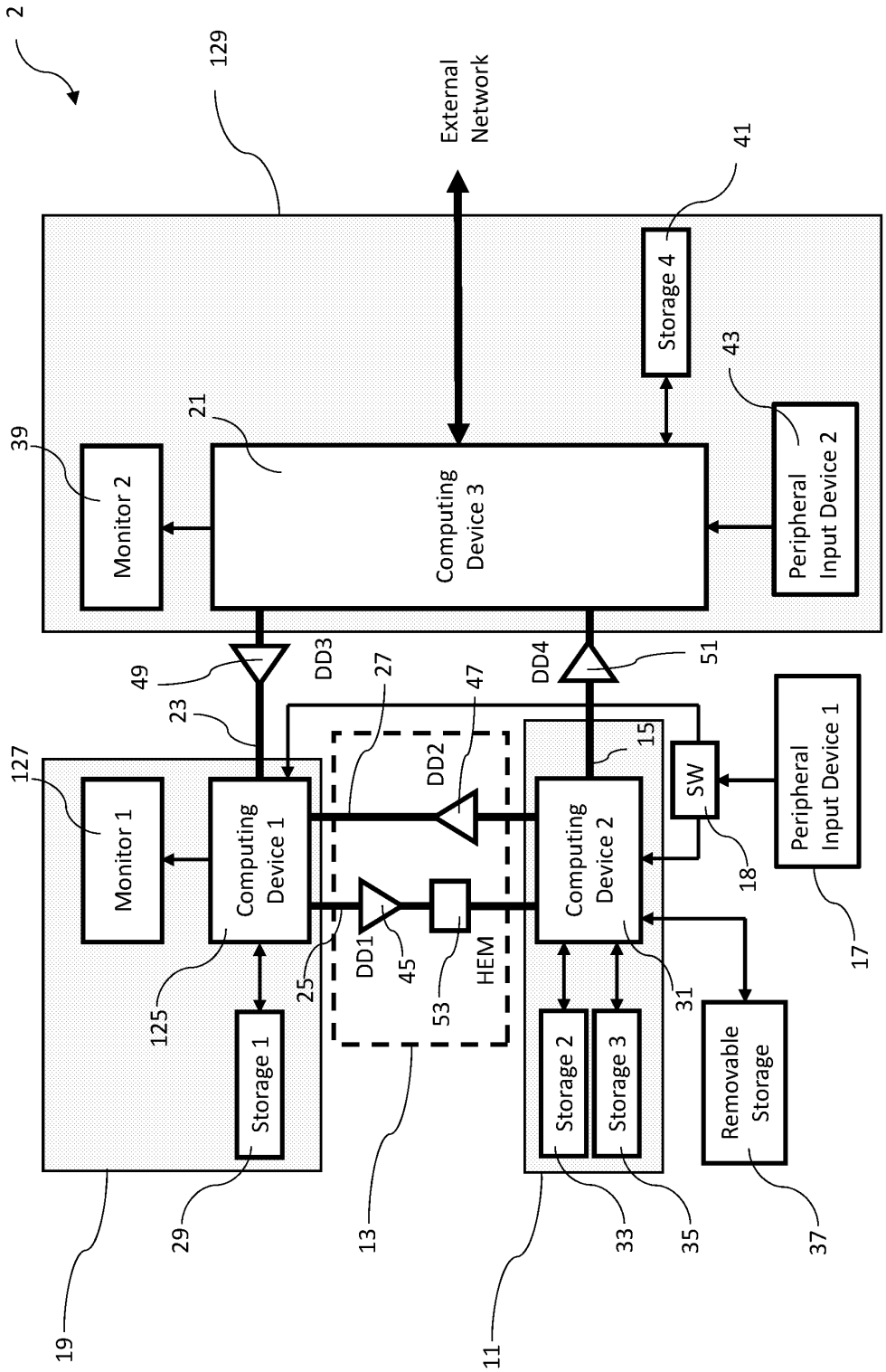

2
129
External Network
41
Storage 4
43
Peripheral Input Device 2
39
Monitor 2
21
Computing Device 3
49
DD3
27
47
DD4
51
23
15
127
Monitor 1
Computing Device 1
DD2
SW
Peripheral Input Device 1
Computing Device 2
18
DD1
45
HEM
53
25
125
31
17
Storage 1
Storage 2
Storage 3
Removable Storage
29
13
33
35
37
19
11

Fig. 1a

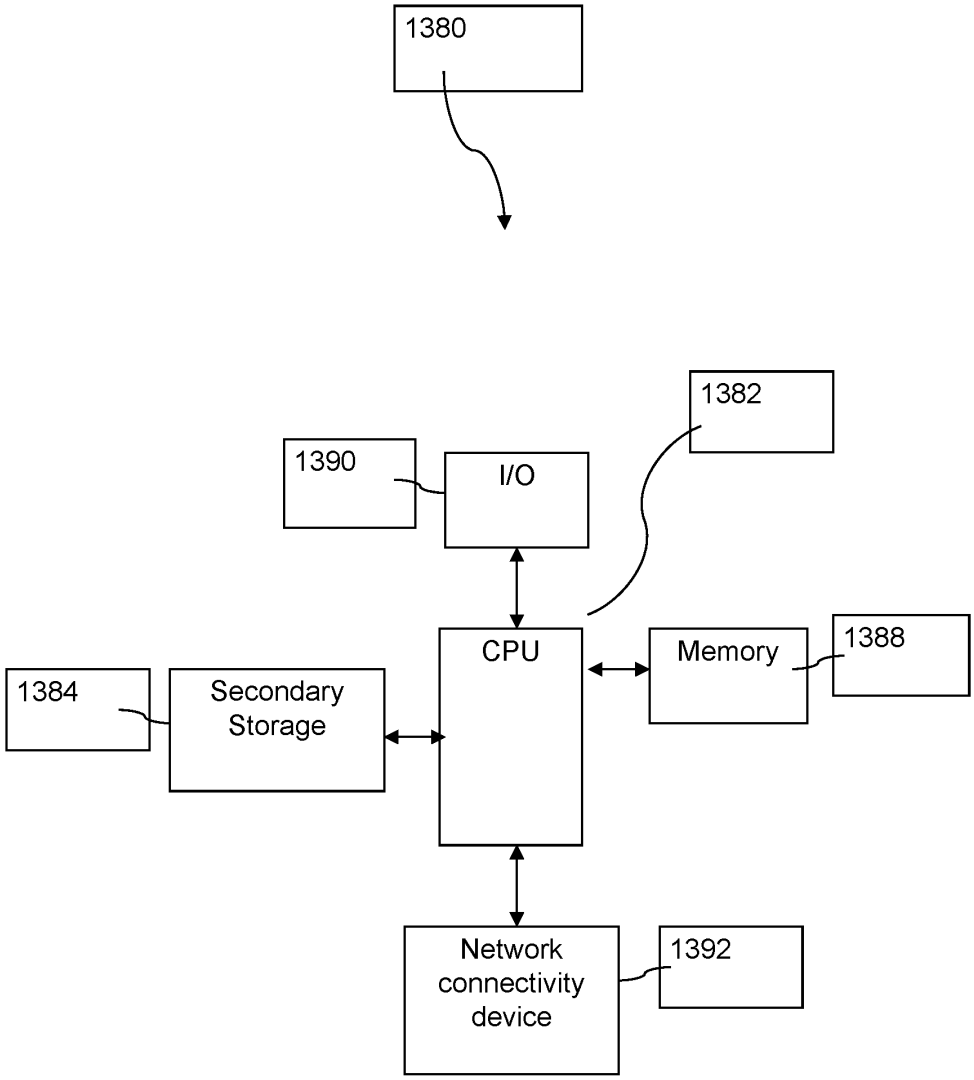

1380
1382
1390
I/O
CPU
Memory
1388
1384
Secondary Storage
Network connectivity device
1392

Fig. 1b

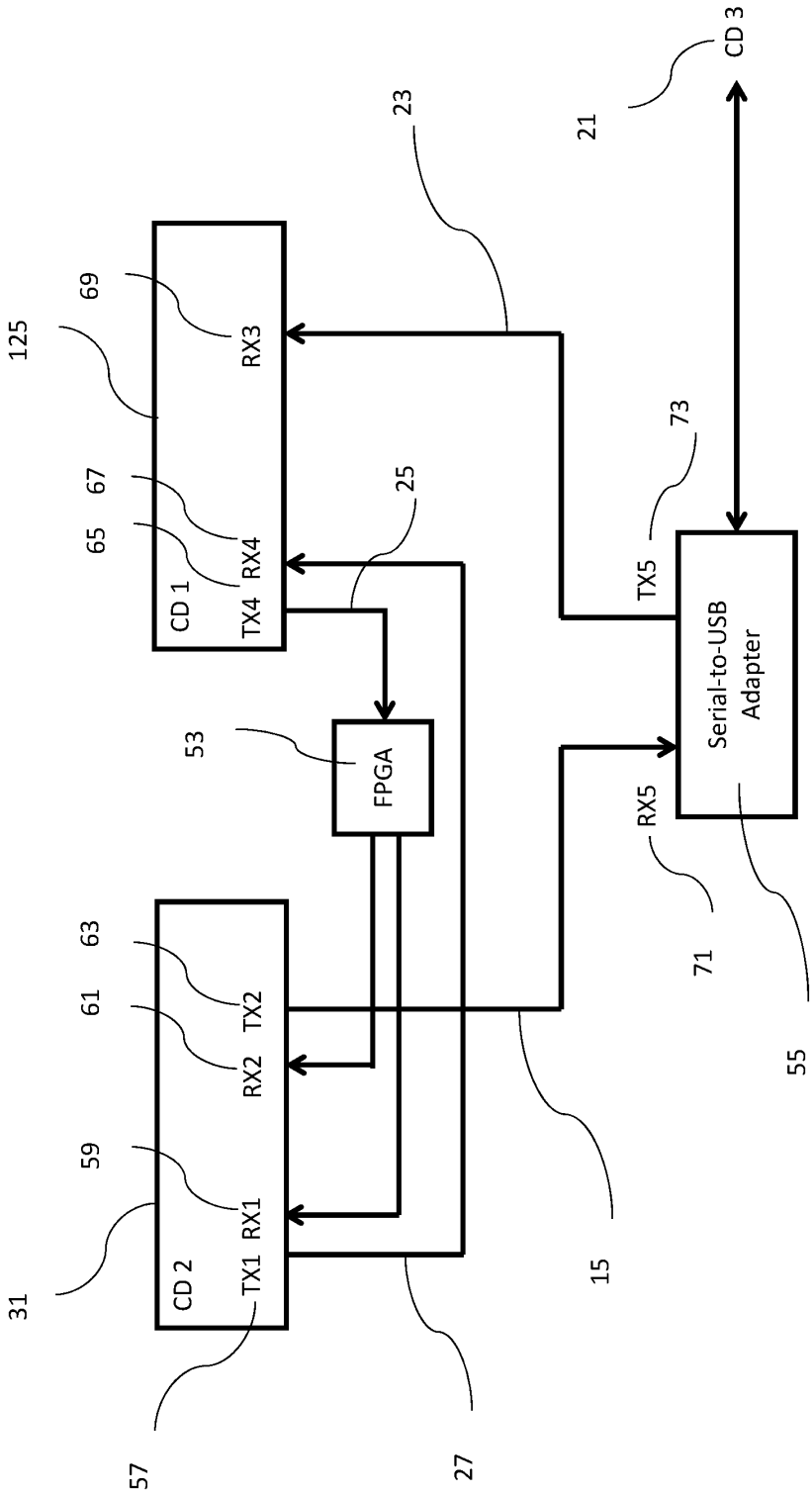
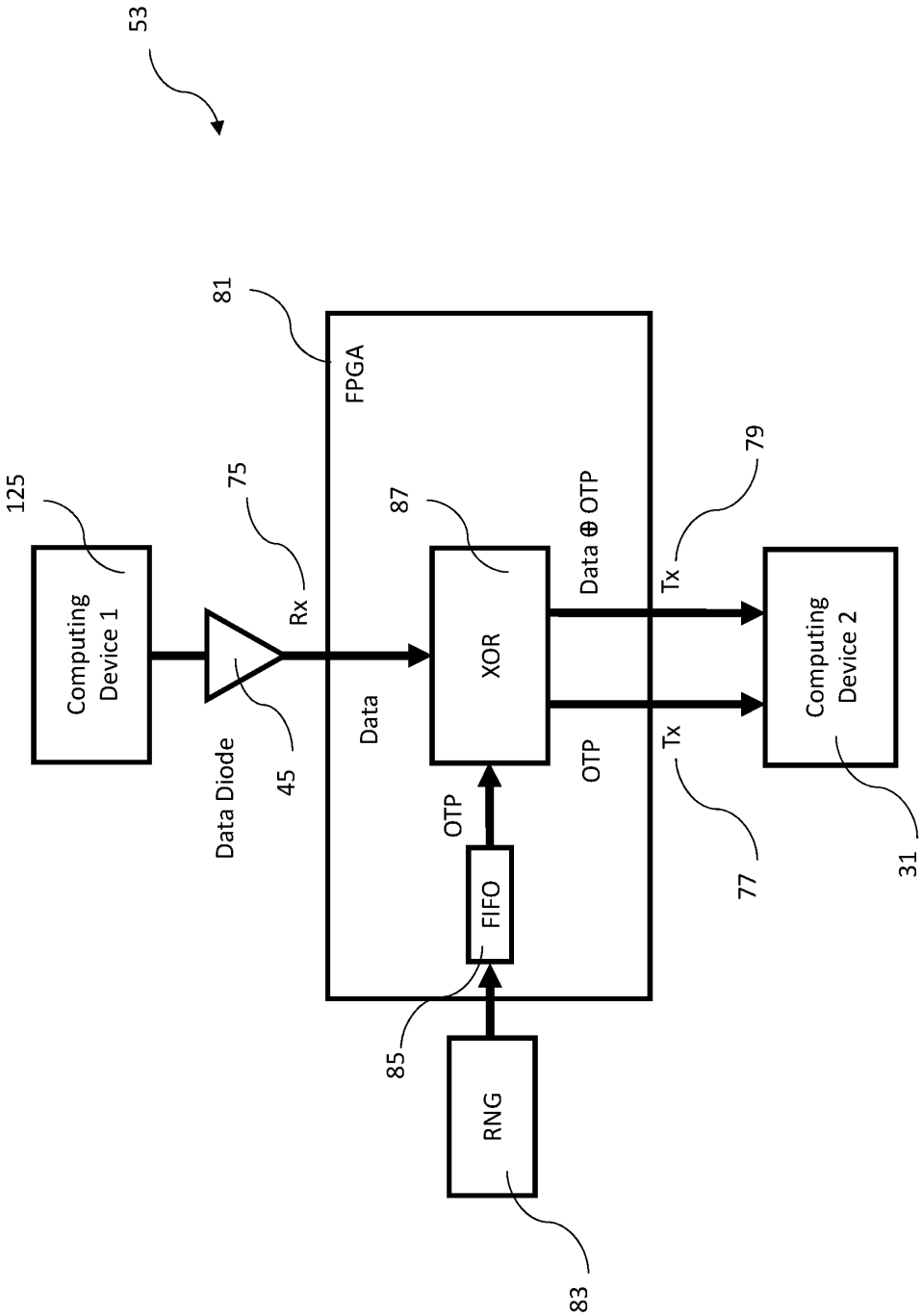

CD 3
21
23
69
RX3
125
67
65
RX4
CD 1
TX4
25
73
TX5
Serial-to-USB Adapter
53
FPGA
RX5
71
55
63
61
TX2
RX2
59
RX1
CD 2
TX1
31
15
57
27

Fig. 2

Fig. 3


53
81
FPGA
125
Computing Device 1
75
Rx
87
XOR
Data ⊕ OTP
79
Tx
Computing Device 2
Data Diode
45
Data
OTP
Tx
77
31
OTP
FIFO
85
RNG
83

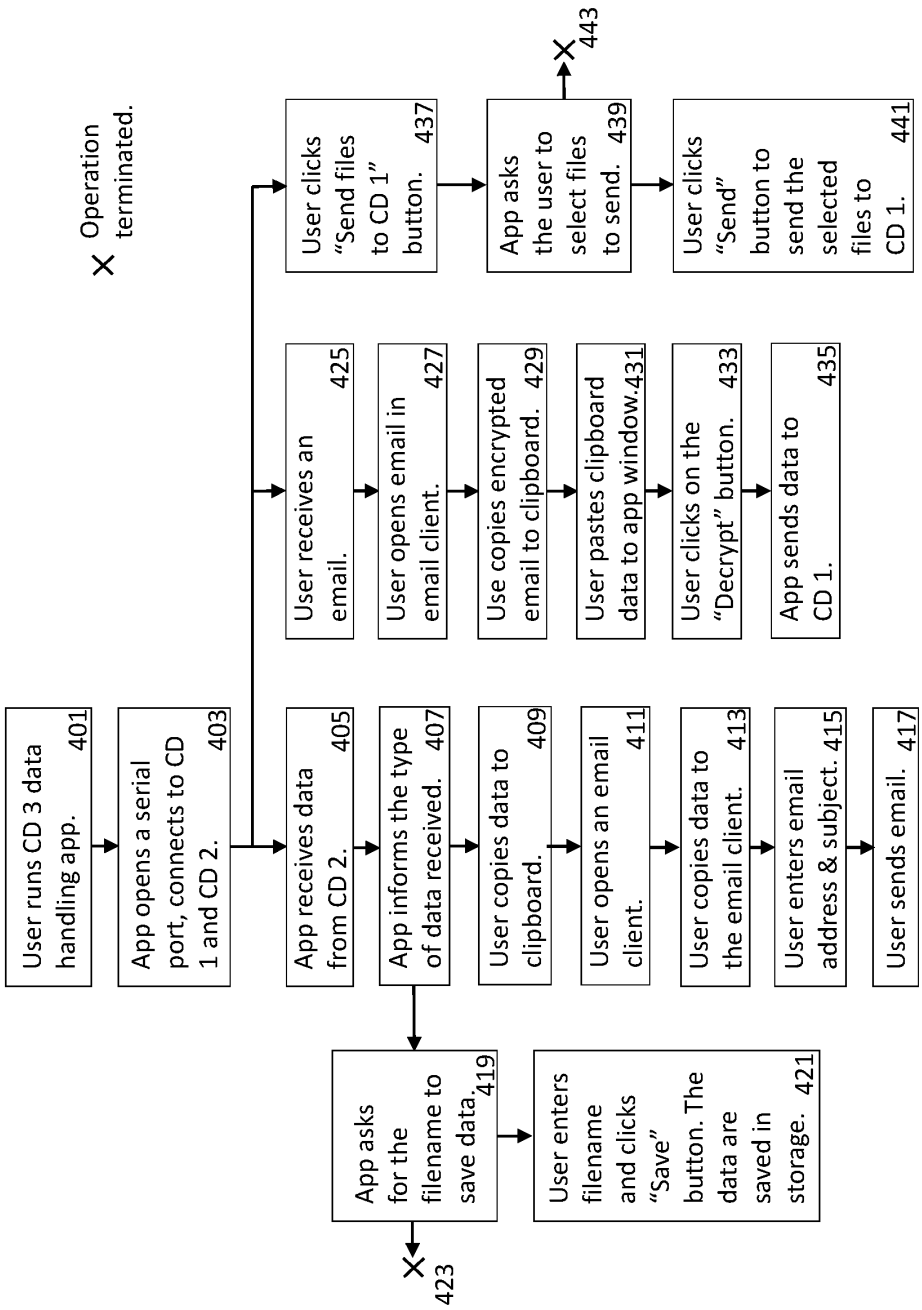

User runs CD 3 data handling app. 401
App opens a serial port, connects to CD 1 and CD 2. 403
App receives data from CD 2. 405
App informs the type of data received. 407
User copies data to clipboard. 409
User opens an email client. 411
User copies data to the email client. 413
User enters email address & subject. 415
User sends email. 417
App asks for the filename to save data. 419
User enters filename and clicks "Save" button. The data are saved in storage. 421
423
Operation terminated.
User receives an email. 425
User opens email in email client. 427
Use copies encrypted email to clipboard. 429
User pastes clipboard data to app window.431
User clicks on the "Decrypt" button. 433
App sends data to CD 1. 435
User clicks "Send files to CD 1" button. 437
App asks the user to select files to send. 439
443
User clicks "Send" button to send the selected files to CD 1. 441

