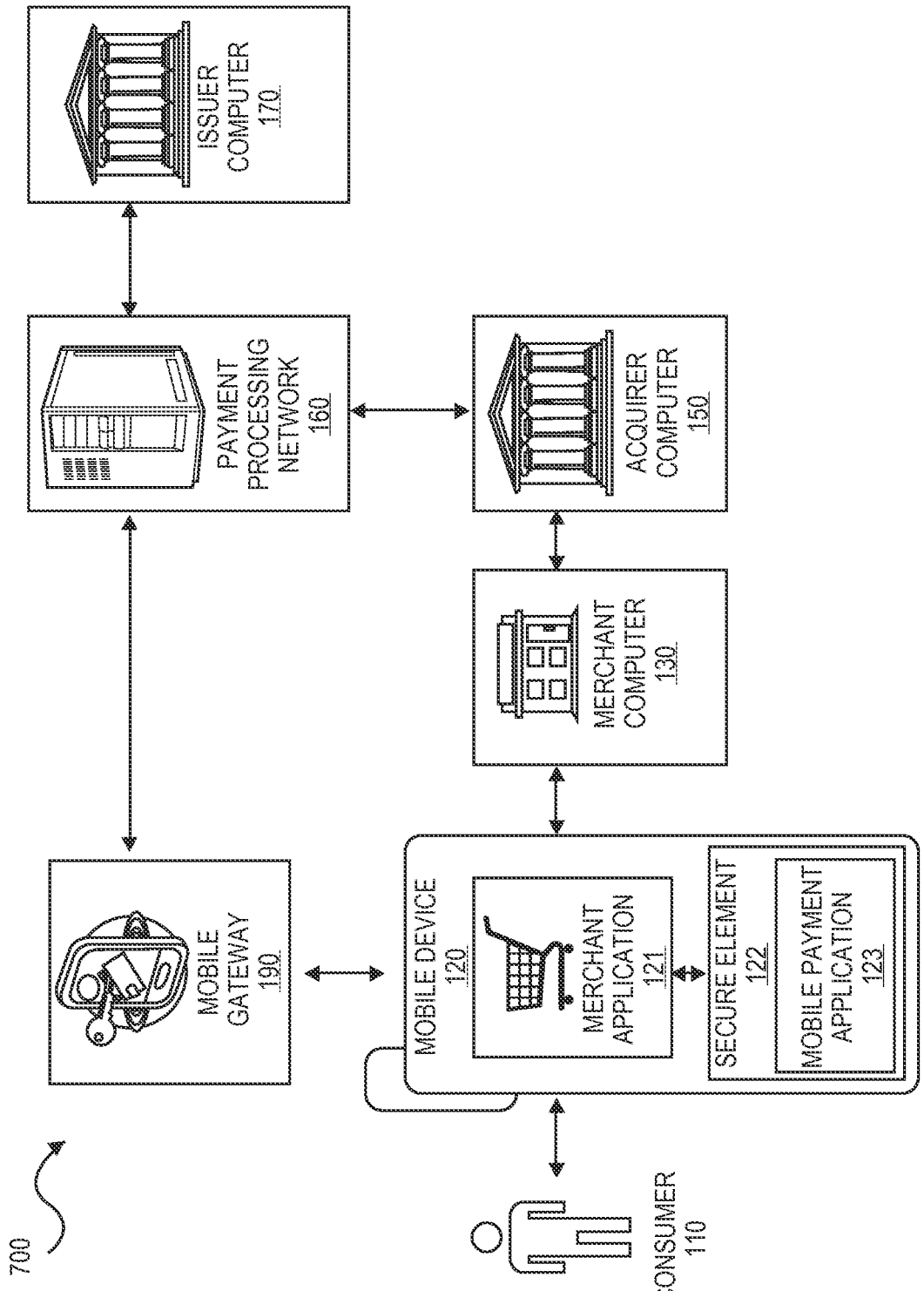

ISSUER COMPUTER 170
PAYMENT PROCESSING NETWORK 160
ACQUIRER COMPUTER 150
MERCHANT COMPUTER 130
MOBILE GATEWAY 190
MOBILE DEVICE 120
MERCHANT APPLICATION 121
SECURE ELEMENT 122
MOBILE PAYMENT APPLICATION 123
CONSUMER 110
700