Fig. 4

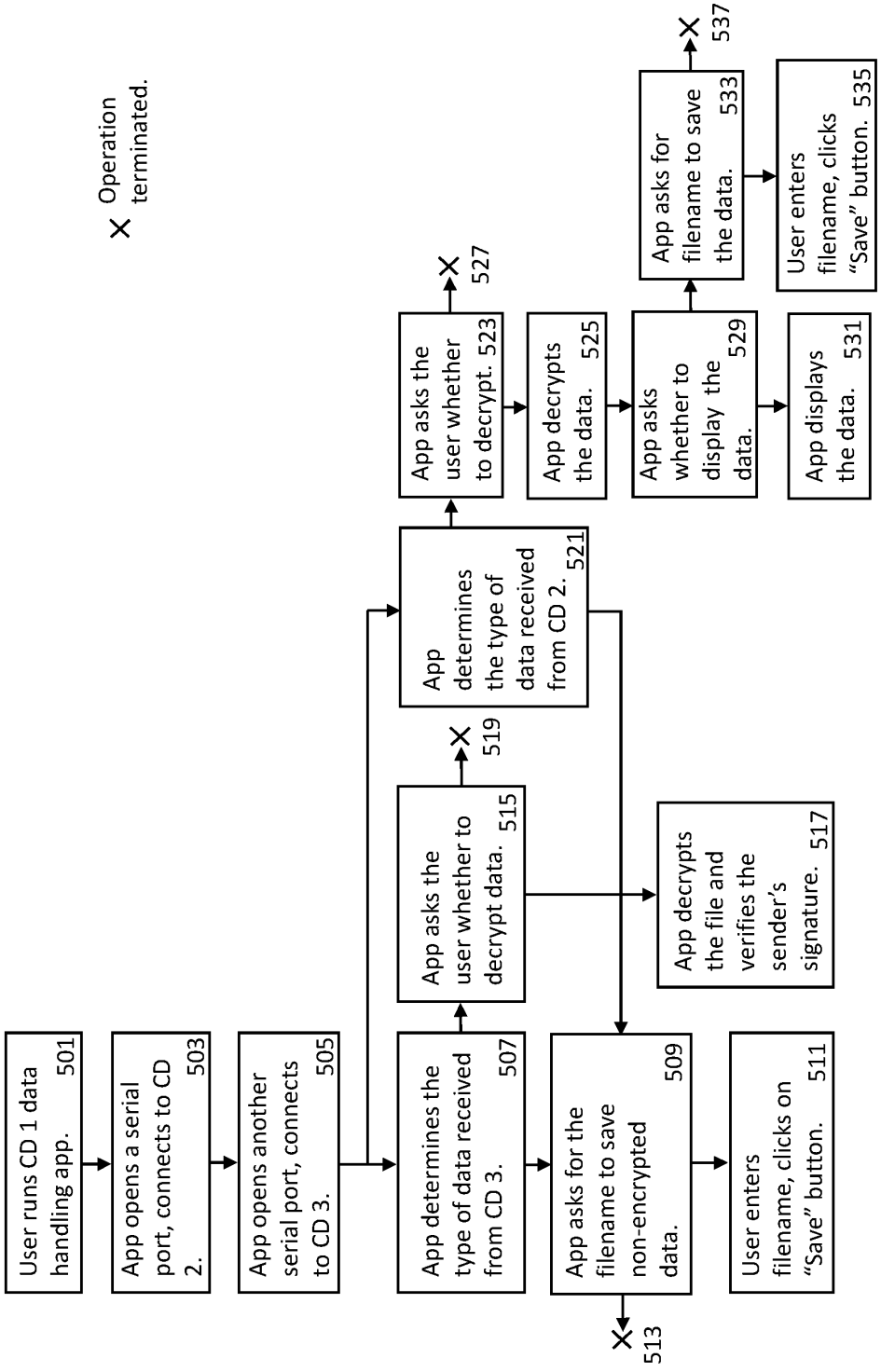

User runs CD 1 data handling app. 501
App opens a serial port, connects to CD 2. 503
App opens another serial port, connects to CD 3. 505
App determines the type of data received from CD 3. 507
App asks for the filename to save non-encrypted data. 509
User enters filename, clicks on "Save" button. 511
513
App asks the user whether to decrypt data. 515
519
App decrypts the file and verifies the sender's signature. 517
App determines the type of data received from CD 2. 521
App asks the user whether to decrypt. 523
527
App decrypts the data. 525
App asks whether to display the data. 529
App displays the data. 531
App asks for filename to save the data. 533
537
User enters filename, clicks "Save" button. 535
Operation terminated.

Fig. 5

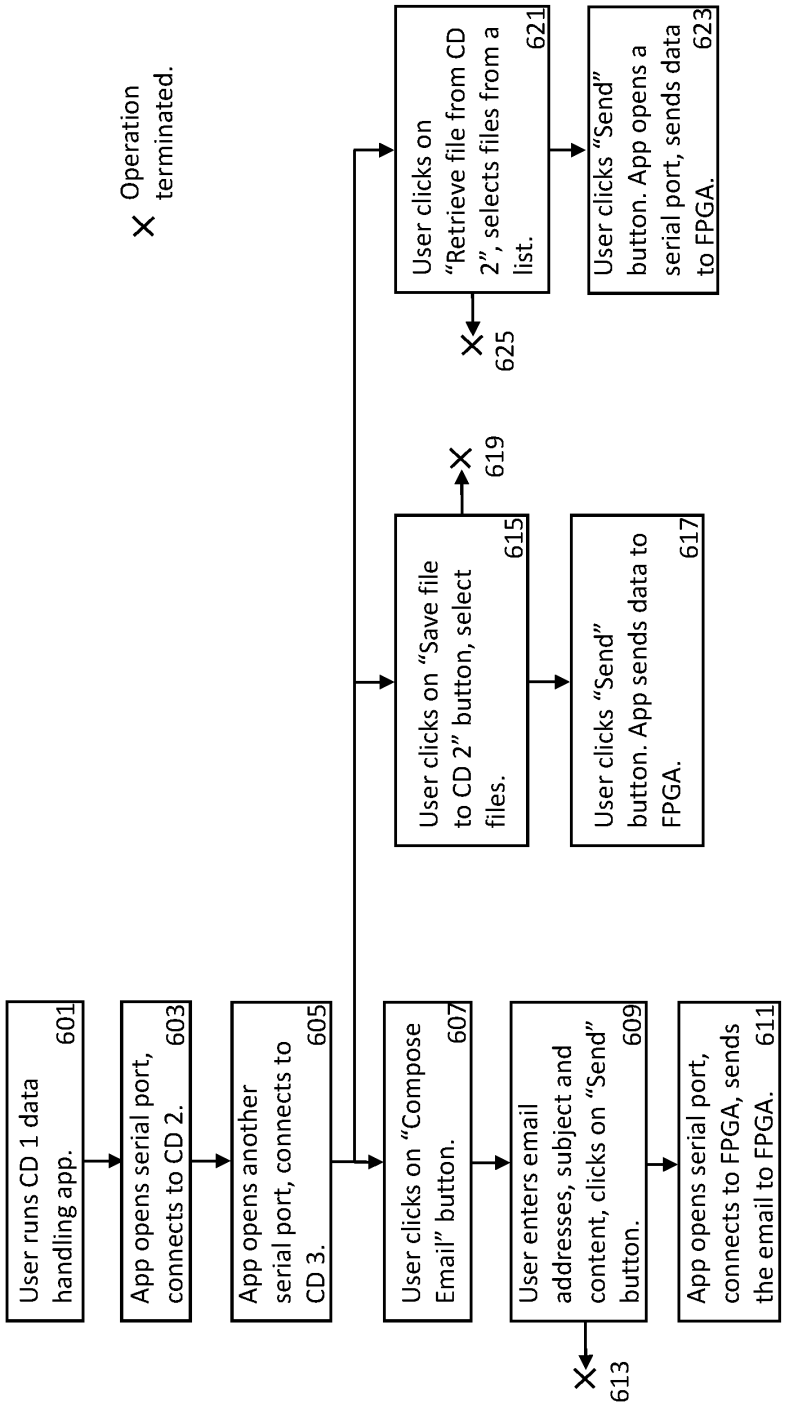

User runs CD 1 data handling app. 601
App opens serial port, connects to CD 2. 603
App opens another serial port, connects to CD 3. 605
User clicks on "Compose Email" button. 607
User enters email addresses, subject and content, clicks on "Send" button. 609
App opens serial port, connects to FPGA, sends the email to FPGA. 611
613
User clicks on "Save file to CD 2" button, select files. 615
619
User clicks "Send" button. App sends data to FPGA. 617
User clicks on "Retrieve file from CD 2", selects files from a list. 621
625
User clicks "Send" button. App opens a serial port, sends data to FPGA. 623
Operation terminated.

Fig. 6

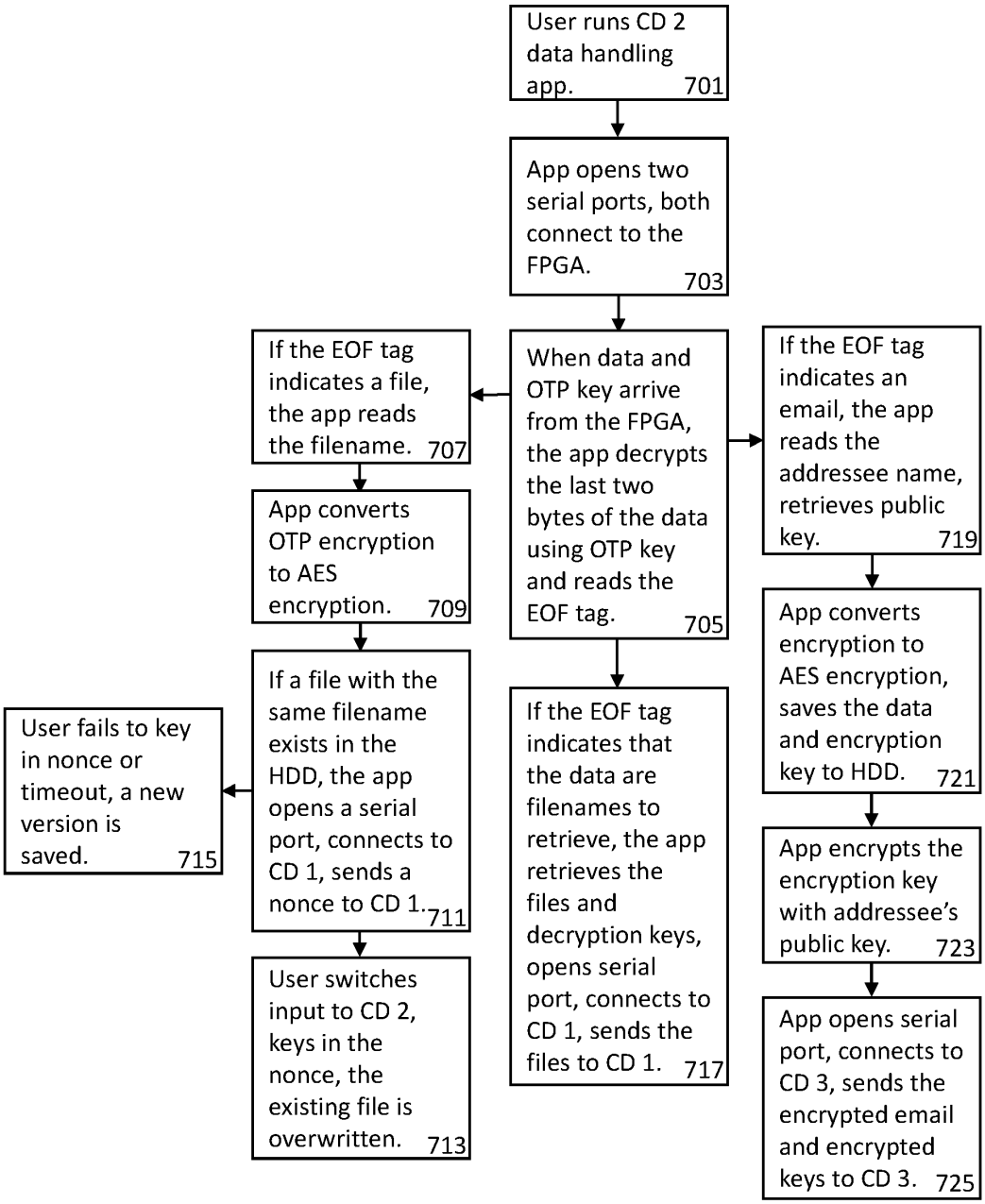
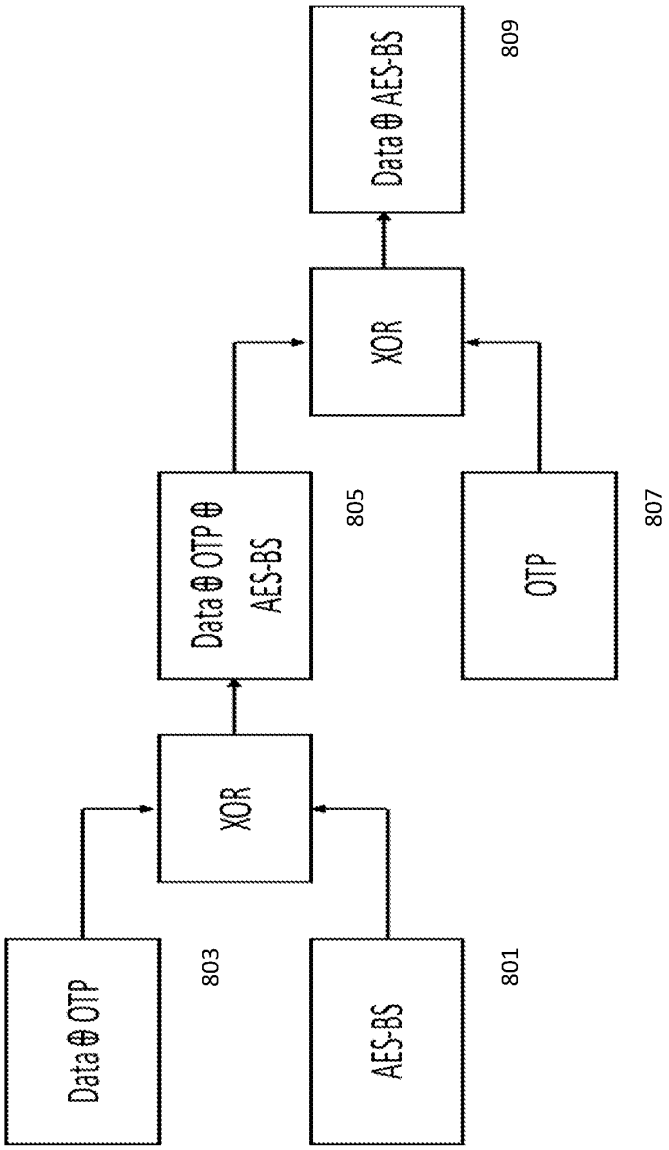

User runs CD 2 data handling app. 701
App opens two serial ports, both connect to the FPGA. 703
When data and OTP key arrive from the FPGA, the app decrypts the last two bytes of the data using OTP key and reads the EOF tag. 705
If the EOF tag indicates a file, the app reads the filename. 707
App converts OTP encryption to AES encryption. 709
If a file with the same filename exists in the HDD, the app opens a serial port, connects to CD 1, sends a nonce to CD 1. 711
User switches input to CD 2, keys in the nonce, the existing file is overwritten. 713
User fails to key in nonce or timeout, a new version is saved. 715
If the EOF tag indicates that the data are filenames to retrieve, the app retrieves the files and decryption keys, opens serial port, connects to CD 1, sends the files to CD 1. 717
If the EOF tag indicates an email, the app reads the addressee name, retrieves public key. 719
App converts encryption to AES encryption, saves the data and encryption key to HDD. 721
App encrypts the encryption key with addressee's public key. 723
App opens serial port, connects to CD 3, sends the encrypted email and encrypted keys to CD 3. 725

Fig. 7

Fig. 8


Data ⊕ OTP
803
AES-BS
801
XOR
Data ⊕ OTP ⊕ AES-BS
805
OTP
807
XOR
Data ⊕ AES-BS
809

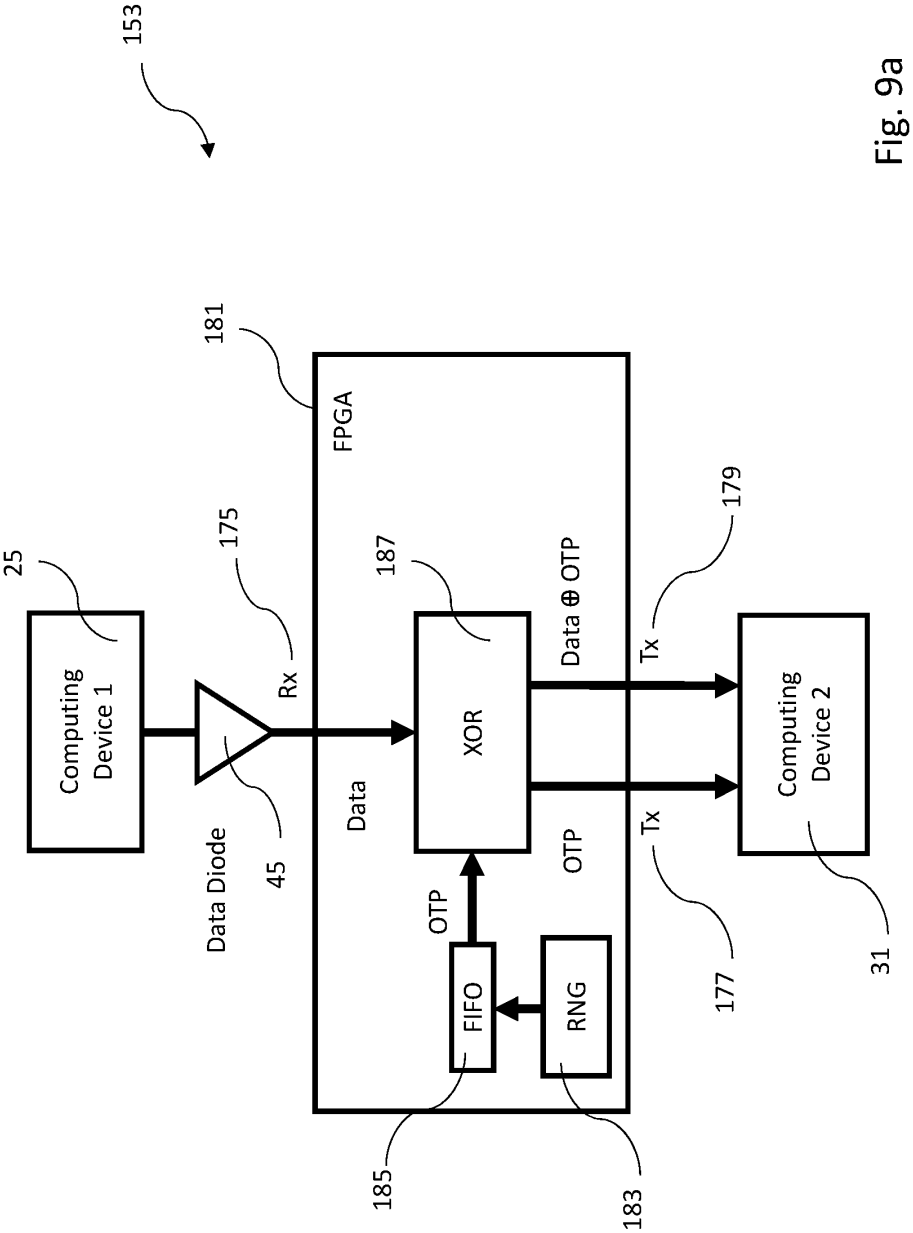

153
181
FPGA
25
Computing Device 1
175
Rx
Data Diode
45
187
XOR
Data ⊕ OTP
179
Tx
Computing Device 2
31
Data
OTP
OTP
FIFO
RNG
185
183
Tx
177

Fig. 9a

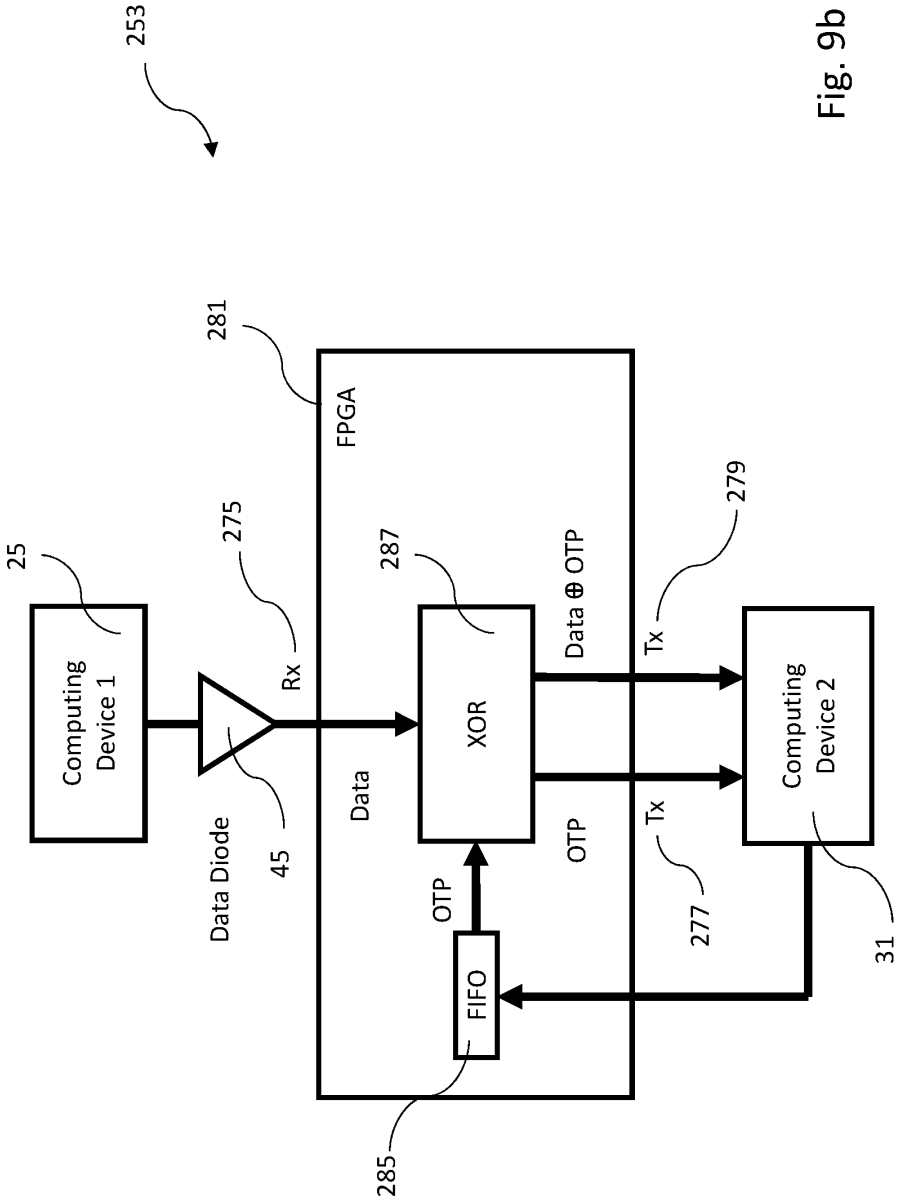

253
281
FPGA
25
Computing Device 1
275
Rx
287
XOR
Data ⊕ OTP
279
Tx
Computing Device 2
Data Diode
45
Data
OTP
Tx
277
31
OTP
FIFO
285

Fig. 9b

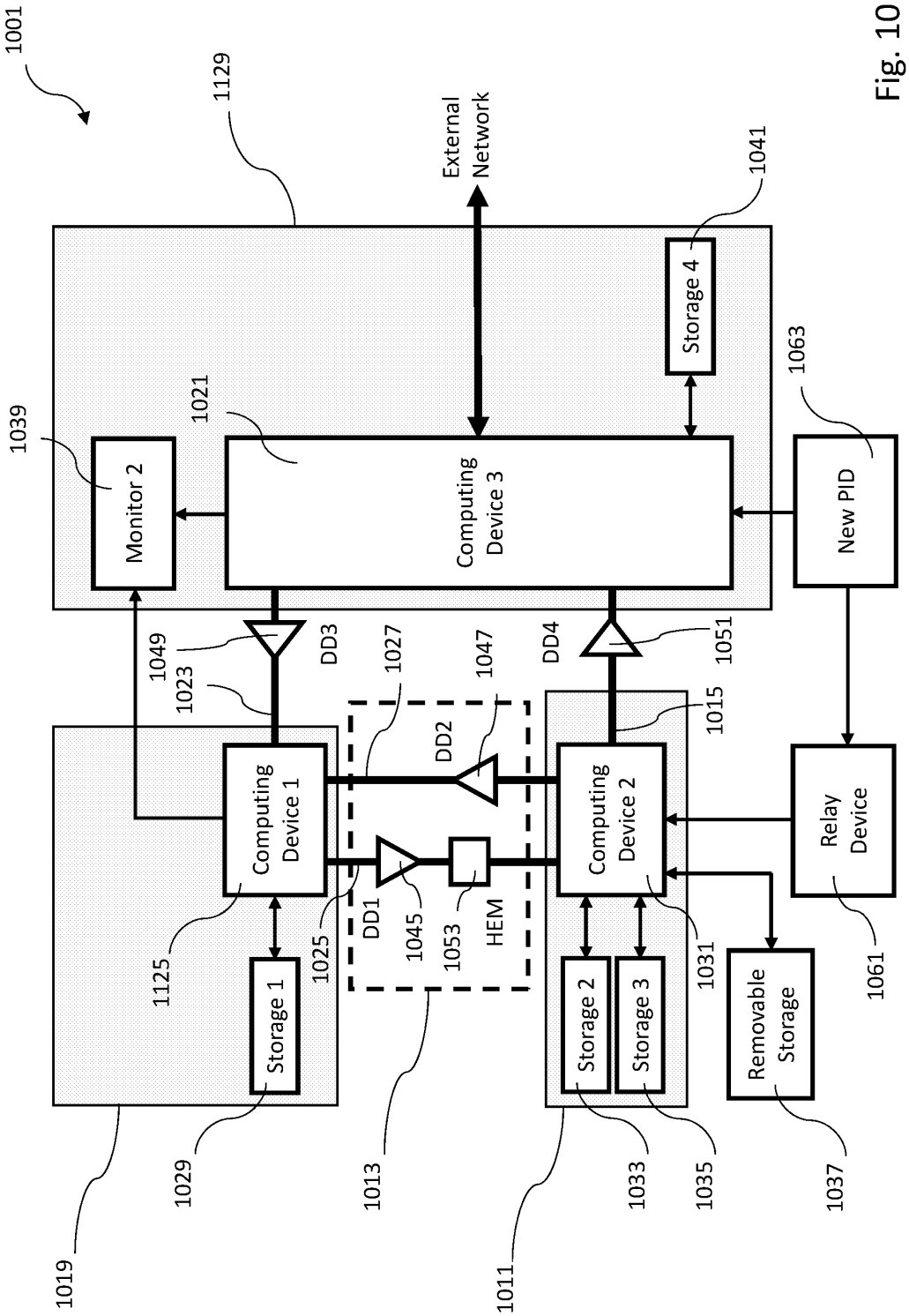

1001
1129
External Network
1041
Storage 4
1063
1039
1021
Monitor 2
Computing Device 3
New PID
1049
DD3
1027
1047
DD4
1051
1023
1015
DD2
Computing Device 1
Computing Device 2
Relay Device
DD1
1045
1053
HEM
1125
1025
1031
1061
Storage 1
Storage 2
Storage 3
Removable Storage
1029
1013
1033
1035
1037
1019
1011

Fig. 10

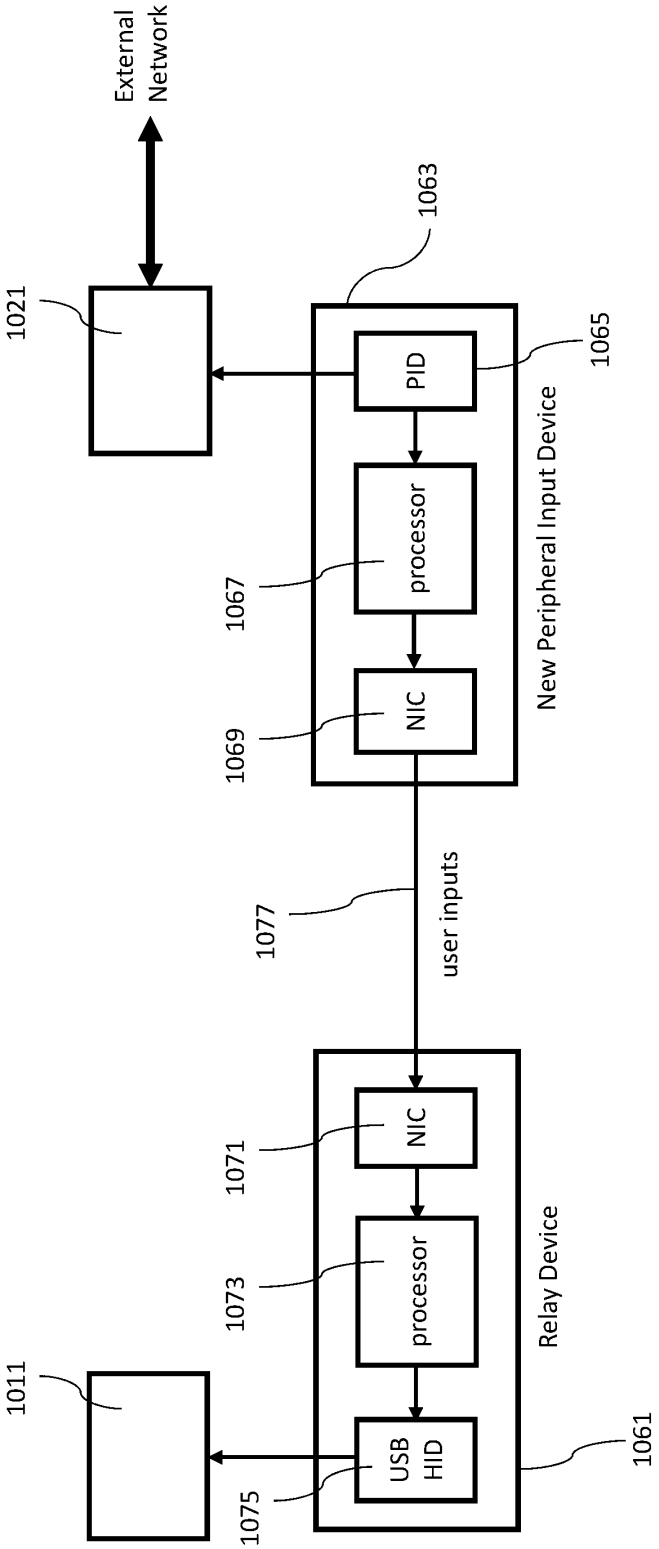

External Network
1021
1063
PID
1065
processor
1067
NIC
1069
New Peripheral Input Device
1077
user inputs
NIC
1071
processor
1073
USB HID
1075
Relay Device
1061
1011

Fig. 11

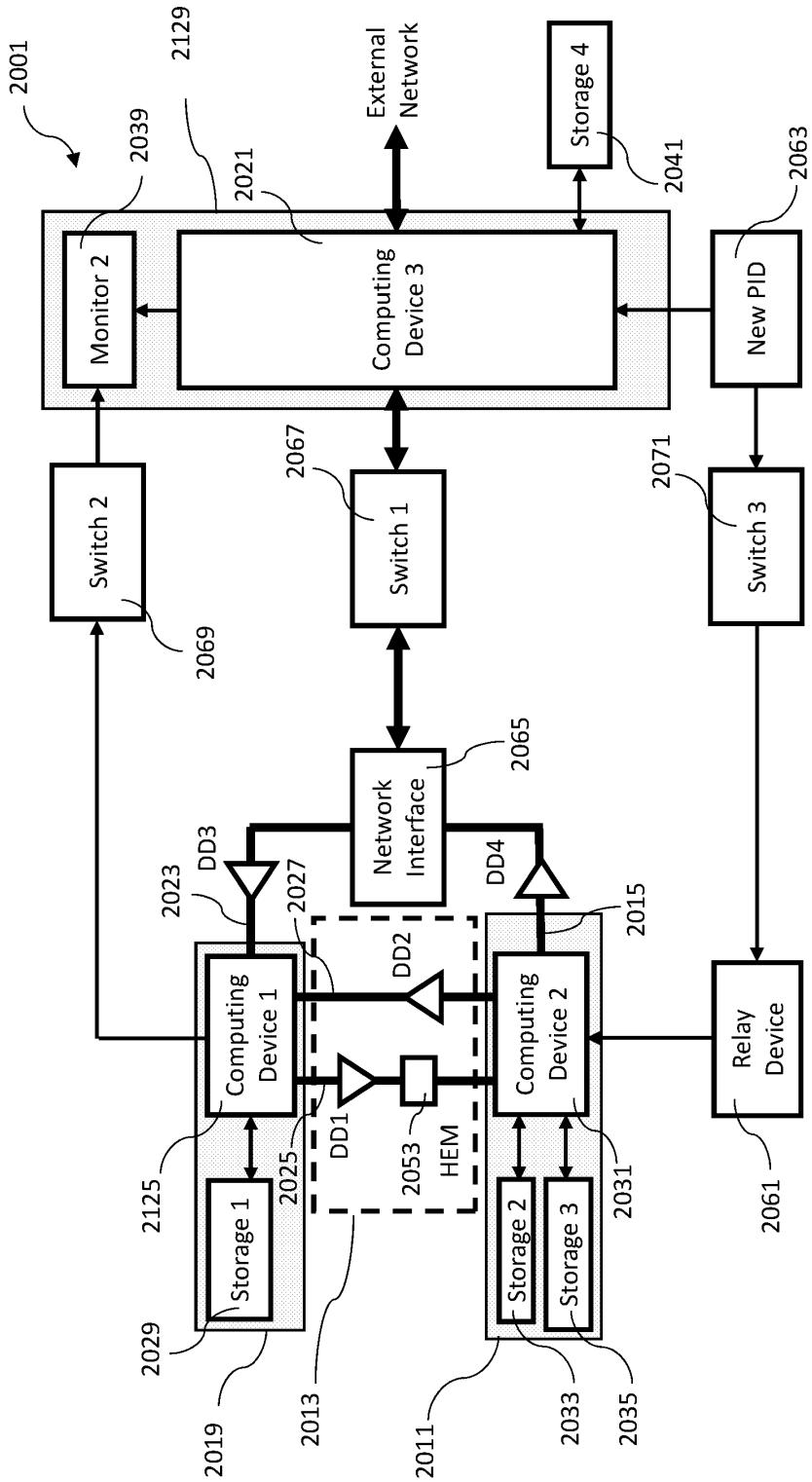

2001
2129
External Network
Storage 4
2041
2039
2021
2063
Monitor 2
Computing Device 3
New PID
2067
2071
Switch 2
Switch 1
Switch 3
2069
Network Interface
2065
DD3
DD4
2023
2027
2015
DD2
Computing Device 1
Computing Device 2
Relay Device
DD1
2053
HEM
2125
2025
2031
2061
Storage 1
Storage 2
Storage 3
2029
2013
2011
2033
2035
2019

Fig. 12

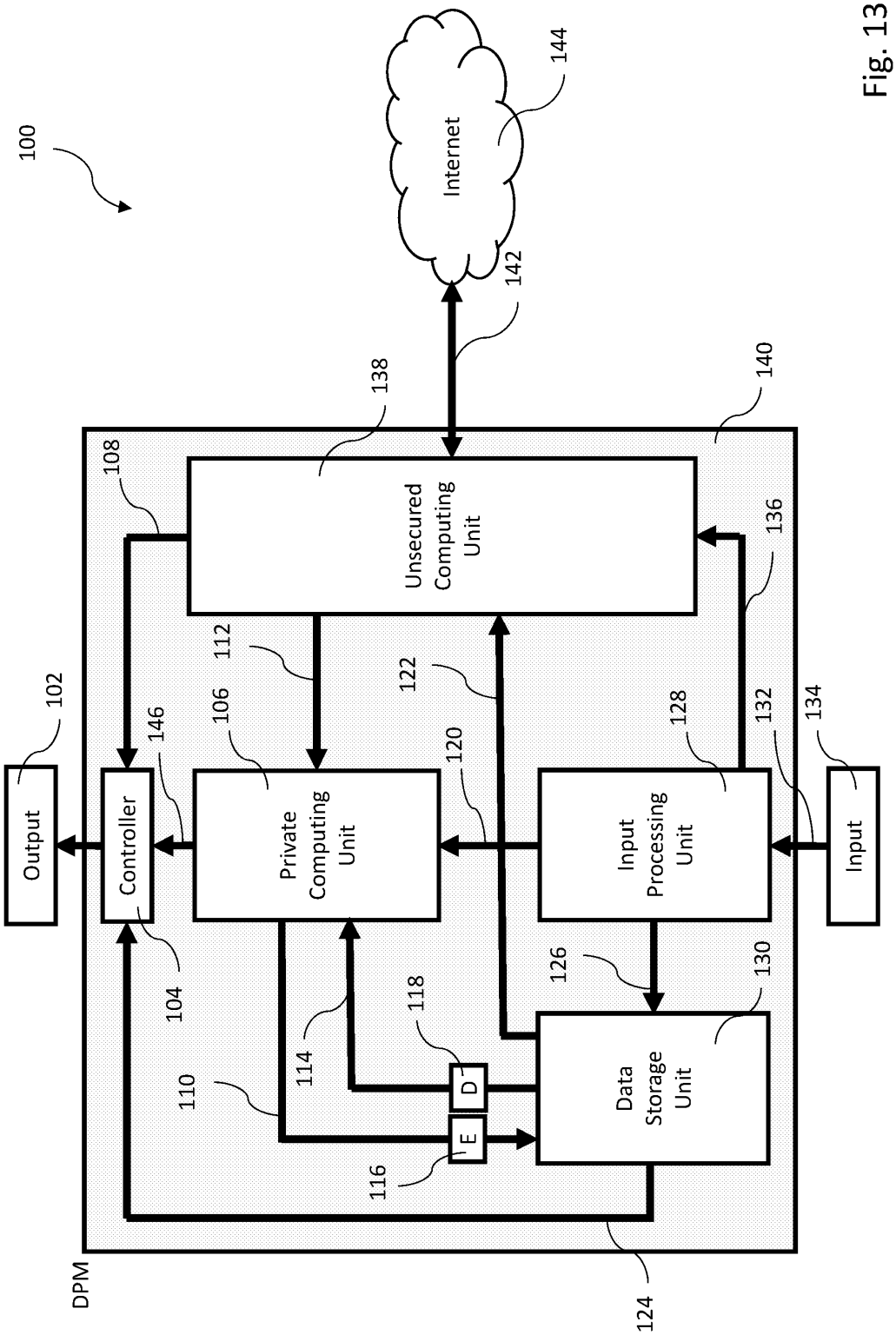

100
Internet
144
142
138
140
108
Unsecured Computing Unit
136
112
122
102
146
106
120
128
132
134
Output
Controller
Private Computing Unit
Input Processing Unit
Input
104
126
130
118
114
110
D
E
Data Storage Unit
116
DPM
124