FIG. 7

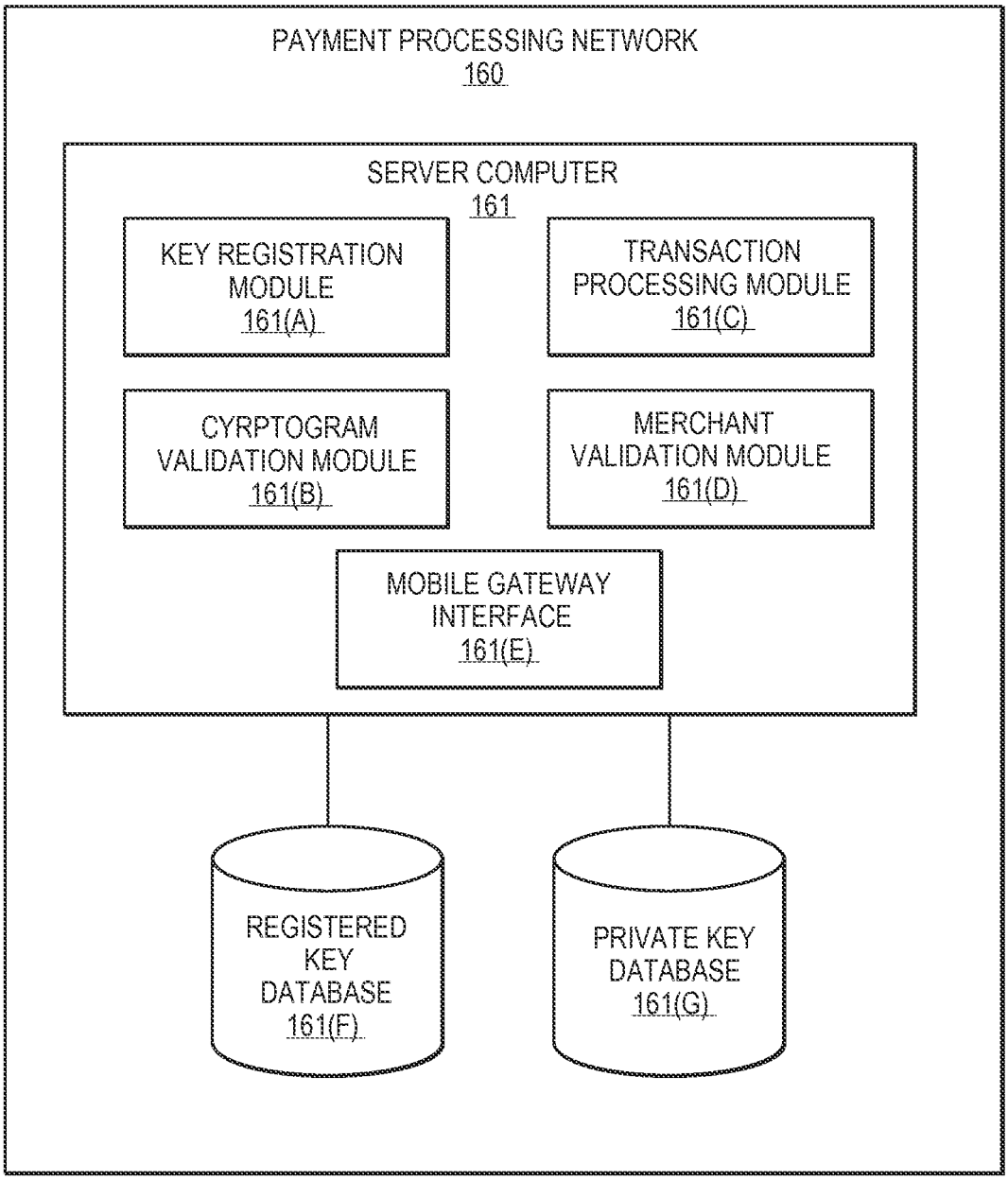

PAYMENT PROCESSING NETWORK
160
SERVER COMPUTER
161
KEY REGISTRATION MODULE
161(A)
TRANSACTION PROCESSING MODULE
161(C)
CYRPTOGRAM VALIDATION MODULE
161(B)
MERCHANT VALIDATION MODULE
161(D)
MOBILE GATEWAY INTERFACE
161(E)
REGISTERED KEY DATABASE
161(F)
PRIVATE KEY DATABASE
161(G)