Fig. 13a

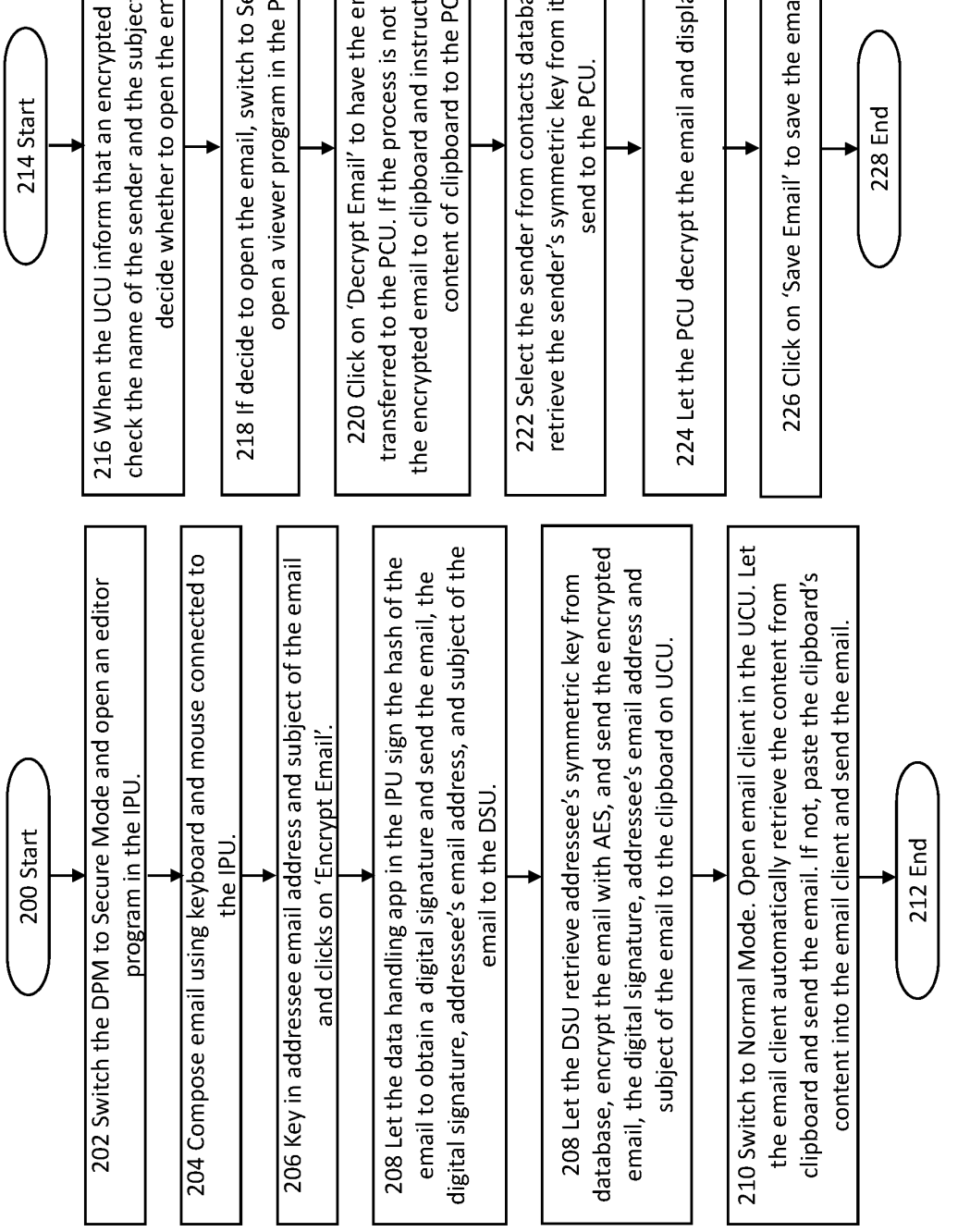

200 Start
202 Switch the DPM to Secure Mode and open an editor program in the IPU.
204 Compose email using keyboard and mouse connected to the IPU.
206 Key in addressee email address and subject of the email and clicks on 'Encrypt Email'.
208 Let the data handling app in the IPU sign the hash of the email to obtain a digital signature and send the email, the digital signature, addressee's email address, and subject of the email to the DSU.
208 Let the DSU retrieve addressee's symmetric key from database, encrypt the email with AES, and send the encrypted email, the digital signature, addressee's email address and subject of the email to the clipboard on UCU.
210 Switch to Normal Mode. Open email client in the UCU. Let the email client automatically retrieve the content from clipboard and send the email. If not, paste the clipboard's content into the email client and send the email.
212 End
214 Start
216 When the UCU inform that an encrypted email has arrived, check the name of the sender and the subject of the email and decide whether to open the email.
218 If decide to open the email, switch to Secure Mode and open a viewer program in the PCU.
220 Click on 'Decrypt Email' to have the encrypted email transferred to the PCU. If the process is not automatic, copy the encrypted email to clipboard and instruct the UCU to send content of clipboard to the PCU
222 Select the sender from contacts database and let DSU retrieve the sender's symmetric key from its database and send to the PCU.
224 Let the PCU decrypt the email and display on the viewer.
226 Click on 'Save Email' to save the email in the DSU.
228 End

Fig. 13b

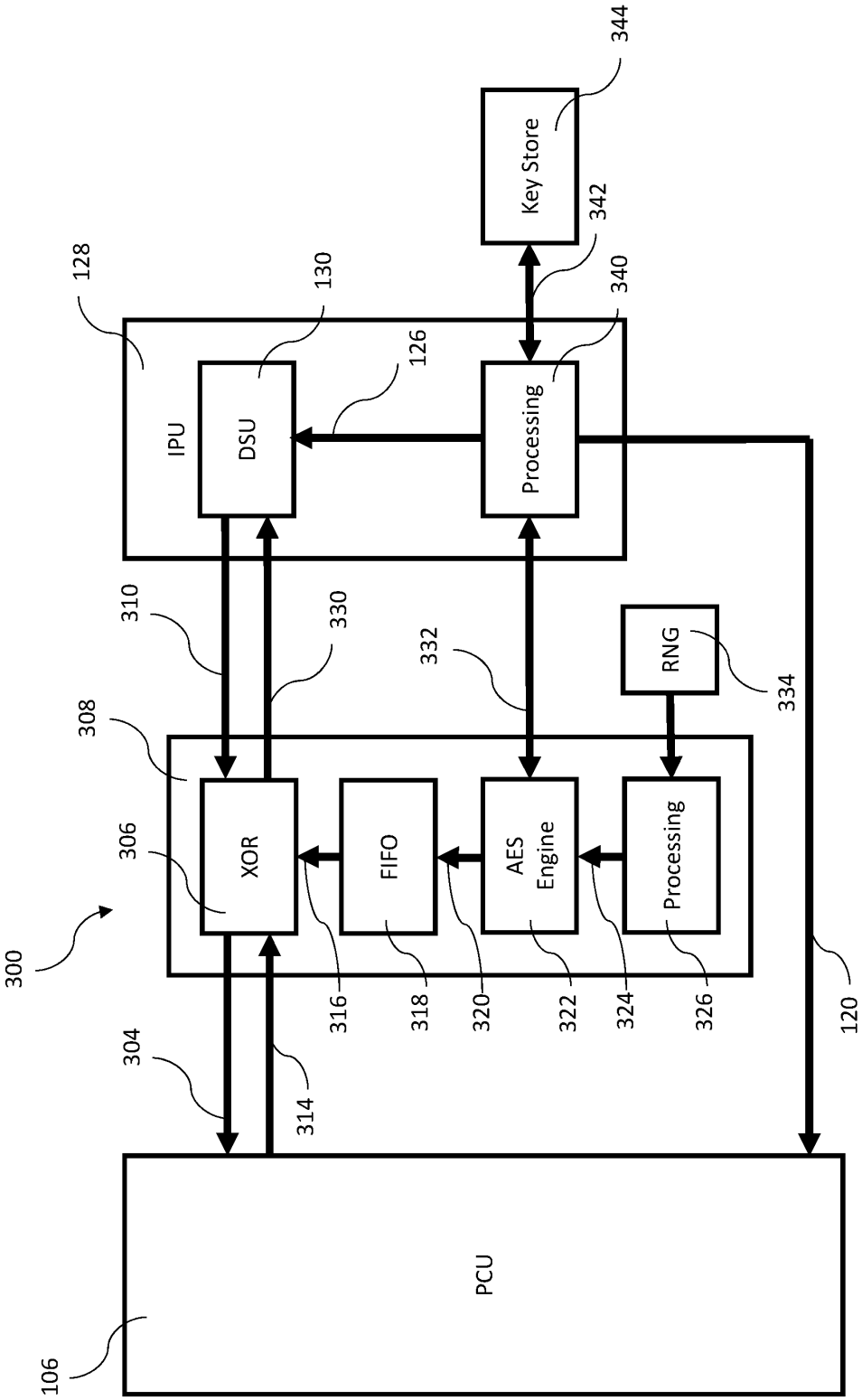

Key Store
344
342
340
128
130
126
IPU
DSU
Processing
310
330
332
RNG
334
308
306
XOR
FIFO
AES Engine
Processing
300
316
318
320
322
324
326
120
304
314
PCU
106

Fig. 14

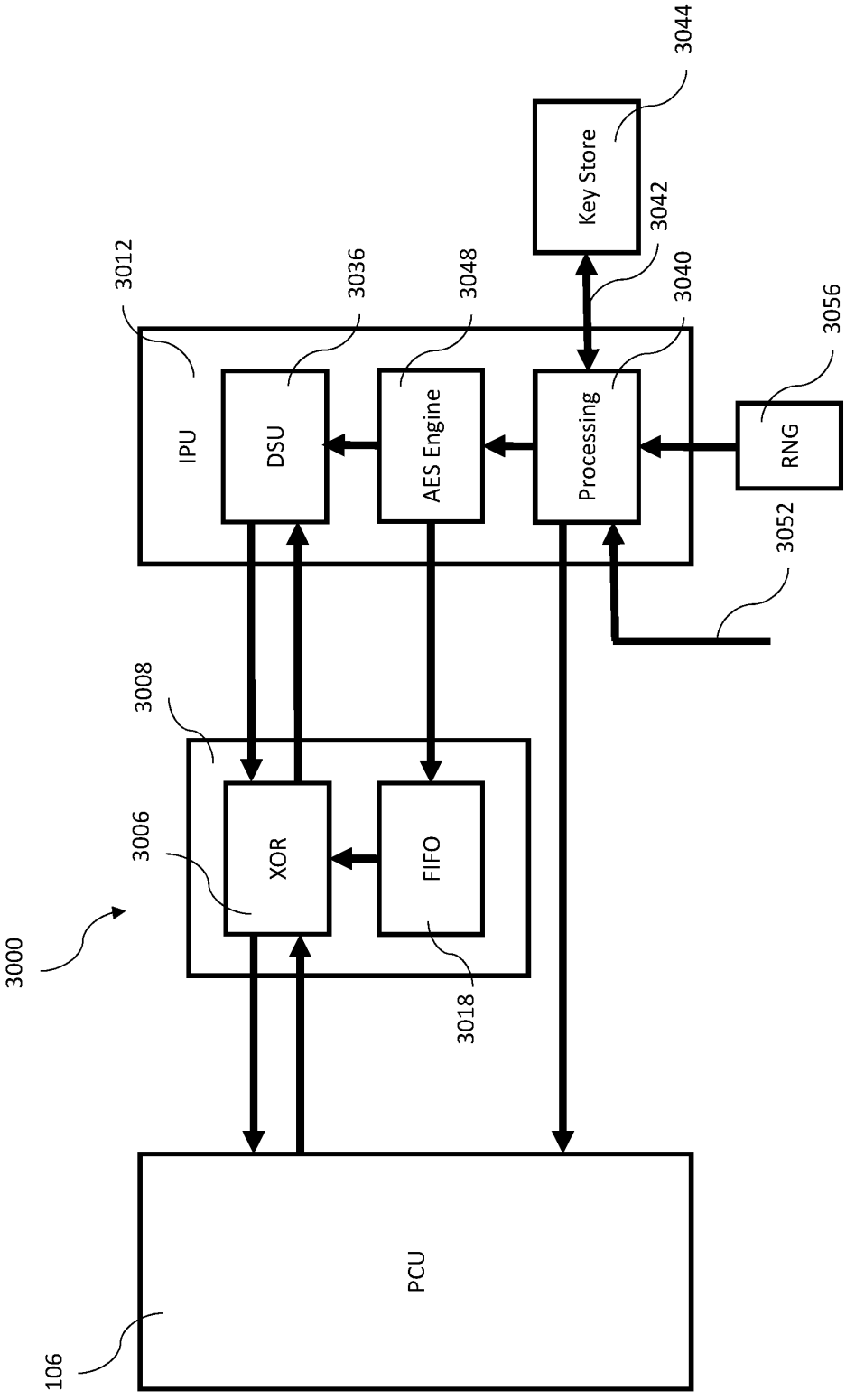

3044
Key Store
3042
3012
3036
3048
3040
3056
IPU
DSU
AES Engine
Processing
RNG
3052
3008
3006
XOR
FIFO
3000
3018
PCU
106

Fig. 15

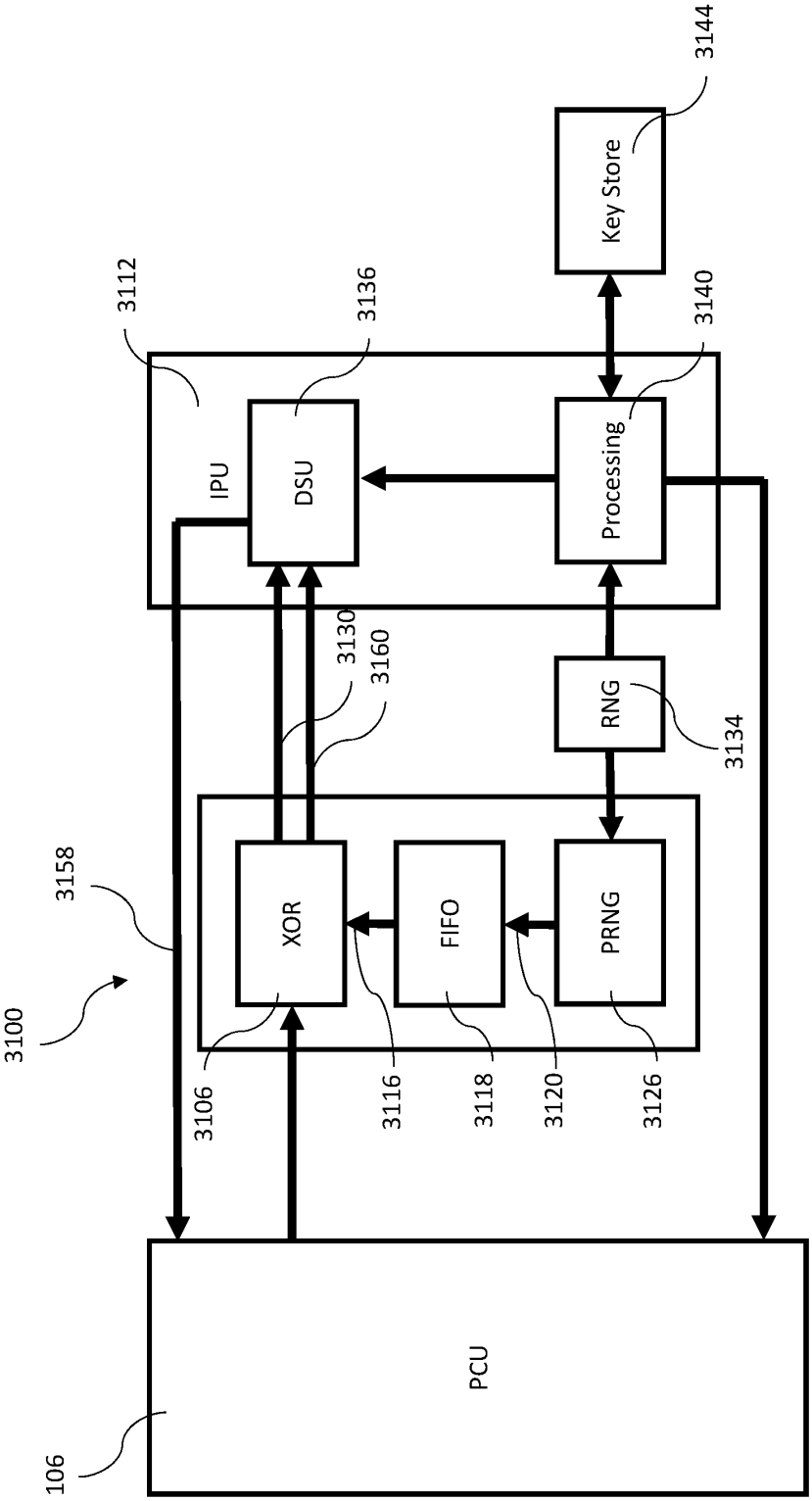

3144
Key Store
3112
3136
3140
IPU
DSU
Processing
3130
3160
RNG
3134
3158
XOR
FIFO
PRNG
3100
3106
3116
3118
3120
3126
PCU
106

Fig. 16

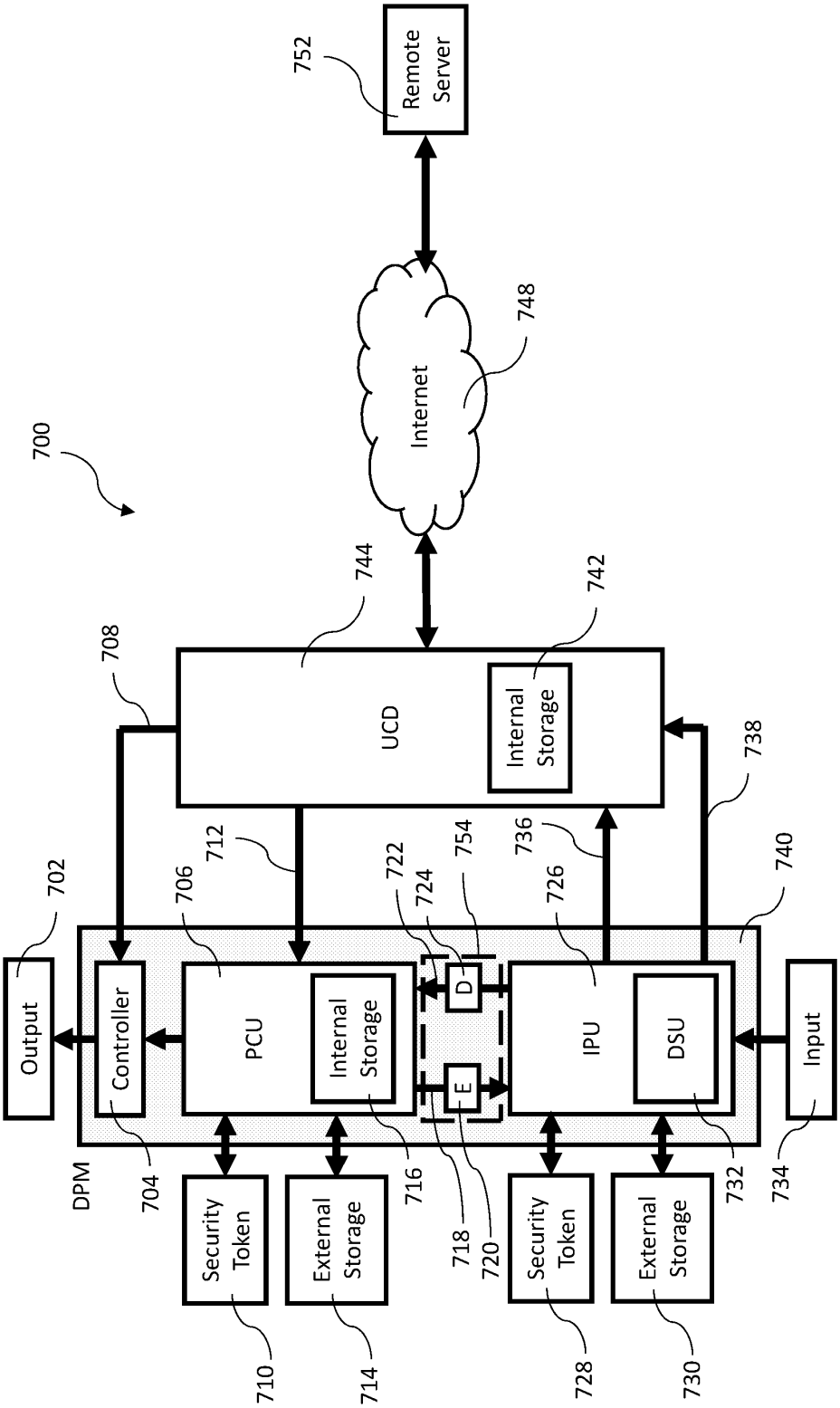

752
Remote Server
748
Internet
700
744
742
708
UCD
Internal Storage
738
712
754
736
740
722
724
726
706
702
Output
Controller
PCU
Internal Storage
D
E
IPU
DSU
Input
DPM
704
716
718
720
732
734
Security Token
External Storage
Security Token
External Storage
710
714
728
730