FIG. 8

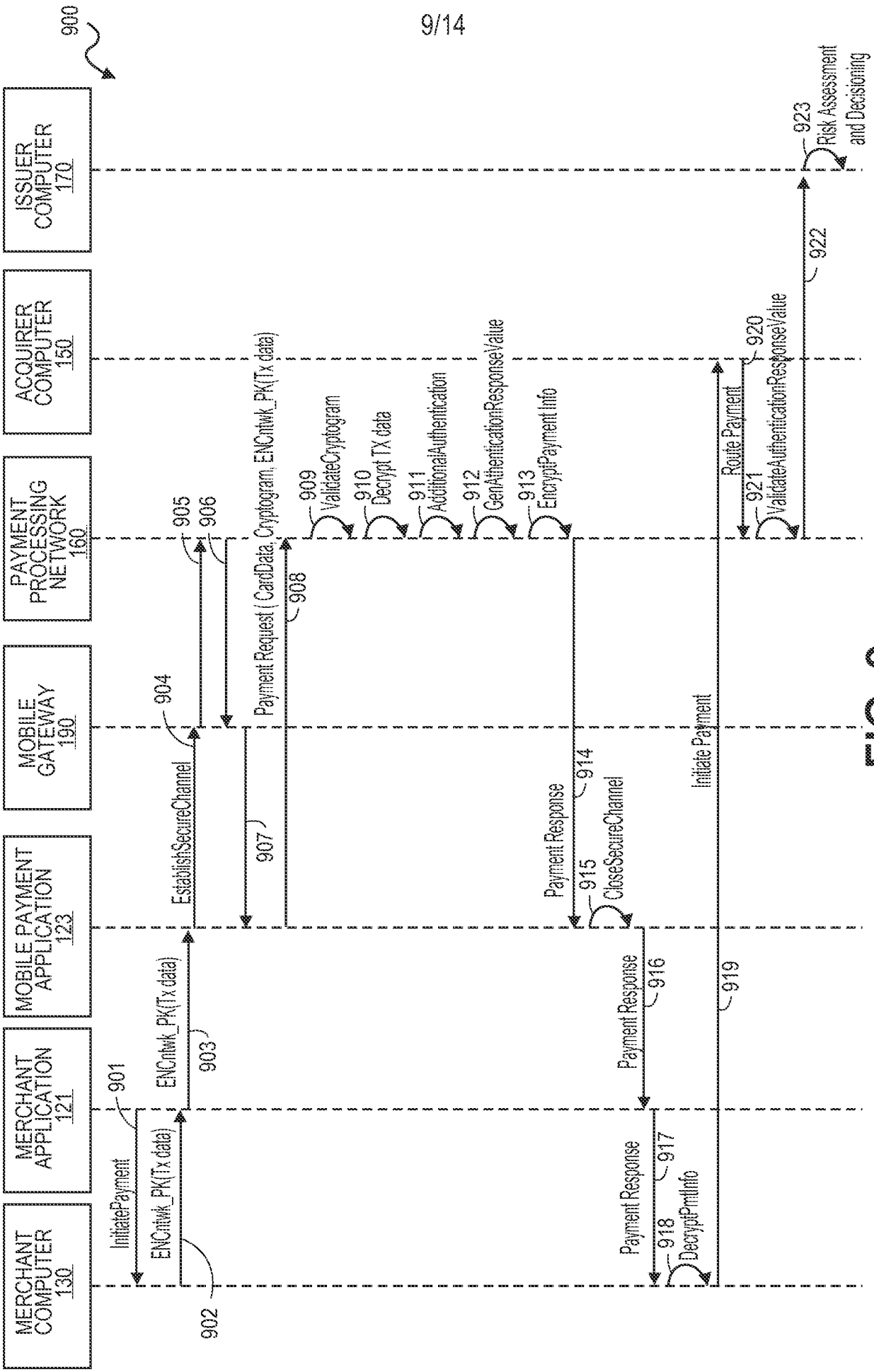

900
MERCHANT COMPUTER 130
MERCHANT APPLICATION 121
MOBILE PAYMENT APPLICATION 123
MOBILE GATEWAY 190
PAYMENT PROCESSING NETWORK 160
ACQUIRER COMPUTER 150
ISSUER COMPUTER 170
InitiatePayment
901
ENCntwk_PK(Tx data)
902
ENCntwk_PK(Tx data)
903
EstablishSecureChannel
904
905
906
Payment Request (CardData, Cryptogram, ENCntwk_PK(Tx data))
907
908
ValidateCryptogram
909
Decrypt TX data
910
AdditionalAuthentication
911
GenAuthenticationResponseValue
912
EncryptPayment Info
913
Payment Response
914
CloseSecureChannel
915
Payment Response
916
Payment Response
917
DecryptPmtInfo
918
Initiate Payment
919
Route Payment
920
ValidateAuthenticationResponseValue
921
922
Risk Assessment and Decisioning
923