Fig. 17

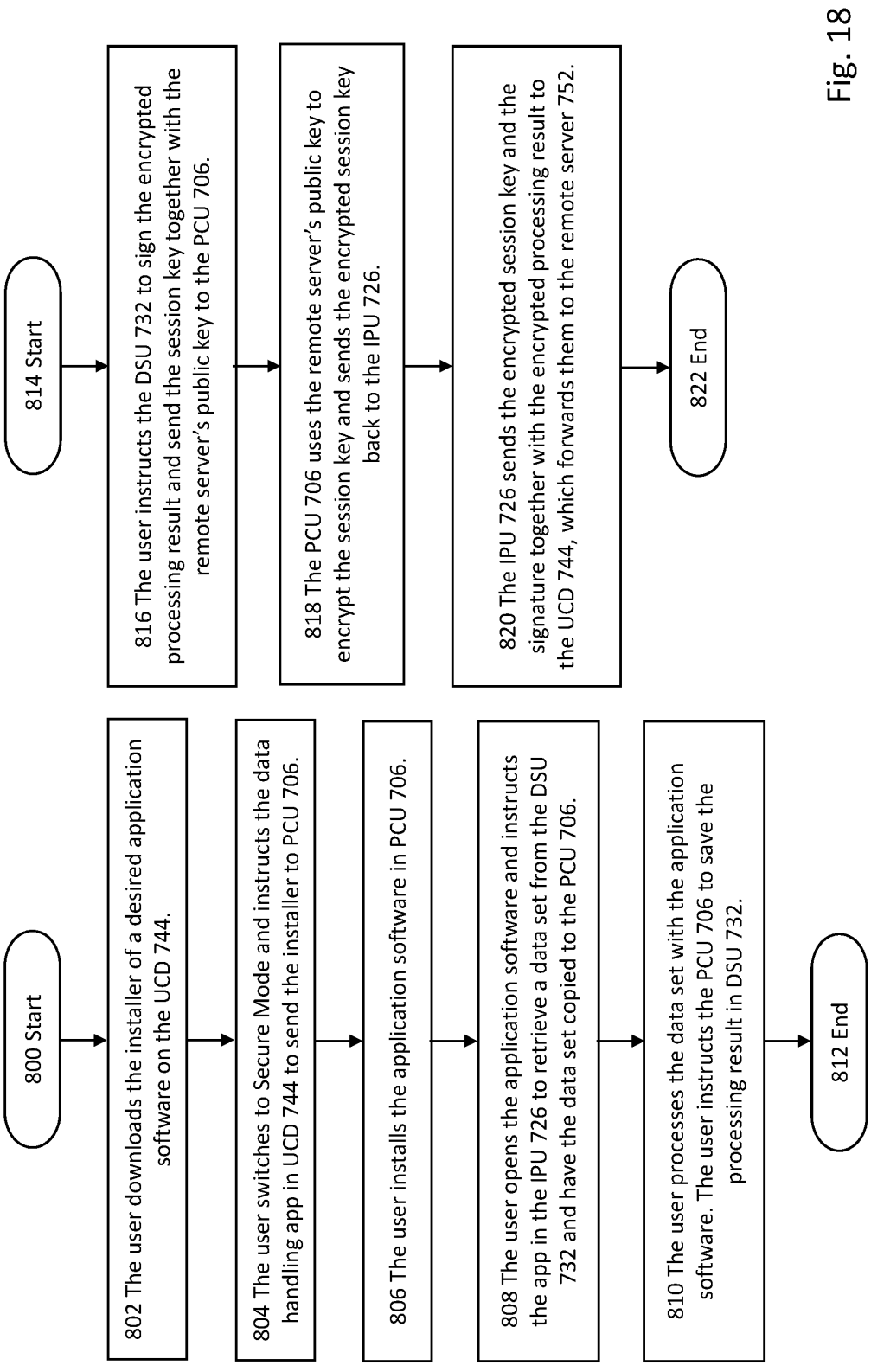

800 Start
802 The user downloads the installer of a desired application software on the UCD 744.
804 The user switches to Secure Mode and instructs the data handling app in UCD 744 to send the installer to PCU 706.
806 The user installs the application software in PCU 706.
808 The user opens the application software and instructs the app in the IPU 726 to retrieve a data set from the DSU 732 and have the data set copied to the PCU 706.
810 The user processes the data set with the application software. The user instructs the PCU 706 to save the processing result in DSU 732.
812 End
814 Start
816 The user instructs the DSU 732 to sign the encrypted processing result and send the session key together with the remote server's public key to the PCU 706.
818 The PCU 706 uses the remote server's public key to encrypt the session key and sends the encrypted session key back to the IPU 726.
820 The IPU 726 sends the encrypted session key and the signature together with the encrypted processing result to the UCD 744, which forwards them to the remote server 752.
822 End

Fig. 18

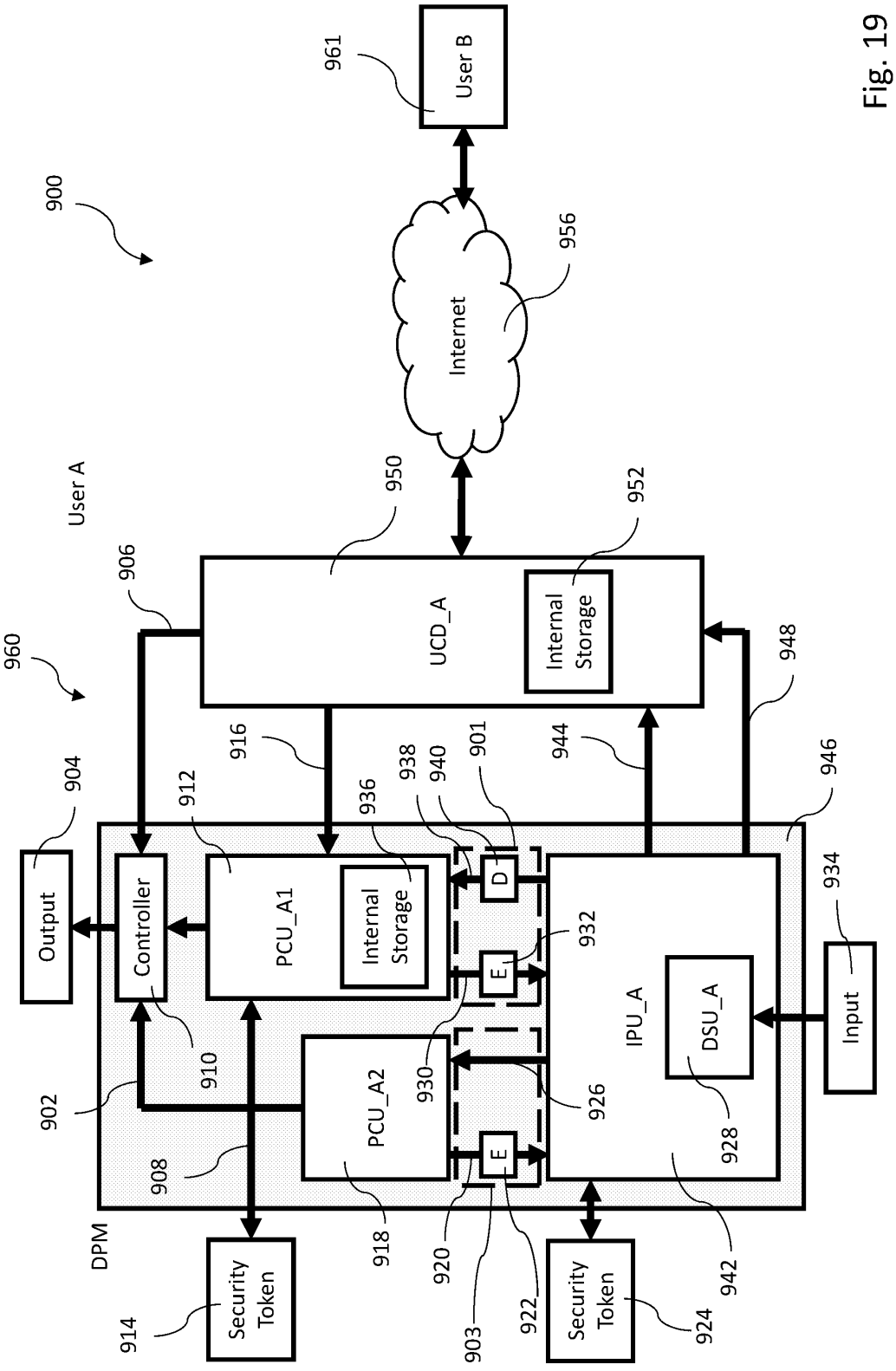

900
User A
960
User B
961
Internet
956
UCD_A
950
Internal Storage
952
906
916
948
944
946
904
Output
Controller
912
PCU_A1
Internal Storage
936
938
940
901
D
E
932
IPU_A
DSU_A
934
Input
910
902
PCU_A2
930
926
928
908
E
DPM
918
920
903
922
942
Security Token
914
Security Token
924

Fig. 19

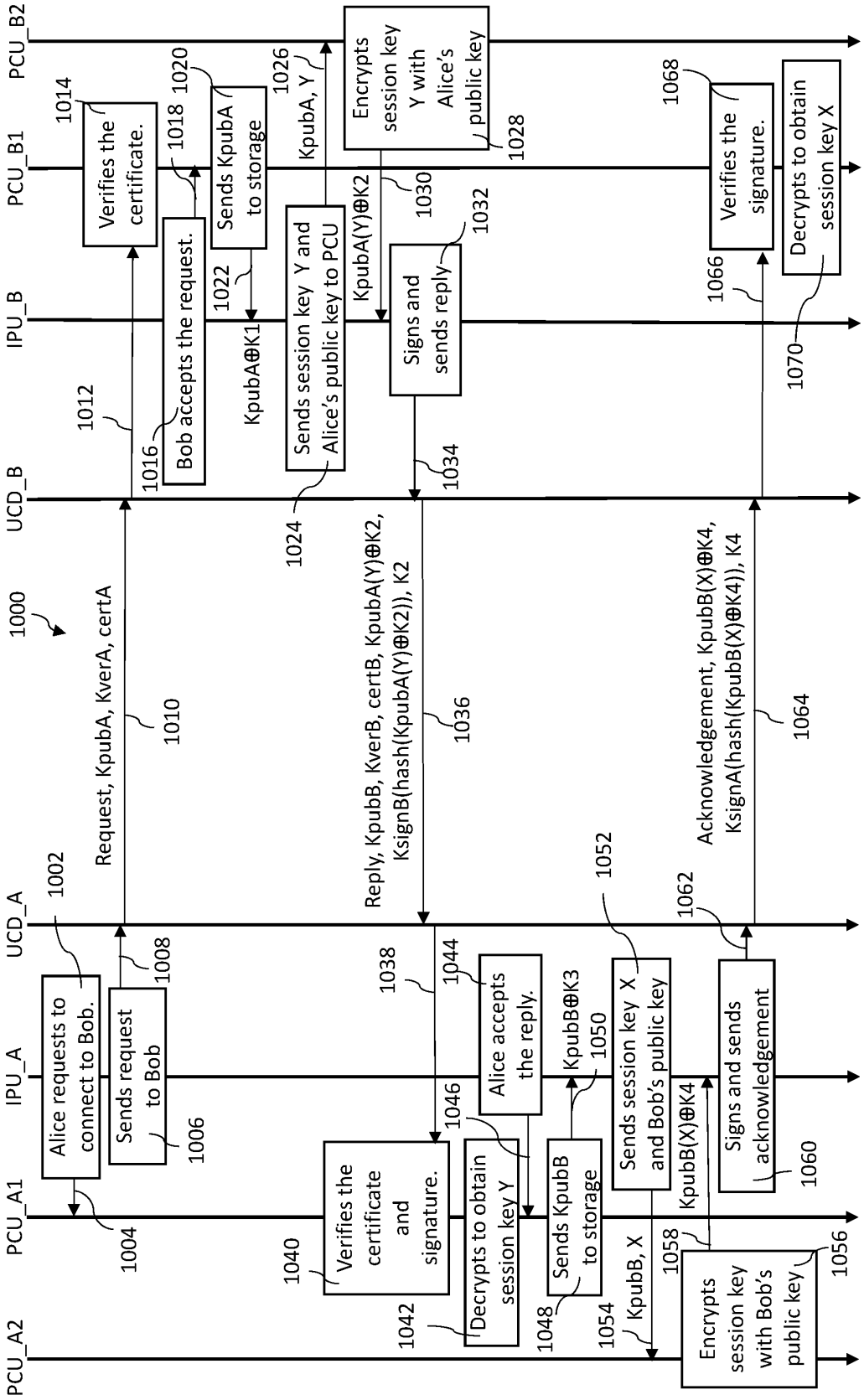

PCU_A2
PCU_A1
IPU_A
UCD_A
UCD_B
IPU_B
PCU_B1
PCU_B2
1000
Alice requests to connect to Bob.
1004
Sends request to Bob
1006
1008
Request, KpubA, KverA, certA
1010
1012
Verifies the certificate.
1014
Bob accepts the request.
1016
1018
Sends KpubA to storage
1020
KpubA⊕K1
1022
KpubA, Y
1026
Sends session key Y and Alice's public key to PCU
1024
Encrypts session key Y with Alice's public key
1028
KpubA(Y)⊕K2
1030
Signs and sends reply
1032
1034
Reply, KpubB, KverB, certB, KpubA(Y)⊕K2, KsignB(hash(KpubA(Y)⊕K2)), K2
1036
1038
Verifies the certificate and signature.
1040
Decrypts to obtain session key Y
1042
1044
Alice accepts the reply.
1046
KpubB⊕K3
1048
Sends KpubB to storage
1050
Sends session key X and Bob's public key
1052
KpubB, X
1054
Encrypts session key with Bob's public key
1056
KpubB(X)⊕K4
1058
Signs and sends acknowledgement
1060
Acknowledgement, KpubB(X)⊕K4, KsignA(hash(KpubB(X)⊕K4)), K4
1062
1064
1066
Verifies the signature.
1068
Decrypts to obtain session key X
1070

Fig. 20

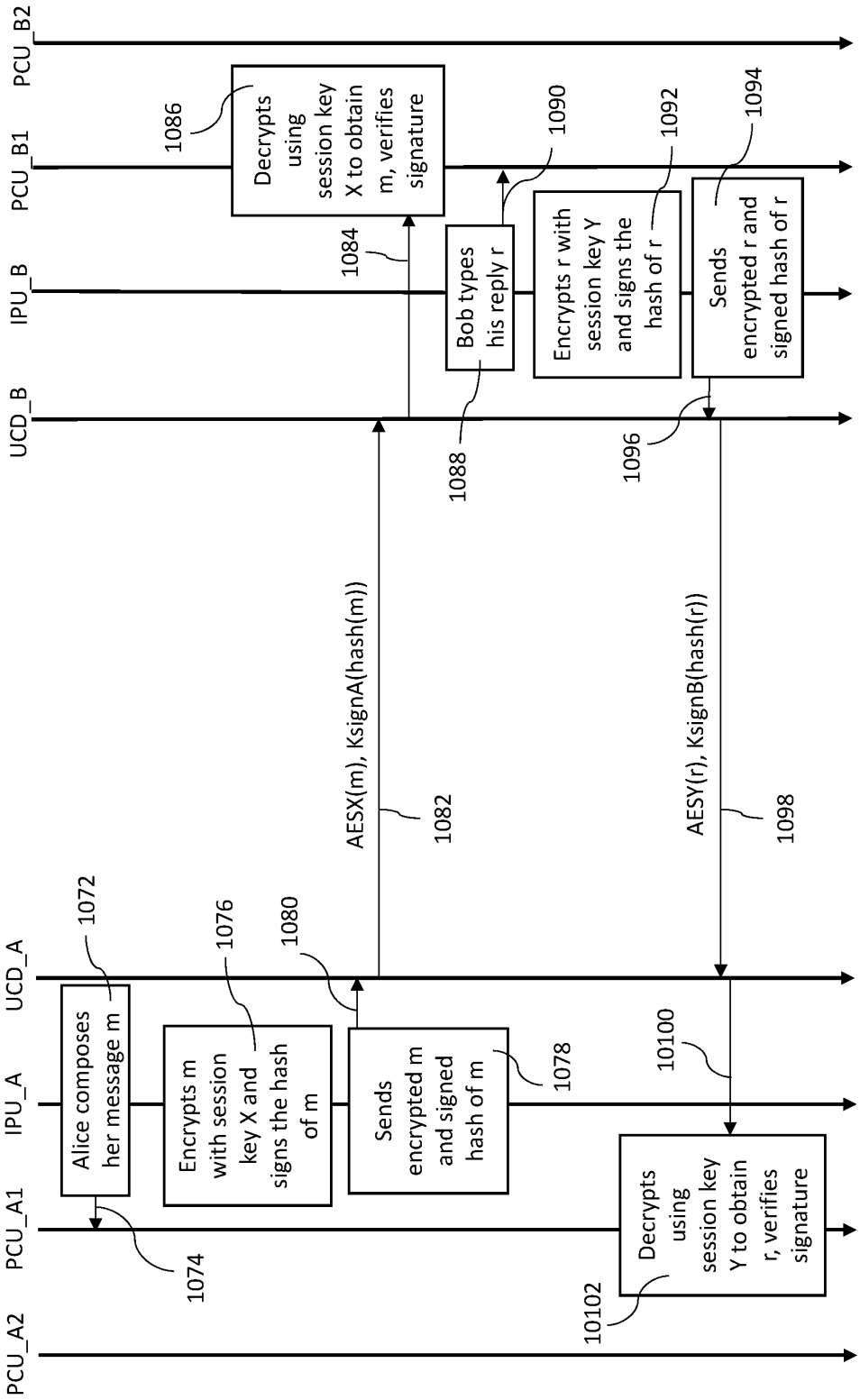

PCU_B2
PCU_B1
IPU_B
UCD_B
UCD_A
IPU_A
PCU_A1
PCU_A2
Alice composes her message m
Encrypts m with session key X and signs the hash of m
Sends encrypted m and signed hash of m
Decrypts using session key Y to obtain r, verifies signature
Bob types his reply r
Encrypts r with session key Y and signs the hash of r
Sends encrypted r and signed hash of r
Decrypts using session key X to obtain m, verifies signature
AESX(m), KsignA(hash(m))
AESY(r), KsignB(hash(r))
1072
1074
1076
1078
1080
1082
1084
1086
1088
1090
1092
1094
1096
1098
10100
10102