FIG. 9

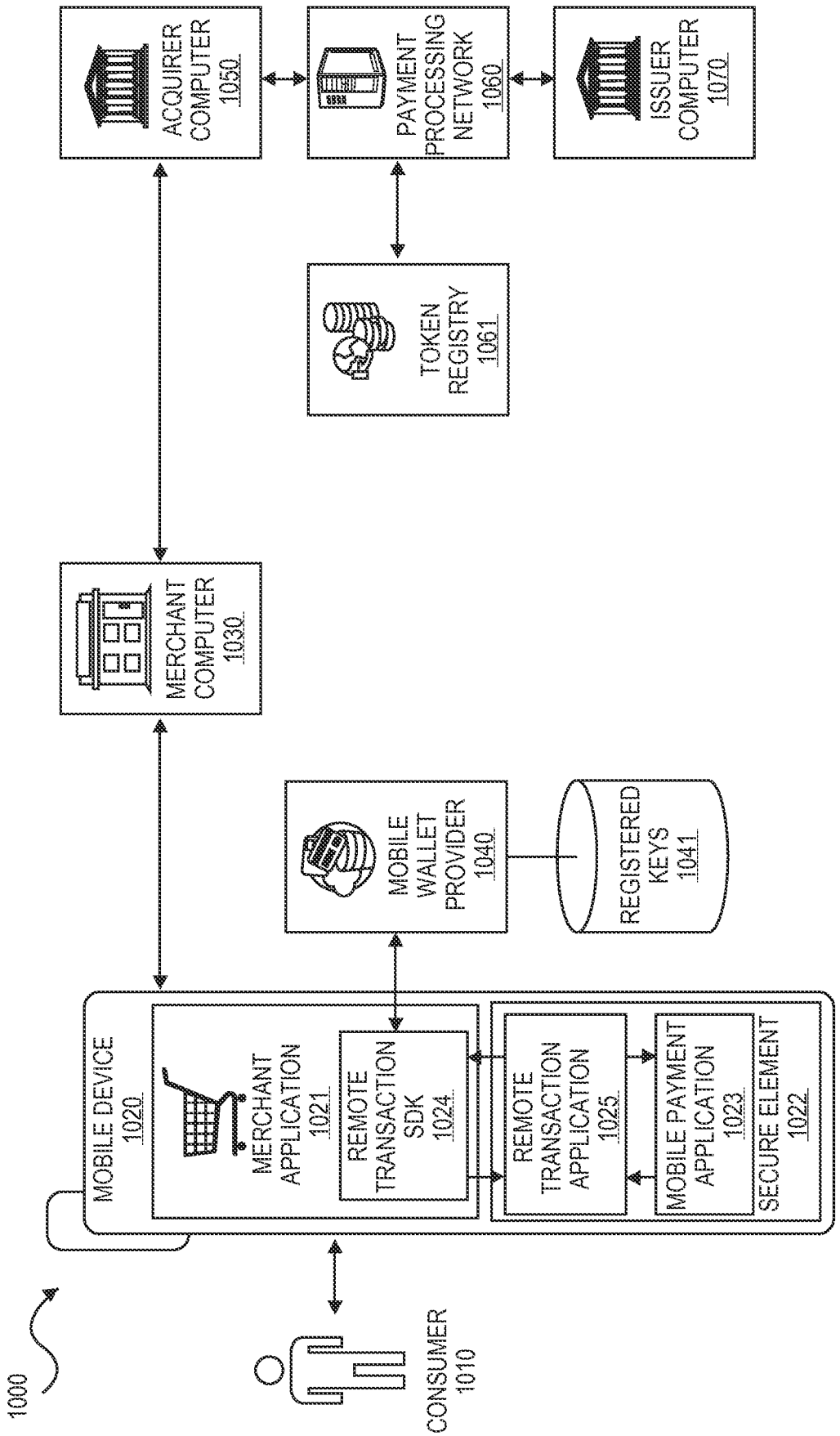

ACQUIRER COMPUTER 1050
PAYMENT PROCESSING NETWORK 1060
ISSUER COMPUTER 1070
TOKEN REGISTRY 1061
MERCHANT COMPUTER 1030
MOBILE WALLET PROVIDER 1040
REGISTERED KEYS 1041
MOBILE DEVICE 1020
MERCHANT APPLICATION 1021
REMOTE TRANSACTION SDK 1024
REMOTE TRANSACTION APPLICATION 1025
MOBILE PAYMENT APPLICATION 1023
SECURE ELEMENT 1022
CONSUMER 1010
1000