Fig. 21

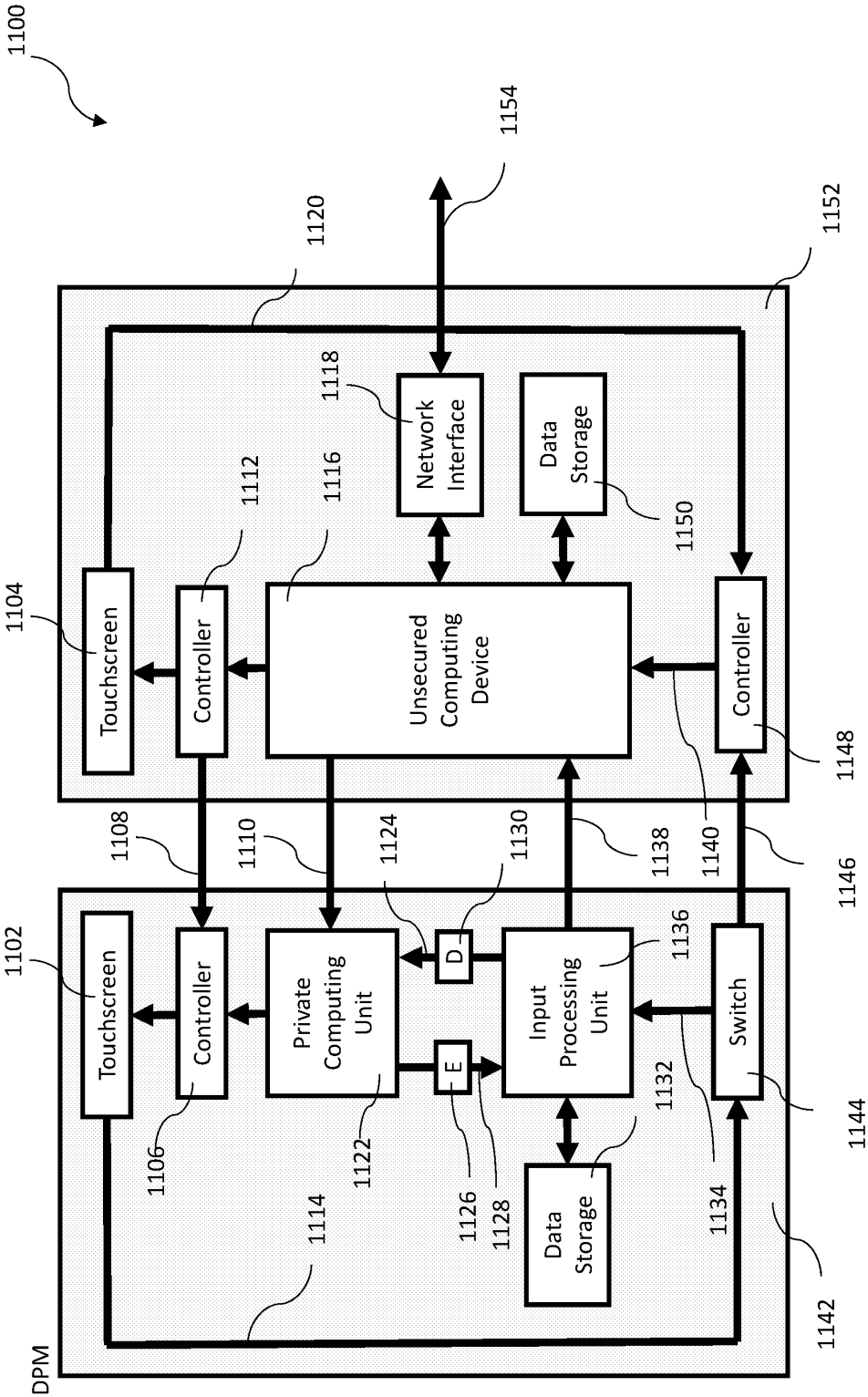

1100
1154
1120
1152
1118
Network Interface
Data Storage
1150
1112
1116
1104
Touchscreen
Controller
Unsecured Computing Device
Controller
1148
1108
1110
1124
1130
1138
1140
1146
1102
Touchscreen
Controller
Private Computing Unit
D
E
Input Processing Unit
1136
Switch
1106
1122
1126
1128
1132
1144
1114
Data Storage
1134
1142
DPM

Fig. 22

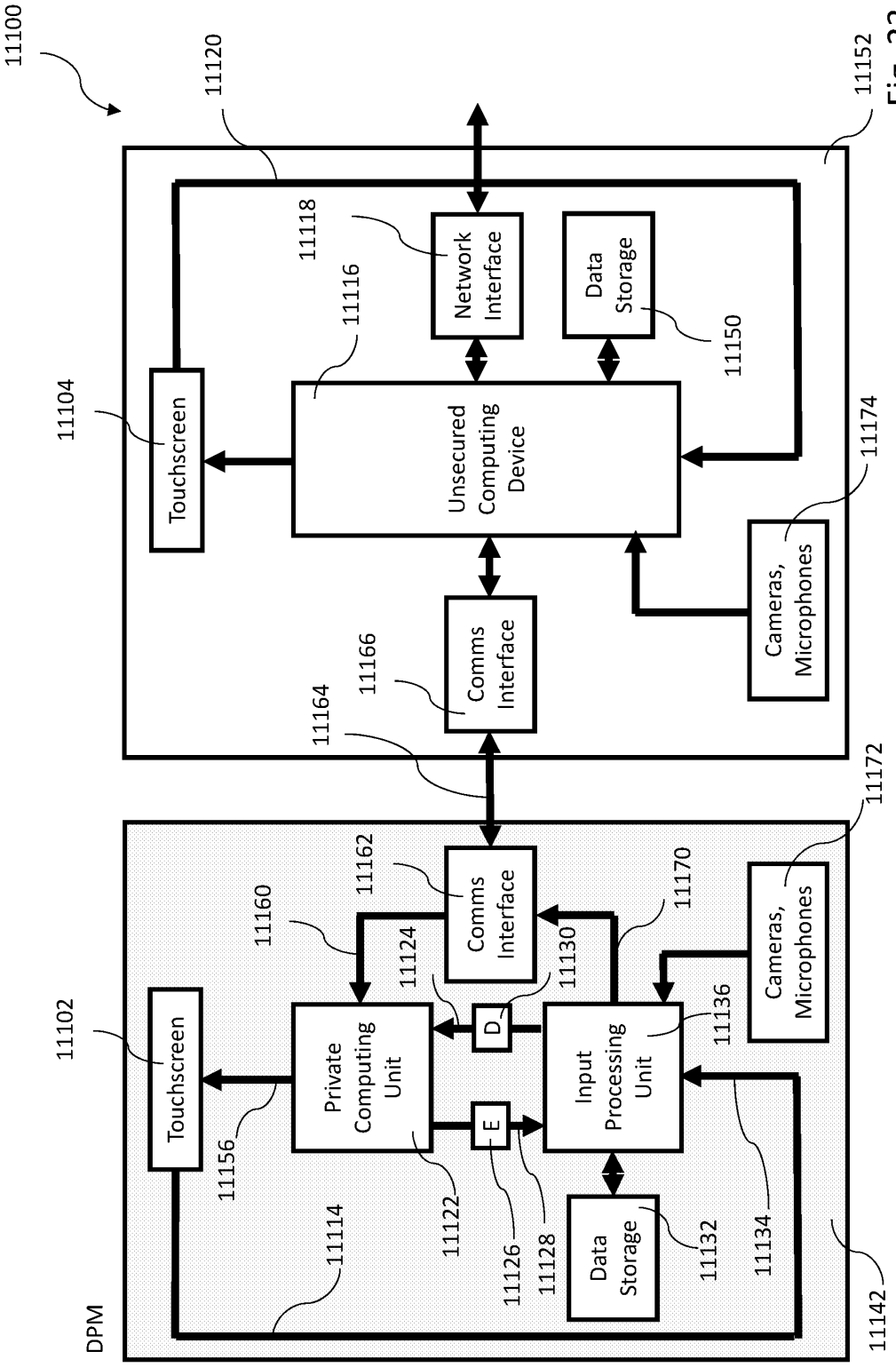

11100
11120
11152
11118
Network Interface
Data Storage
11150
11116
11104
Touchscreen
Unsecured Computing Device
11174
Cameras, Microphones
11166
Comms Interface
11164
11172
11162
Comms Interface
11160
11170
11124
11130
Cameras, Microphones
11102
Touchscreen
Private Computing Unit
D
Input Processing Unit
11136
11156
E
11122
11126
11128
Data Storage
11132
11134
11114
DPM
11142

Fig. 23

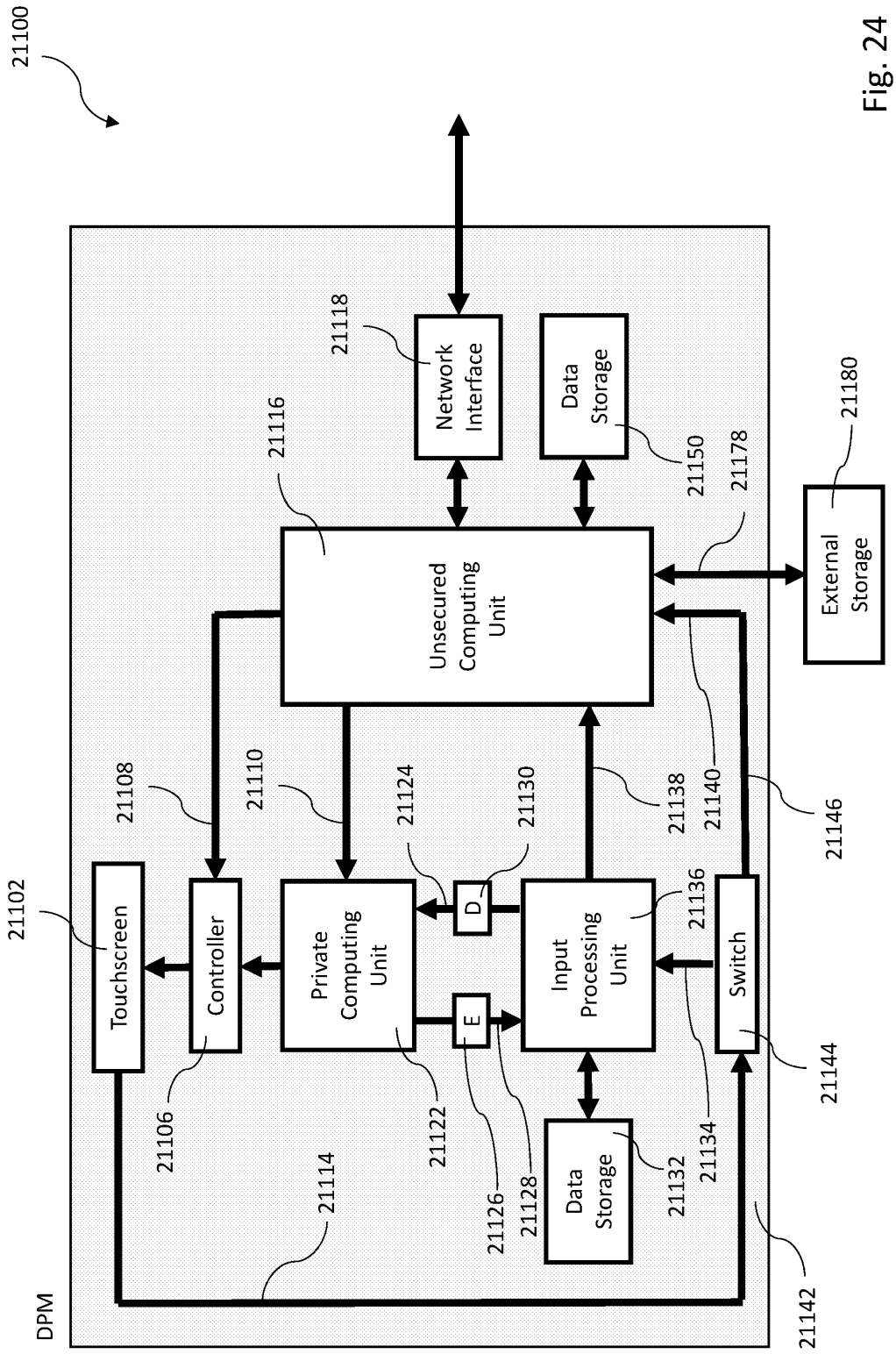

21100
DPM
21102
Touchscreen
21106
Controller
21108
21110
Private Computing Unit
21114
21116
Unsecured Computing Unit
21118
Network Interface
21122
21124
D
21126
E
21128
21130
Data Storage
21132
21134
21136
Input Processing Unit
21138
21140
21142
21144
Switch
21146
Data Storage
21150
21178
External Storage
21180

Fig. 24

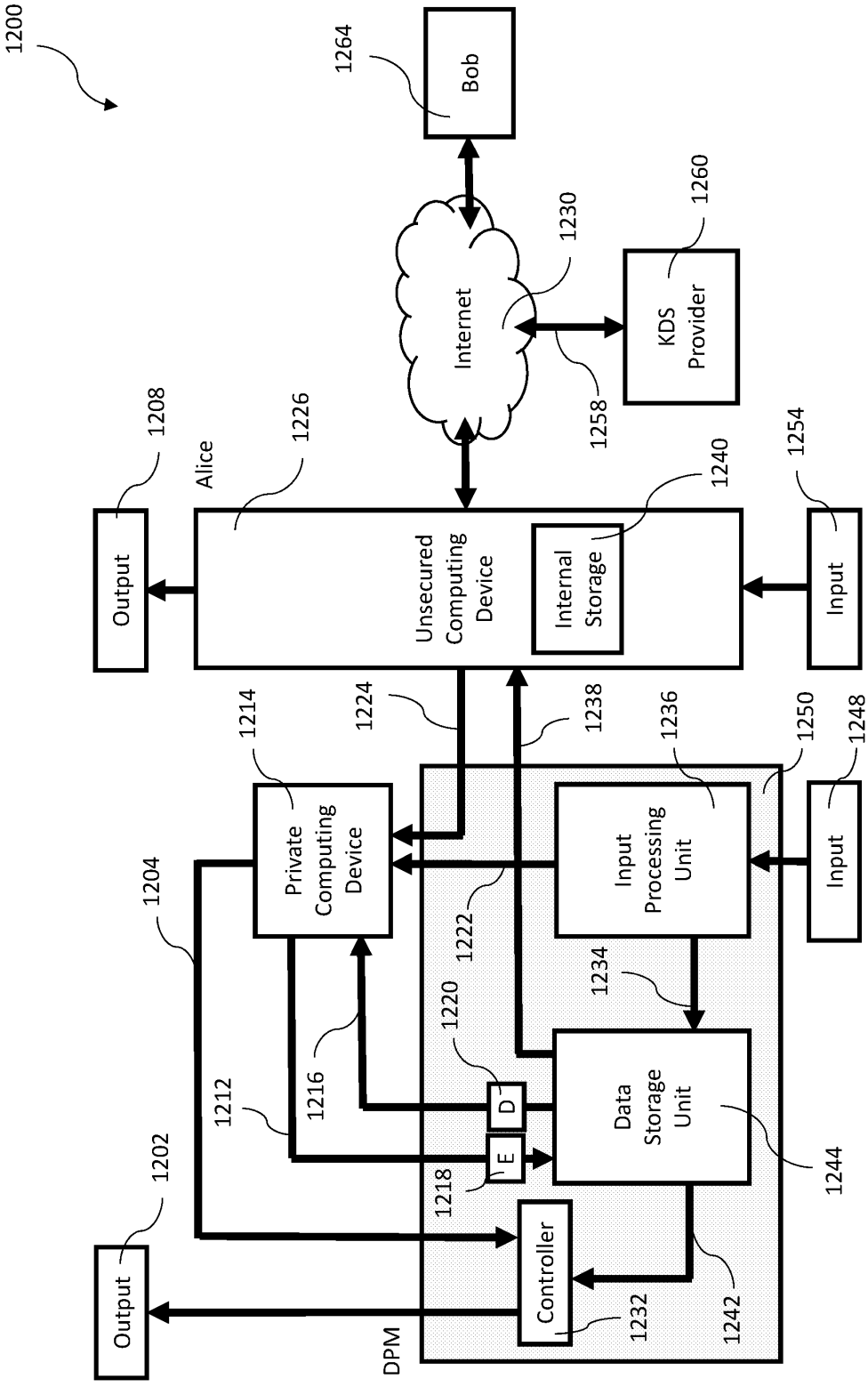

1200
1264
Bob
1230
Internet
1260
KDS Provider
1258
1208
Alice
1226
1240
1254
Output
Unsecured Computing Device
Internal Storage
Input
1214
1224
1238
1236
1250
1248
Private Computing Device
Input Processing Unit
Input
1204
1222
1234
1220
1216
D
Data Storage Unit
1212
E
1244
1202
1218
Output
Controller
1232
1242
DPM

Fig. 25

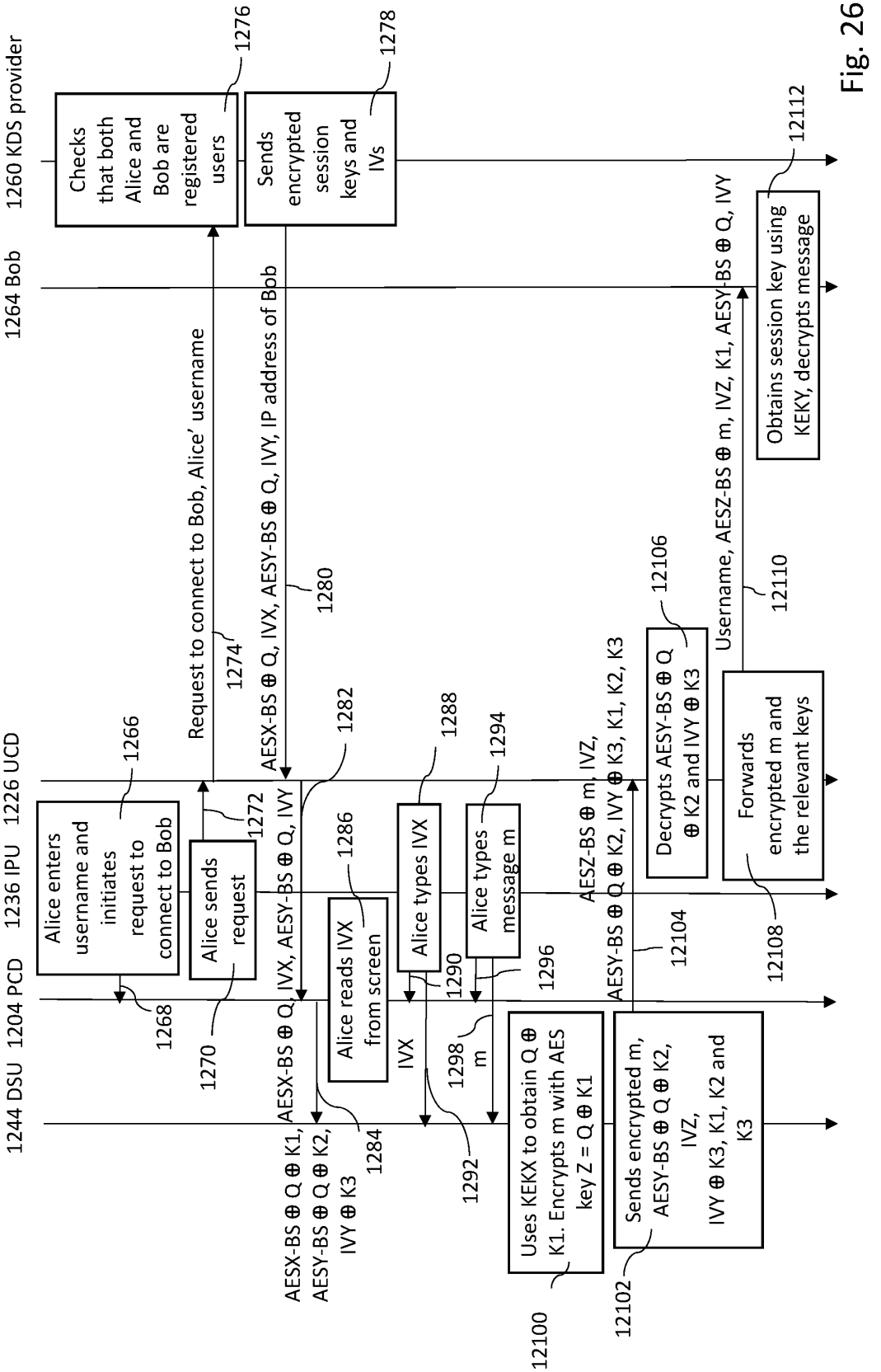

1244 DSU
1204 PCD
1236 IPU
1226 UCD
1264 Bob
1260 KDS provider
Alice enters username and initiates request to connect to Bob
1266
Alice sends request
1272
Request to connect to Bob, Alice' username
1274
Checks that both Alice and Bob are registered users
1276
Sends encrypted session keys and IVs
1278
AESX-BS ⊕ Q, IVX, AESY-BS ⊕ Q, IVY, IP address of Bob
1280
AESX-BS ⊕ Q, IVX, AESY-BS ⊕ Q, IVY
1282
Alice reads IVX from screen
1286
Alice types IVX
1288
Alice types message m
1294
AESZ-BS ⊕ m, IVZ, AESY-BS ⊕ Q ⊕ K2, IVY ⊕ K3, K1, K2, K3
12104
Decrypts AESY-BS ⊕ Q ⊕ K2 and IVY ⊕ K3
12106
Forwards encrypted m and the relevant keys
12108
Username, AESZ-BS ⊕ m, IVZ, K1, AESY-BS ⊕ Q, IVY
12110
Obtains session key using KEKY, decrypts message
12112
1268
1270
AESX-BS ⊕ Q ⊕ K1, AESY-BS ⊕ Q ⊕ K2, IVY ⊕ K3
1284
IVX
1290
1298 m
1292
1296
Uses KEKX to obtain Q ⊕ K1. Encrypts m with AES key Z = Q ⊕ K1
12100
Sends encrypted m, AESY-BS ⊕ Q ⊕ K2, IVZ, IVY ⊕ K3, K1, K2 and K3
12102

Fig. 26

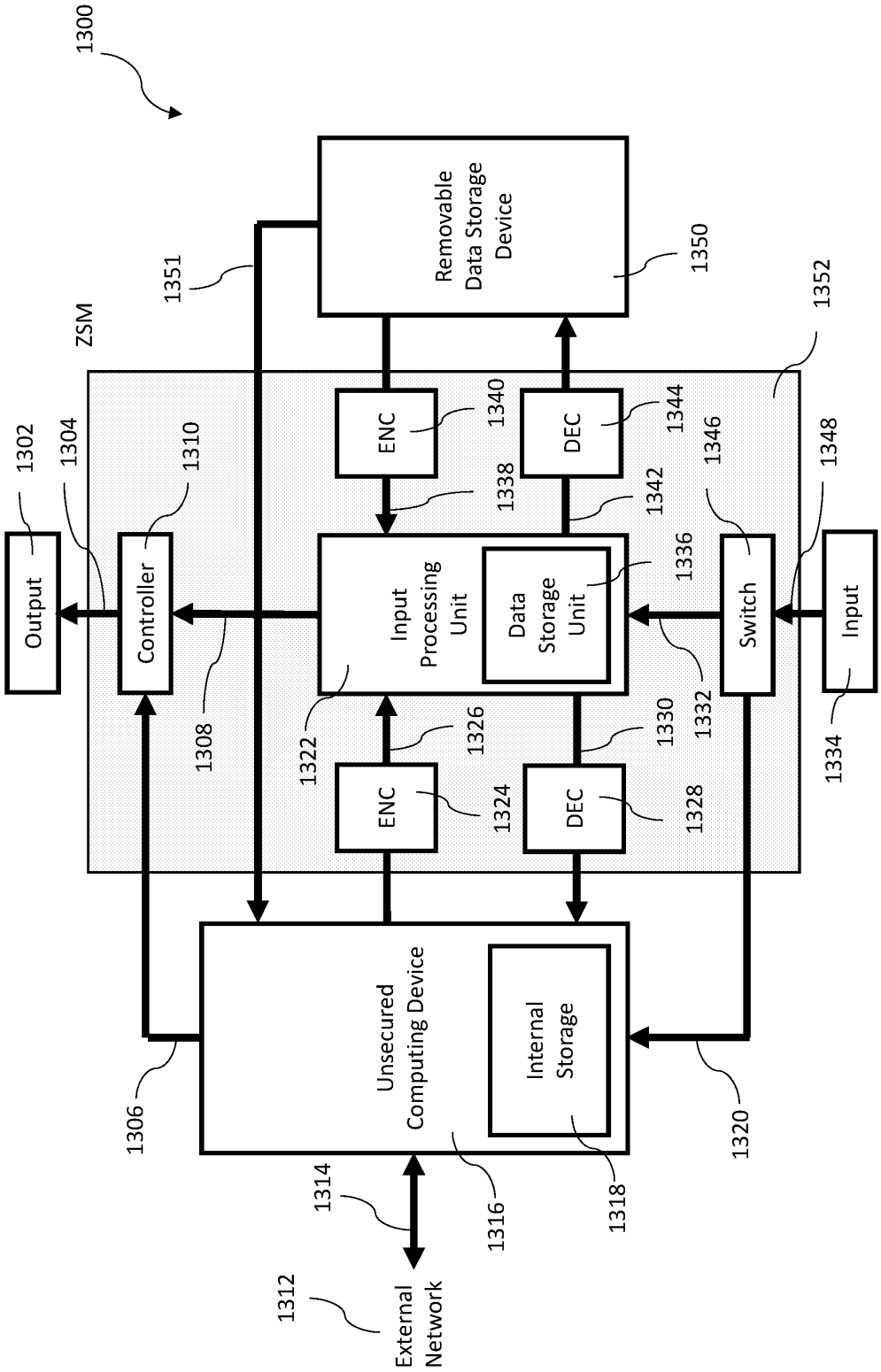

1300
Removable Data Storage Device
1350
1351
1352
ZSM
ENC
1340
DEC
1344
1338
1342
1346
1348
1302
1304
1310
Output
Controller
Input Processing Unit
Data Storage Unit
1336
Switch
Input
1308
1322
1326
1330
1332
1334
ENC
1324
DEC
1328
Unsecured Computing Device
Internal Storage
1306
1320
1314
1316
1318
1312
External Network

Fig. 27

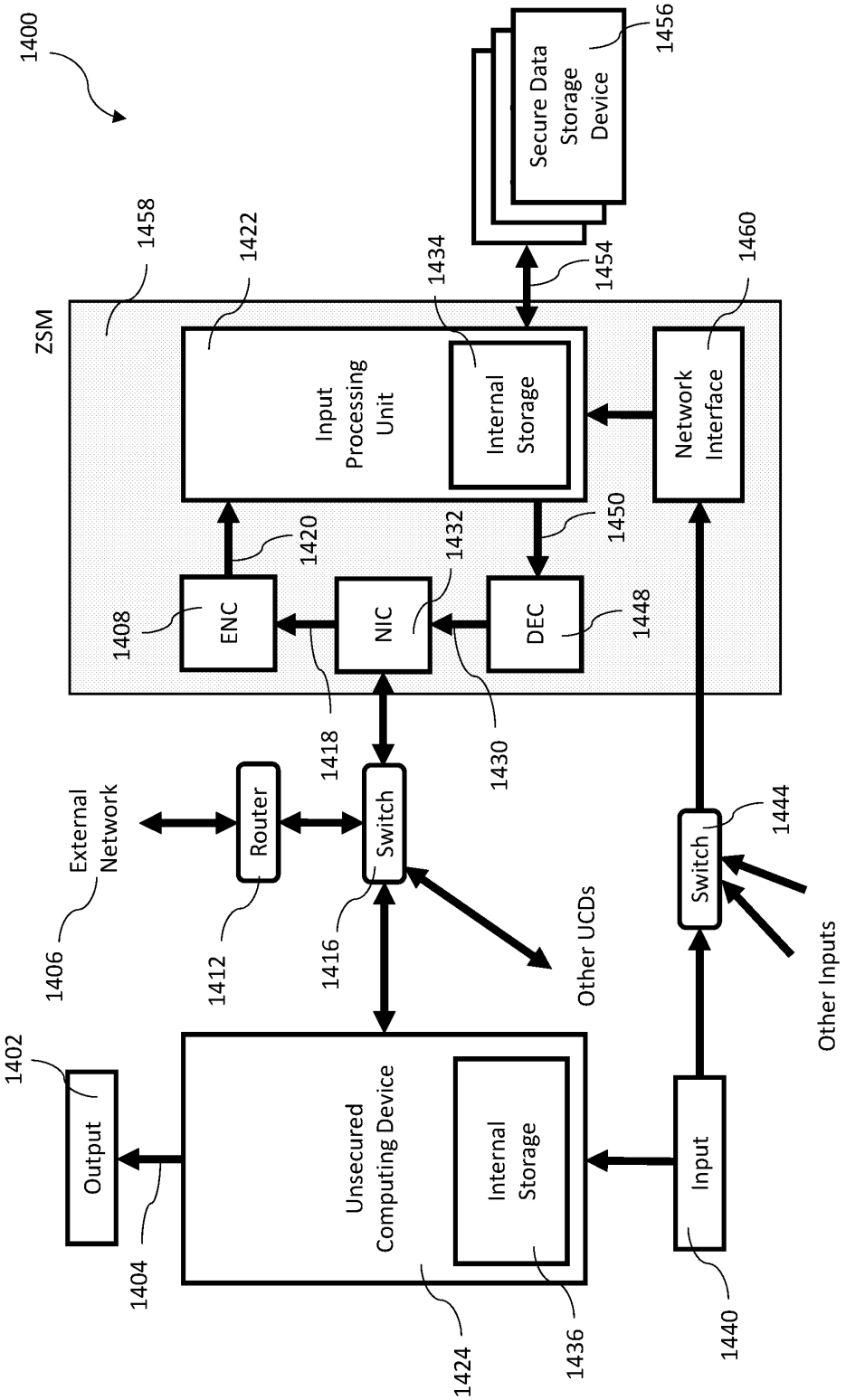

1400
Secure Data Storage Device
1456
1458
1422
1434
1454
1460
ZSM
Input Processing Unit
Internal Storage
Network Interface
1420
1432
1450
1408
ENC
NIC
DEC
1448
1418
1430
External Network
Router
Switch
1444
1406
1412
1416
Other UCDs
Switch
Other Inputs
1402
Output
Unsecured Computing Device
Internal Storage
Input
1404
1424
1436
1440

Fig. 28

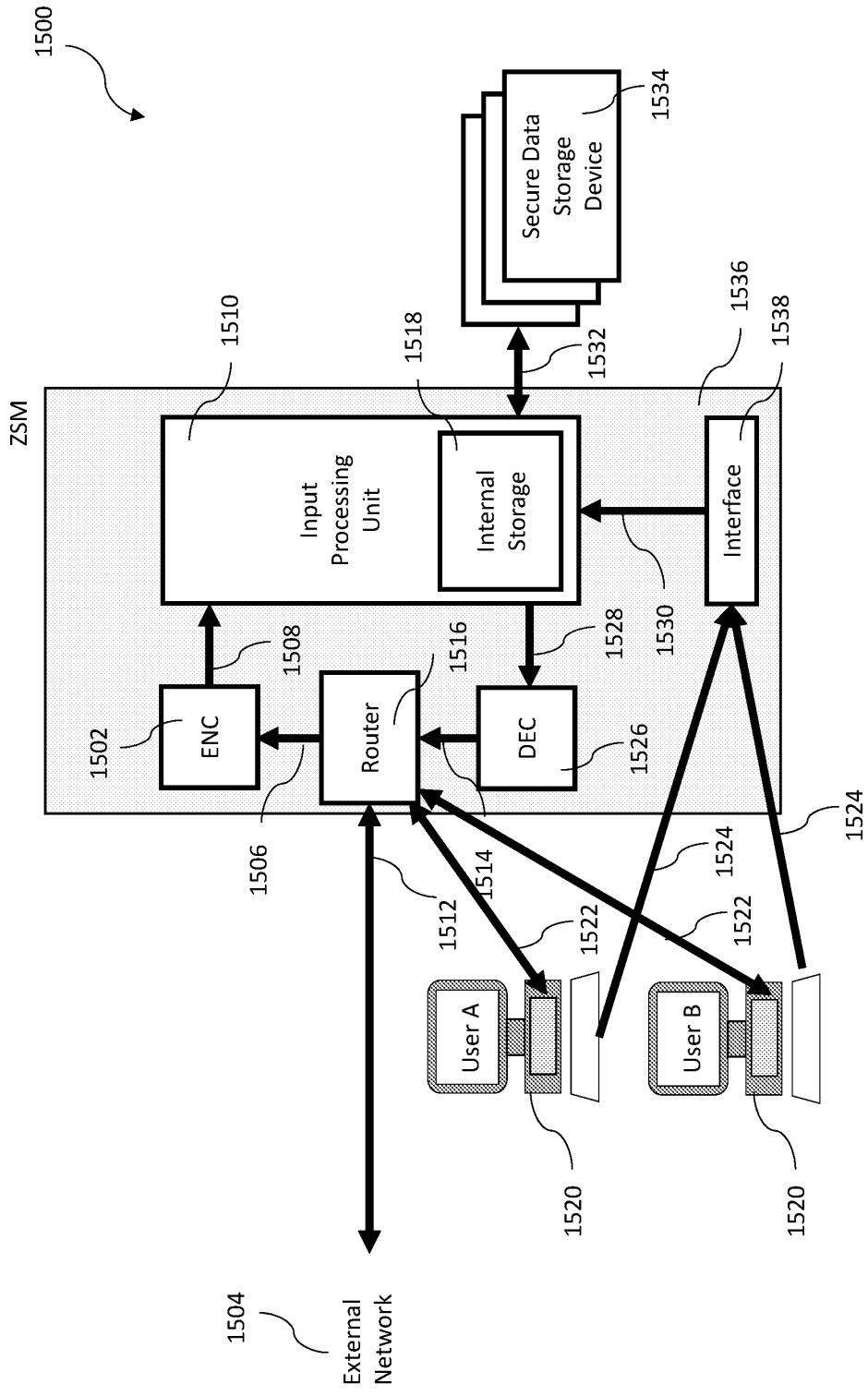

1500
Secure Data Storage Device
1534
1510
1518
1532
1536
1538
ZSM
Input Processing Unit
Internal Storage
Interface
1508
1516
1528
1530
1502
ENC
Router
DEC
1526
1506
1524
1514
1512
1522
1524
1522
User A
User B
1520
1520
1504
External Network

Fig. 29

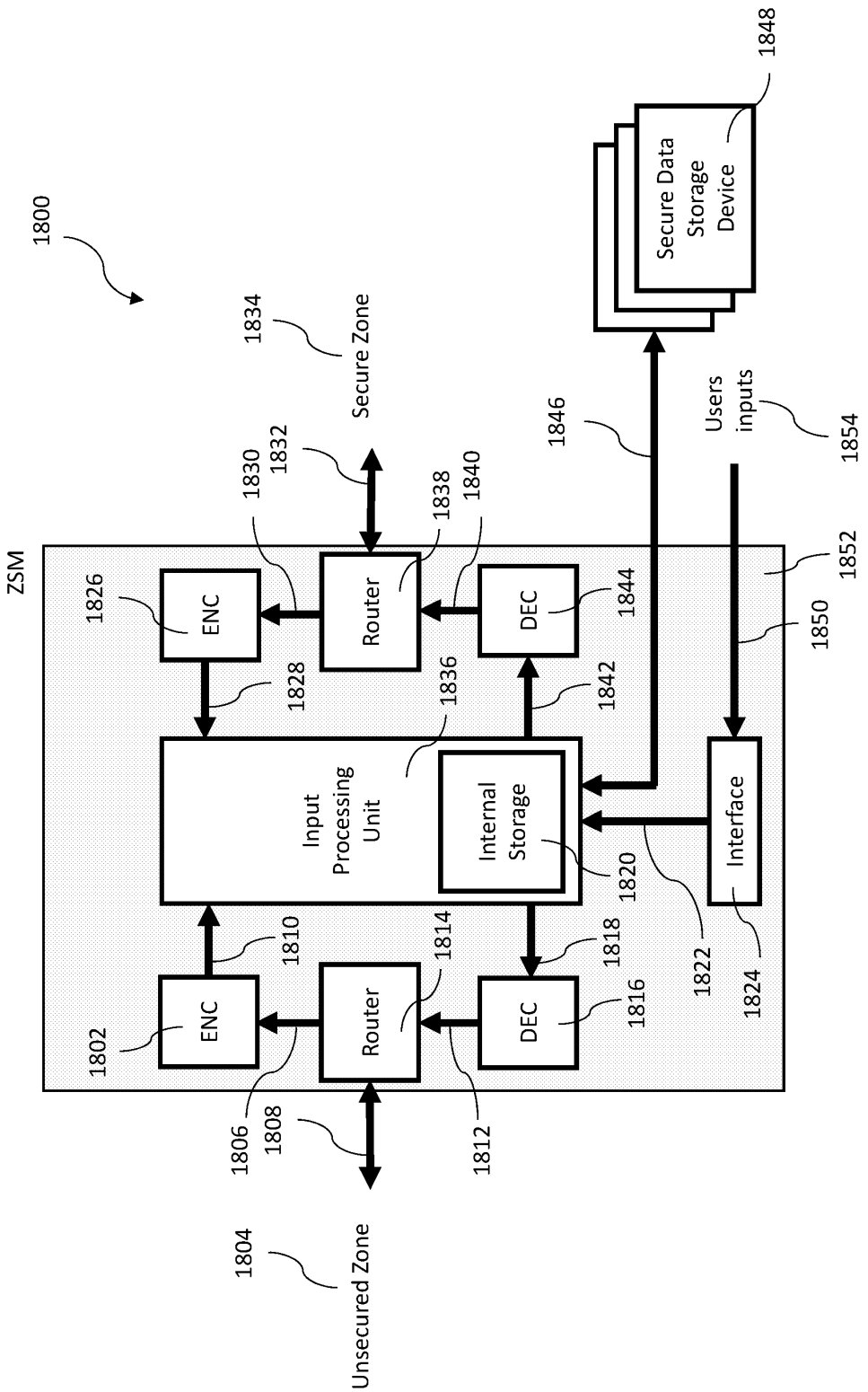

1800
1834
Secure Zone
1848
Secure Data Storage Device
1846
Users inputs
1854
1830
1832
1838
1840
ZSM
1852
1826
ENC
Router
DEC
1844
1850
1828
1836
1842
Input Processing Unit
Internal Storage
Interface
1820
1822
1824
1810
1814
1818
1802
ENC
Router
DEC
1816
1806
1808
1812
1804
Unsecured Zone