FIG. 10

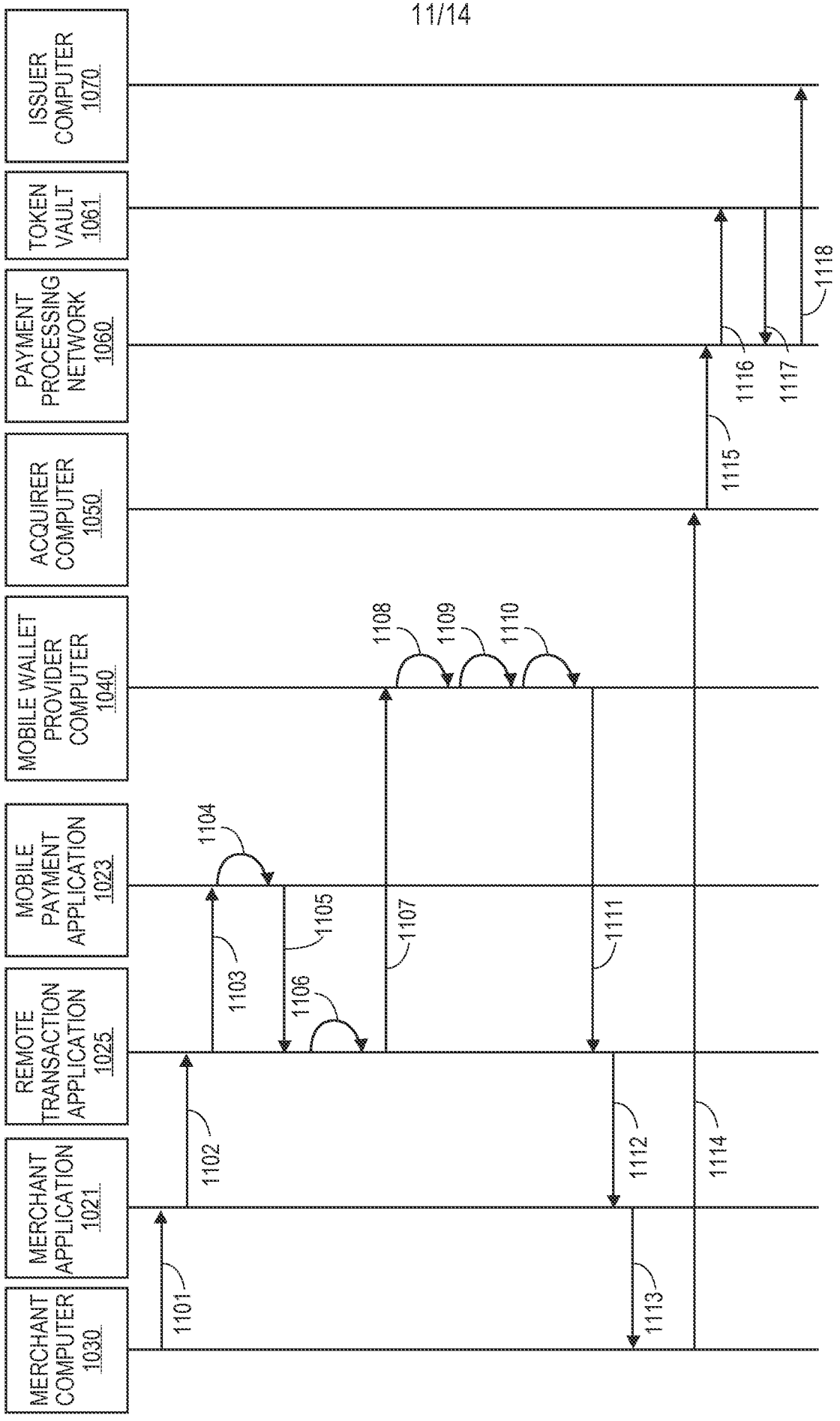

MERCHANT COMPUTER 1030
MERCHANT APPLICATION 1021
REMOTE TRANSACTION APPLICATION 1025
MOBILE PAYMENT APPLICATION 1023
MOBILE WALLET PROVIDER COMPUTER 1040
ACQUIRER COMPUTER 1050
PAYMENT PROCESSING NETWORK 1060
TOKEN VAULT 1061
ISSUER COMPUTER 1070
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118

FIG. 11

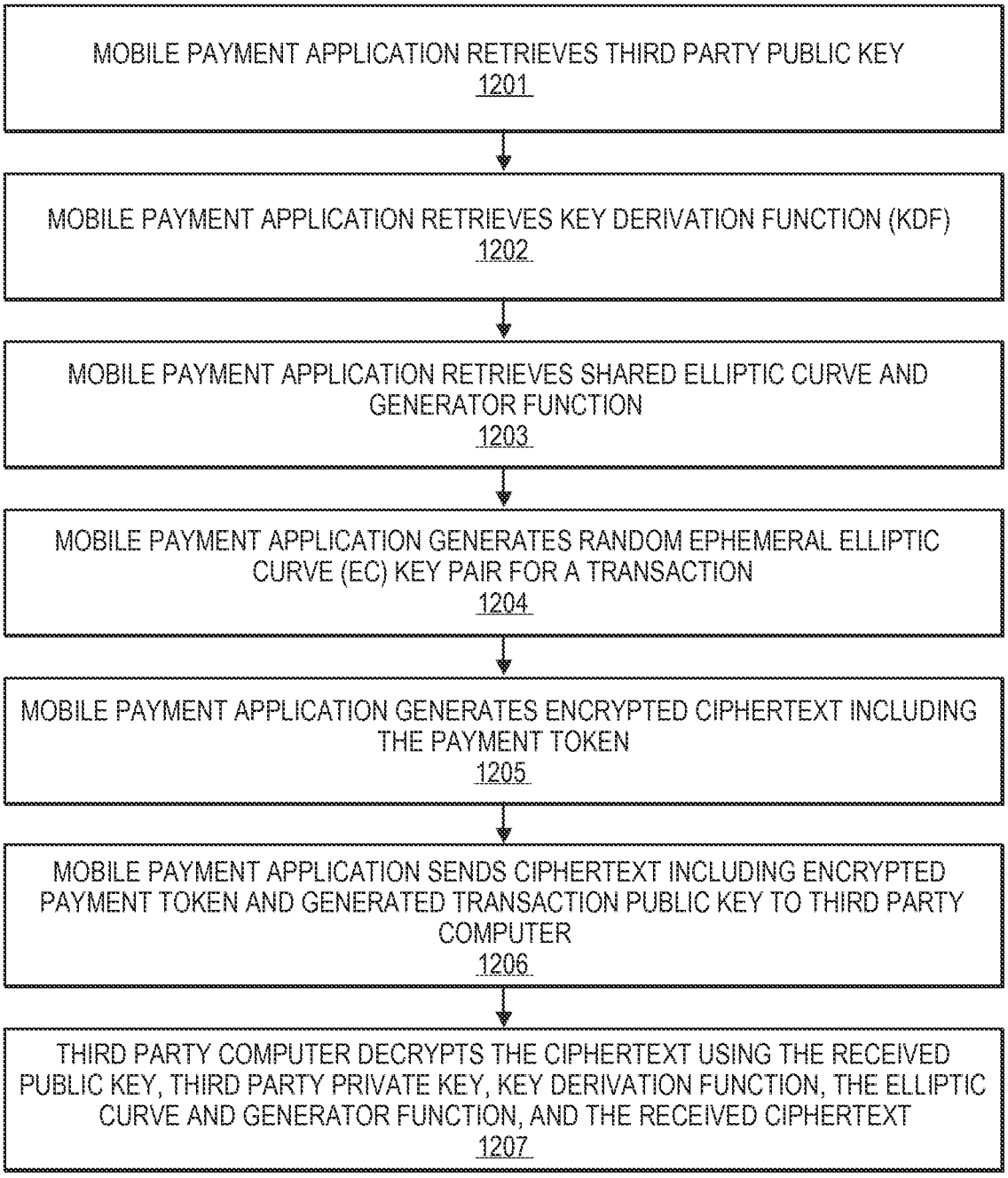

MOBILE PAYMENT APPLICATION RETRIEVES THIRD PARTY PUBLIC KEY
1201
MOBILE PAYMENT APPLICATION RETRIEVES KEY DERIVATION FUNCTION (KDF)
1202
MOBILE PAYMENT APPLICATION RETRIEVES SHARED ELLIPTIC CURVE AND GENERATOR FUNCTION
1203
MOBILE PAYMENT APPLICATION GENERATES RANDOM EPHEMERAL ELLIPTIC CURVE (EC) KEY PAIR FOR A TRANSACTION
1204
MOBILE PAYMENT APPLICATION GENERATES ENCRYPTED CIPHERTEXT INCLUDING THE PAYMENT TOKEN
1205
MOBILE PAYMENT APPLICATION SENDS CIPHERTEXT INCLUDING ENCRYPTED PAYMENT TOKEN AND GENERATED TRANSACTION PUBLIC KEY TO THIRD PARTY COMPUTER
1206
THIRD PARTY COMPUTER DECRYPTS THE CIPHERTEXT USING THE RECEIVED PUBLIC KEY, THIRD PARTY PRIVATE KEY, KEY DERIVATION FUNCTION, THE ELLIPTIC CURVE AND GENERATOR FUNCTION, AND THE RECEIVED CIPHERTEXT
1207