Fig. 30

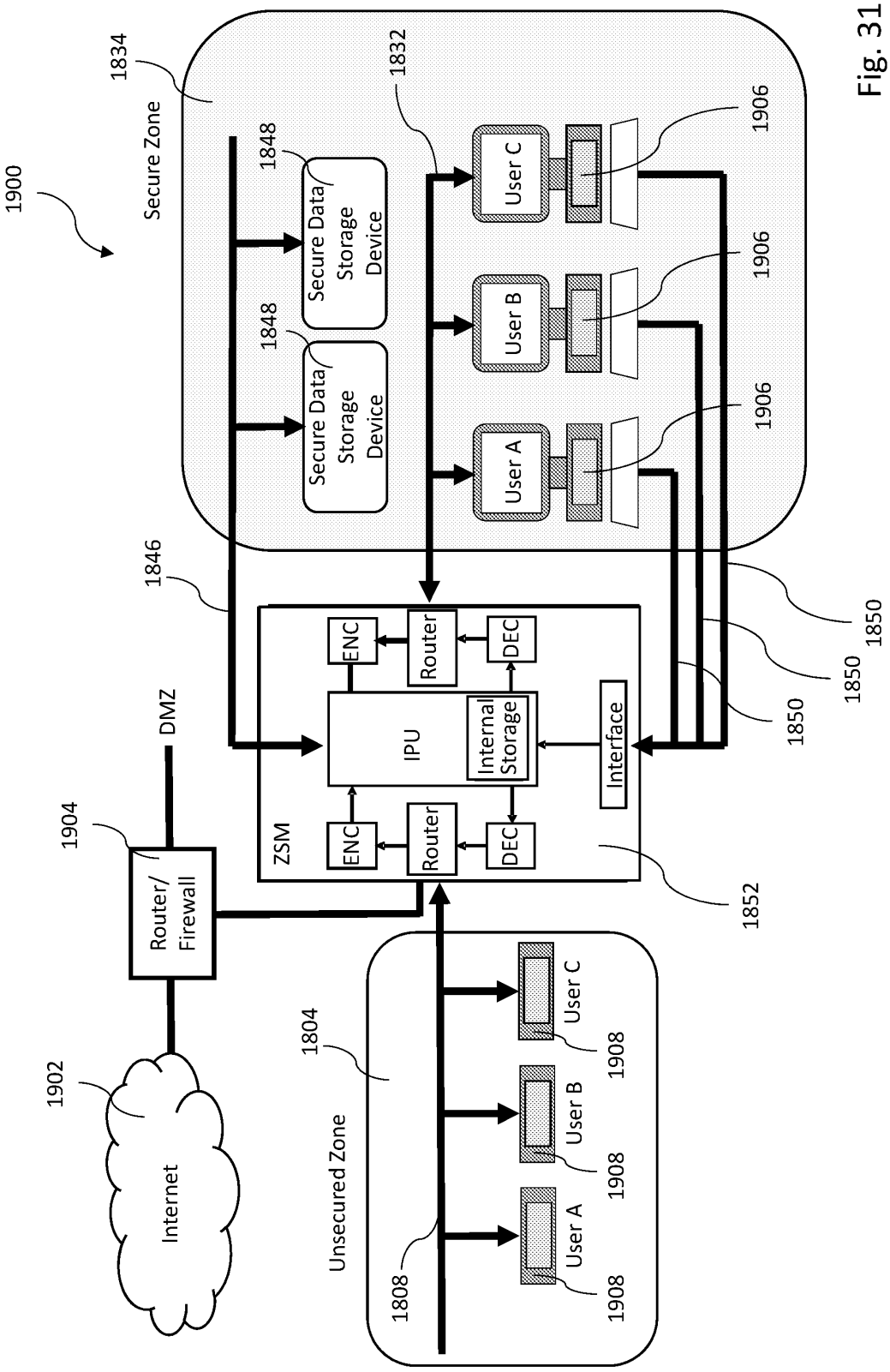

1900
1834
Secure Zone
1832
1848
Secure Data Storage Device
1848
Secure Data Storage Device
User C
User B
User A
1906
1906
1906
1846
1850
1850
1850
ENC
Router
DEC
IPU
Internal Storage
Interface
ZSM
ENC
Router
DEC
1852
DMZ
1904
Router/ Firewall
1902
Internet
1804
Unsecured Zone
User C
User B
User A
1908
1908
1908
1808

Fig. 31

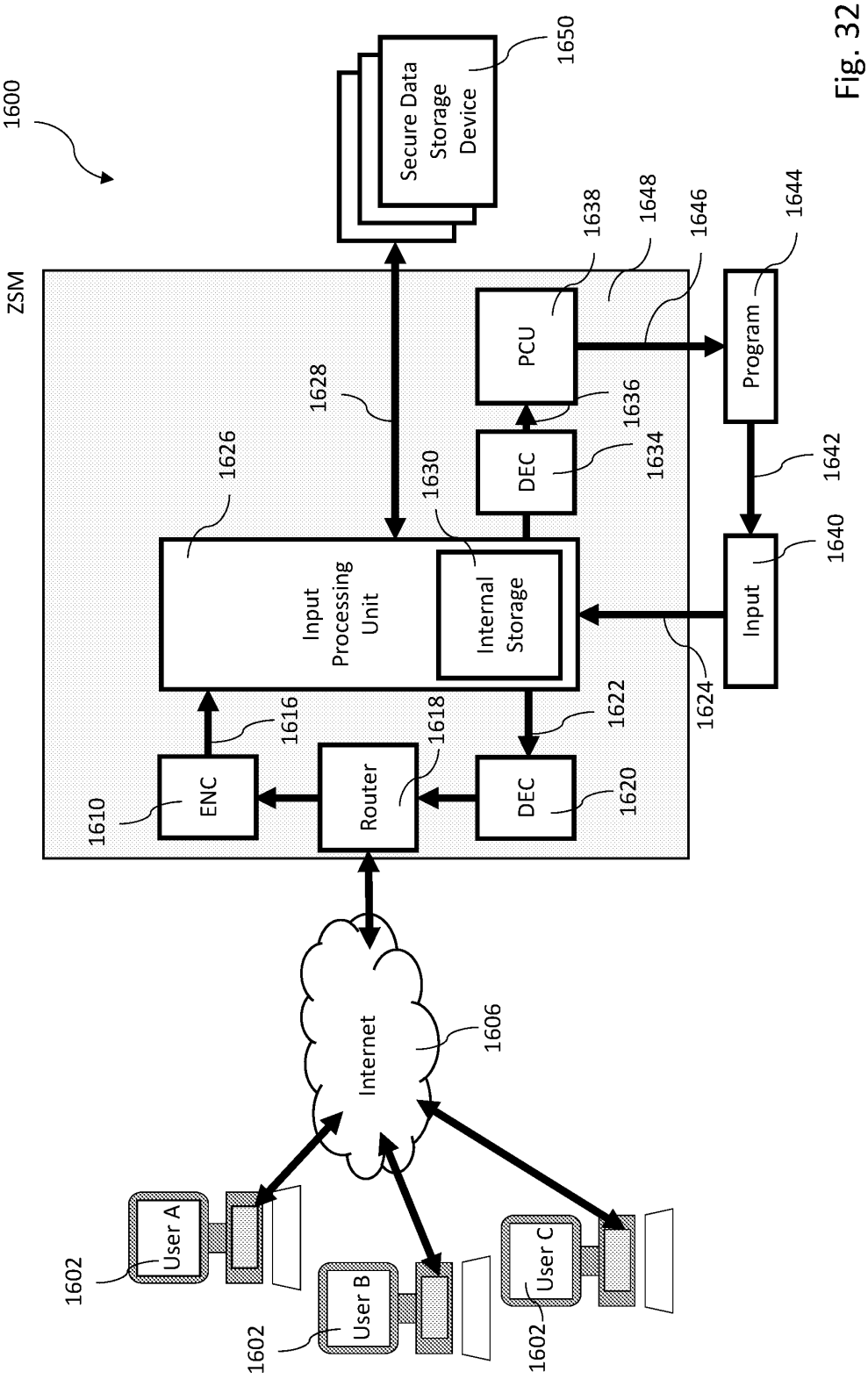

1600
Secure Data Storage Device
1650
ZSM
1638
1648
1646
1644
PCU
Program
1628
1636
1634
1642
1626
1630
DEC
Input Processing Unit
Internal Storage
Input
1640
1624
1622
1616
1618
1610
ENC
Router
DEC
1620
Internet
1606
User A
User B
User C
1602
1602
1602

Fig. 32

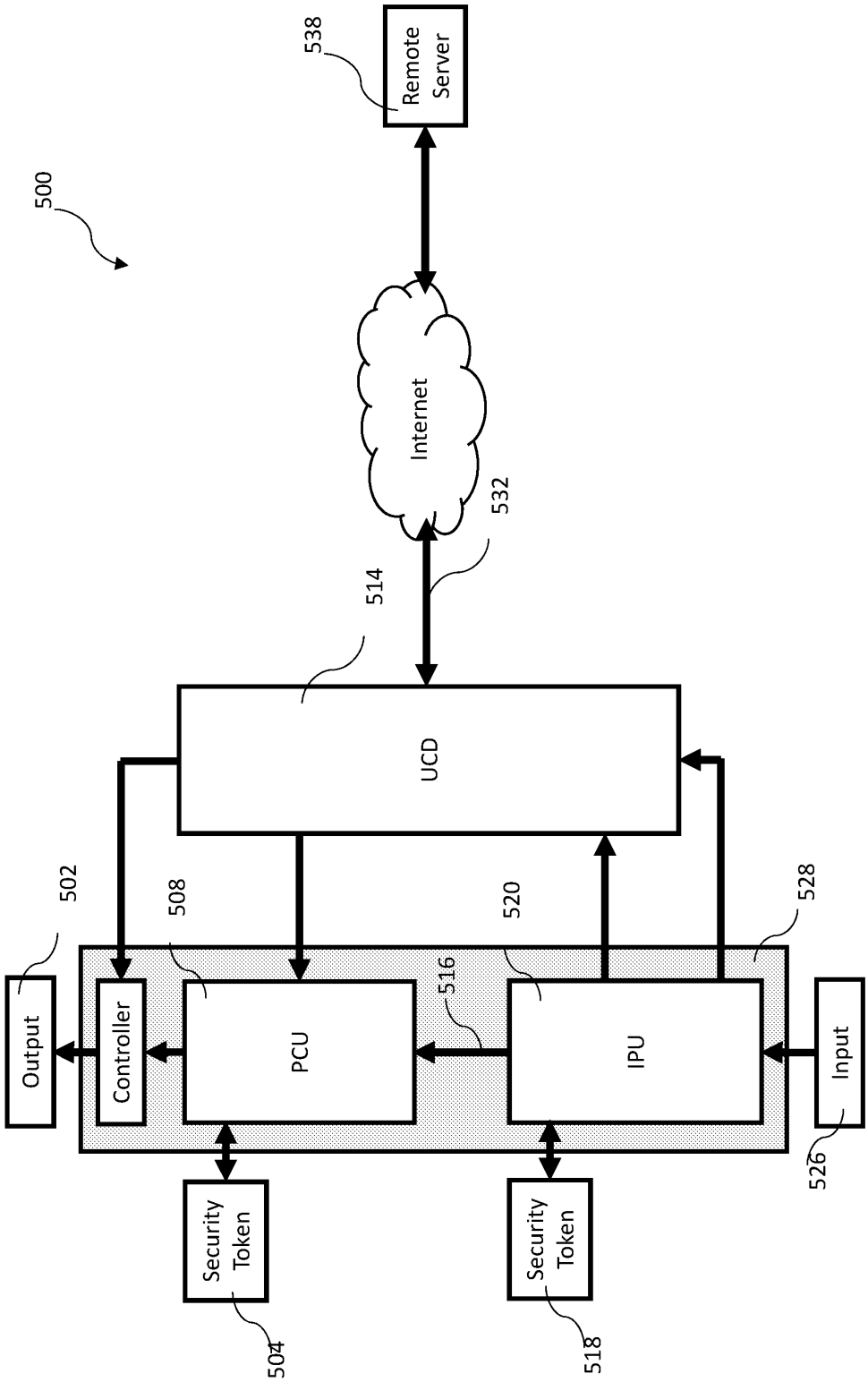

500
538
Remote Server
Internet
532
514
UCD
502
508
520
528
Output
Controller
PCU
516
IPU
Input
526
Security Token
504
Security Token
518

Fig. 33

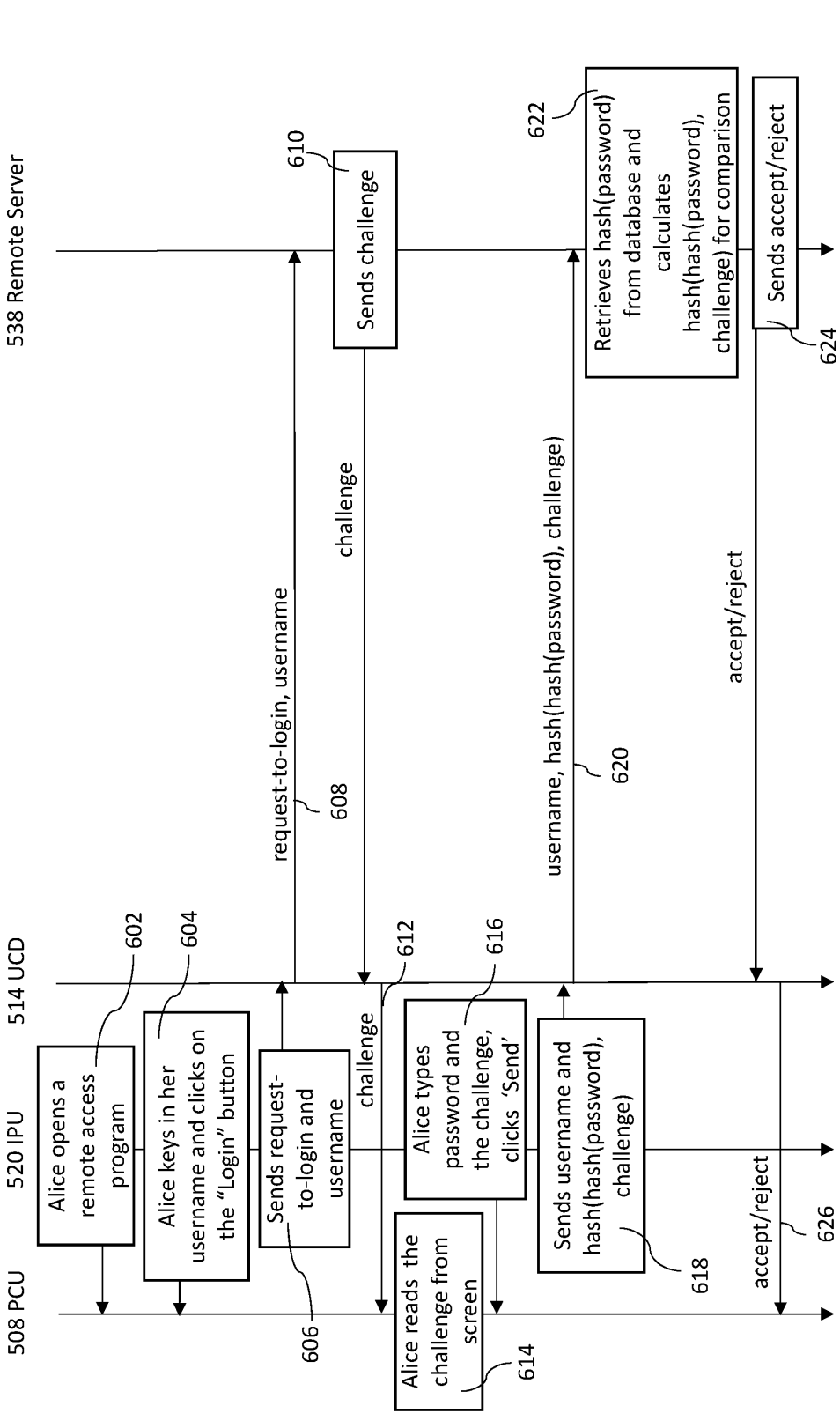

538 Remote Server
514 UCD
520 IPU
508 PCU
Alice opens a remote access program
602
Alice keys in her username and clicks on the "Login" button
604
Sends request-to-login and username
606
request-to-login, username
608
Sends challenge
610
challenge
612
Alice reads the challenge from screen
614
Alice types password and the challenge, clicks 'Send'
616
Sends username and hash(hash(password), challenge)
618
username, hash(hash(password), challenge)
620
Retrieves hash(password) from database and calculates hash(hash(password), challenge) for comparison
622
Sends accept/reject
624
accept/reject
626

Fig. 34

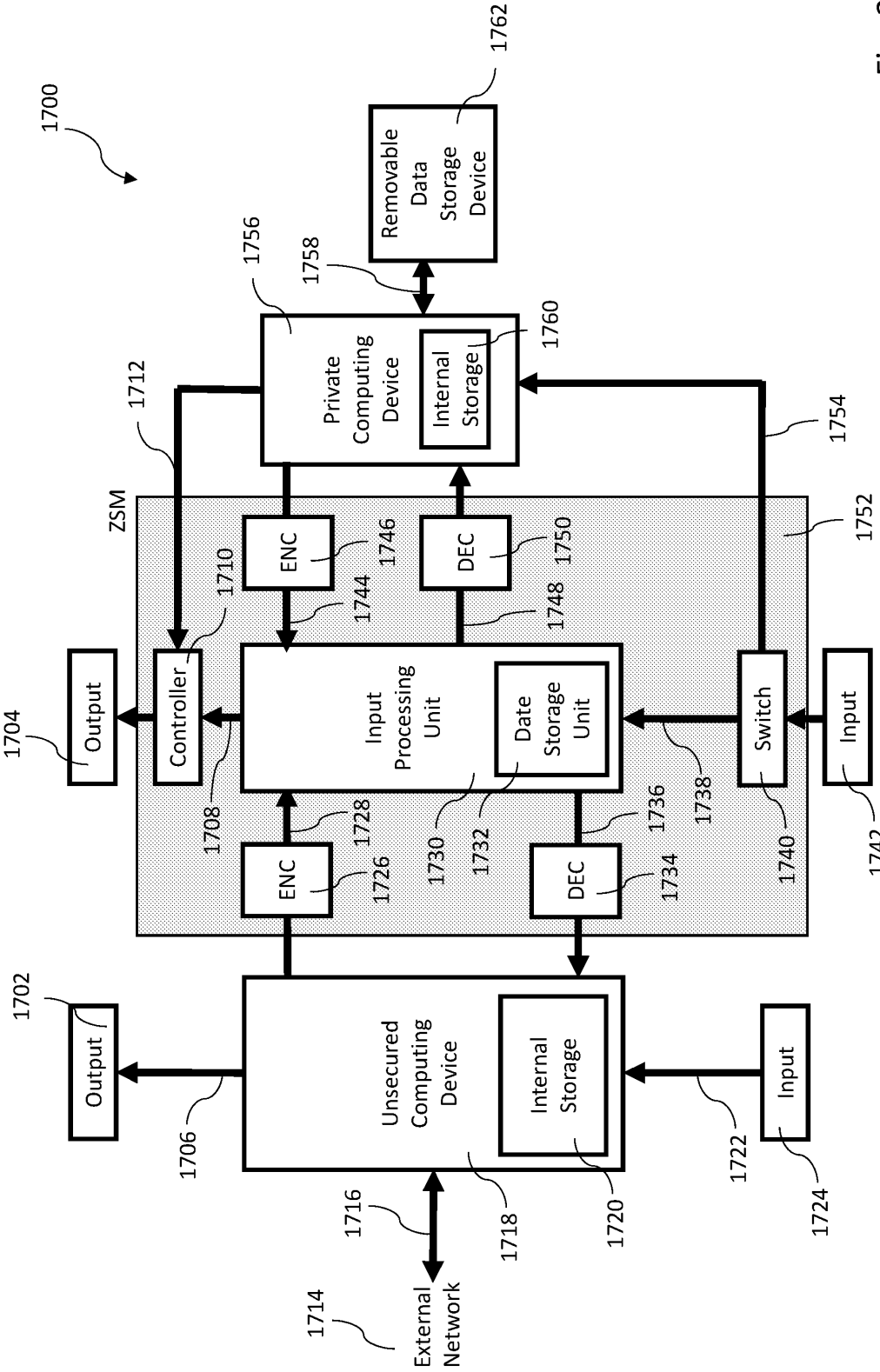

1700
Removable Data Storage Device
1762
1758
1756
Private Computing Device
Internal Storage
1760
1712
1754
ZSM
1752
ENC
1746
DEC
1750
1744
1748
1710
Output
Controller
Input Processing Unit
Date Storage Unit
Switch
Input
1704
1708
1728
1730
1732
1736
1738
1740
1742
ENC
1726
DEC
1734
1702
Output
Unsecured Computing Device
Internal Storage
Input
1706
1722
1724
1716
1718
1720
1714
External Network

Fig. 35