FIG. 12

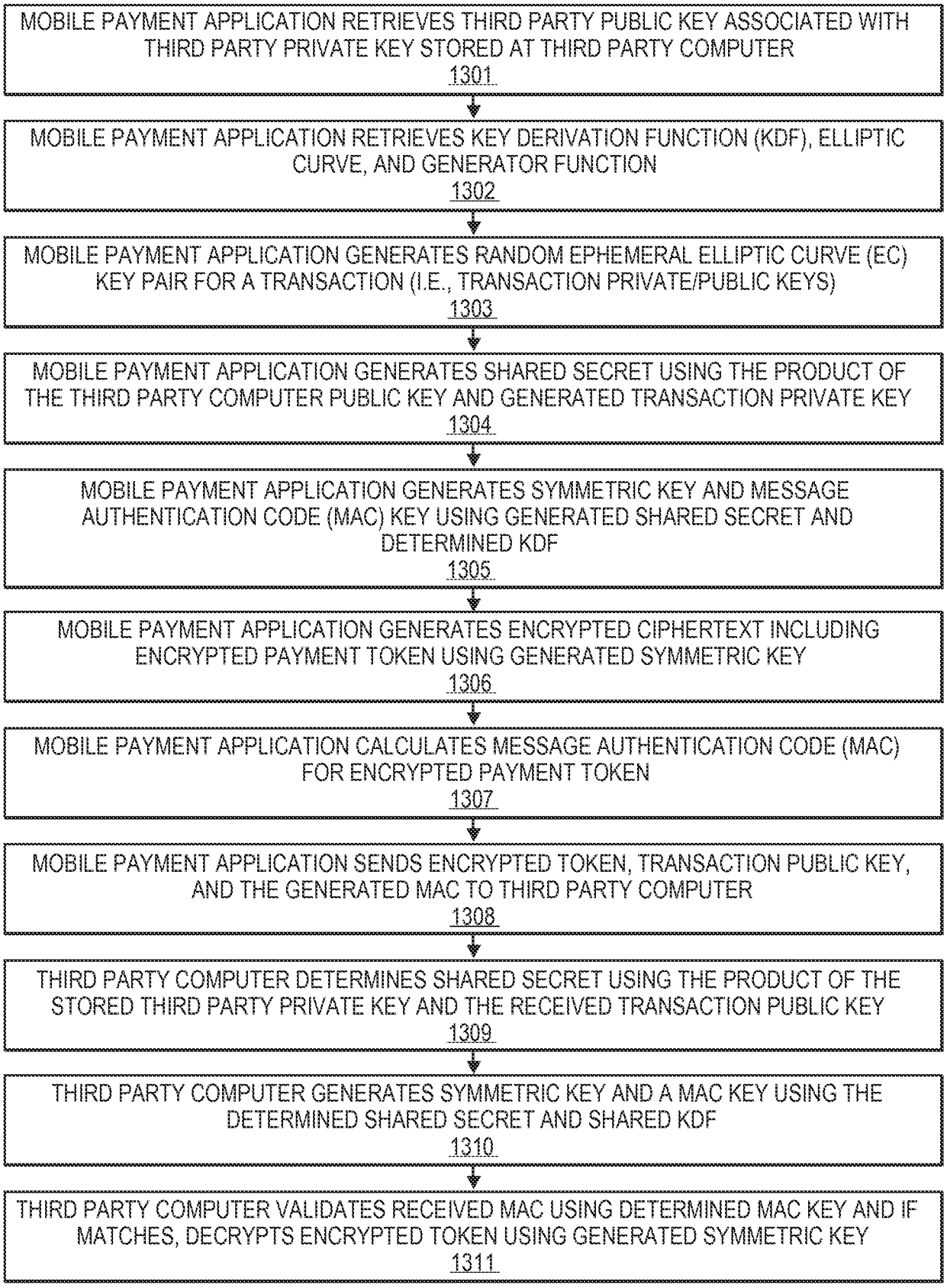

MOBILE PAYMENT APPLICATION RETRIEVES THIRD PARTY PUBLIC KEY ASSOCIATED WITH THIRD PARTY PRIVATE KEY STORED AT THIRD PARTY COMPUTER
1301
MOBILE PAYMENT APPLICATION RETRIEVES KEY DERIVATION FUNCTION (KDF), ELLIPTIC CURVE, AND GENERATOR FUNCTION
1302
MOBILE PAYMENT APPLICATION GENERATES RANDOM EPHEMERAL ELLIPTIC CURVE (EC) KEY PAIR FOR A TRANSACTION (I.E., TRANSACTION PRIVATE/PUBLIC KEYS)
1303
MOBILE PAYMENT APPLICATION GENERATES SHARED SECRET USING THE PRODUCT OF THE THIRD PARTY COMPUTER PUBLIC KEY AND GENERATED TRANSACTION PRIVATE KEY
1304
MOBILE PAYMENT APPLICATION GENERATES SYMMETRIC KEY AND MESSAGE AUTHENTICATION CODE (MAC) KEY USING GENERATED SHARED SECRET AND DETERMINED KDF
1305
MOBILE PAYMENT APPLICATION GENERATES ENCRYPTED CIPHERTEXT INCLUDING ENCRYPTED PAYMENT TOKEN USING GENERATED SYMMETRIC KEY
1306
MOBILE PAYMENT APPLICATION CALCULATES MESSAGE AUTHENTICATION CODE (MAC) FOR ENCRYPTED PAYMENT TOKEN
1307
MOBILE PAYMENT APPLICATION SENDS ENCRYPTED TOKEN, TRANSACTION PUBLIC KEY, AND THE GENERATED MAC TO THIRD PARTY COMPUTER
1308
THIRD PARTY COMPUTER DETERMINES SHARED SECRET USING THE PRODUCT OF THE STORED THIRD PARTY PRIVATE KEY AND THE RECEIVED TRANSACTION PUBLIC KEY
1309
THIRD PARTY COMPUTER GENERATES SYMMETRIC KEY AND A MAC KEY USING THE DETERMINED SHARED SECRET AND SHARED KDF
1310
THIRD PARTY COMPUTER VALIDATES RECEIVED MAC USING DETERMINED MAC KEY AND IF MATCHES, DECRYPTS ENCRYPTED TOKEN USING GENERATED SYMMETRIC KEY
1311

FIG. 13

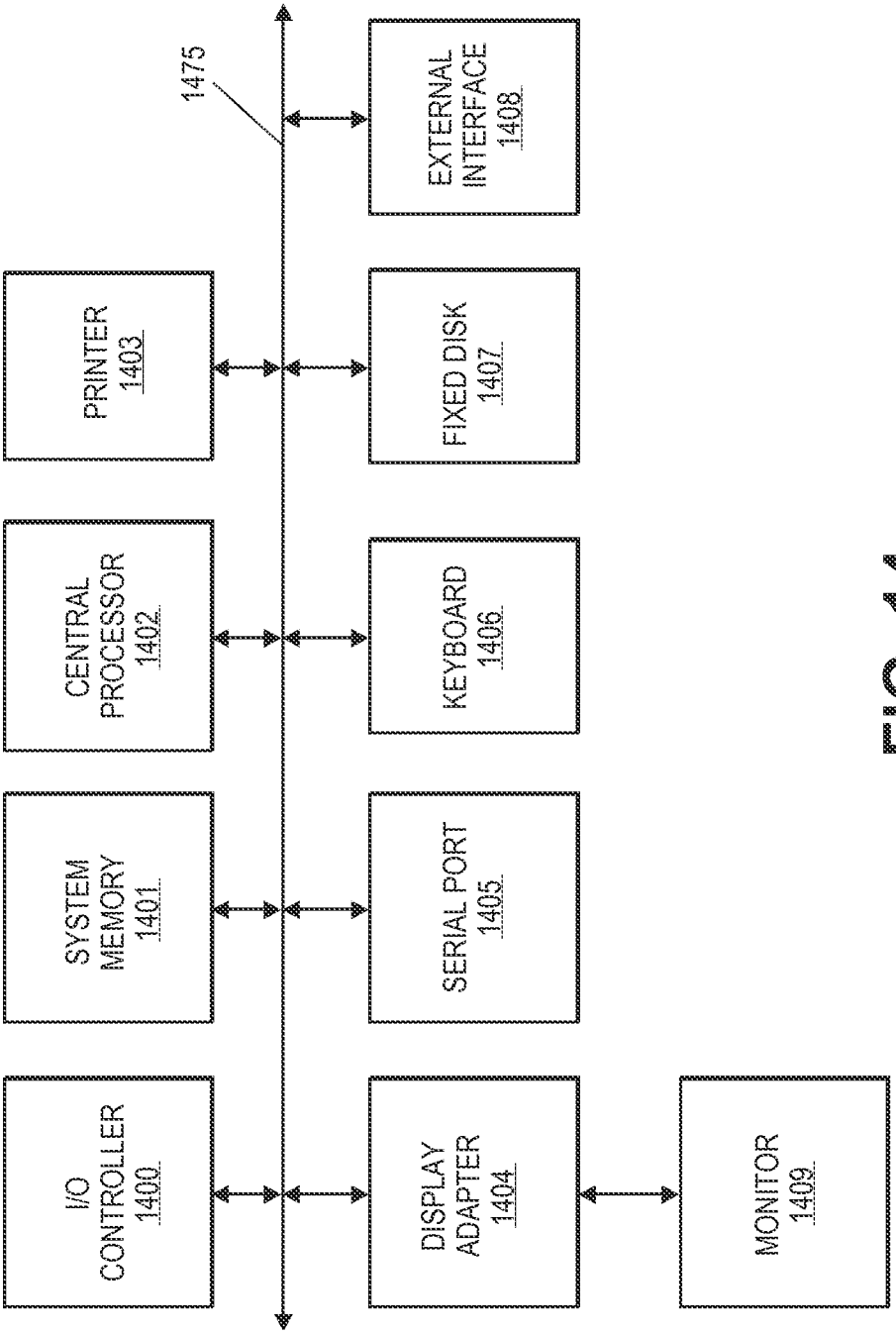

1475
EXTERNAL INTERFACE 1408
PRINTER 1403
FIXED DISK 1407
CENTRAL PROCESSOR 1402
KEYBOARD 1406
SYSTEM MEMORY 1401
SERIAL PORT 1405
I/O CONTROLLER 1400
DISPLAY ADAPTER 1404
MONITOR 1409

FIG. 14