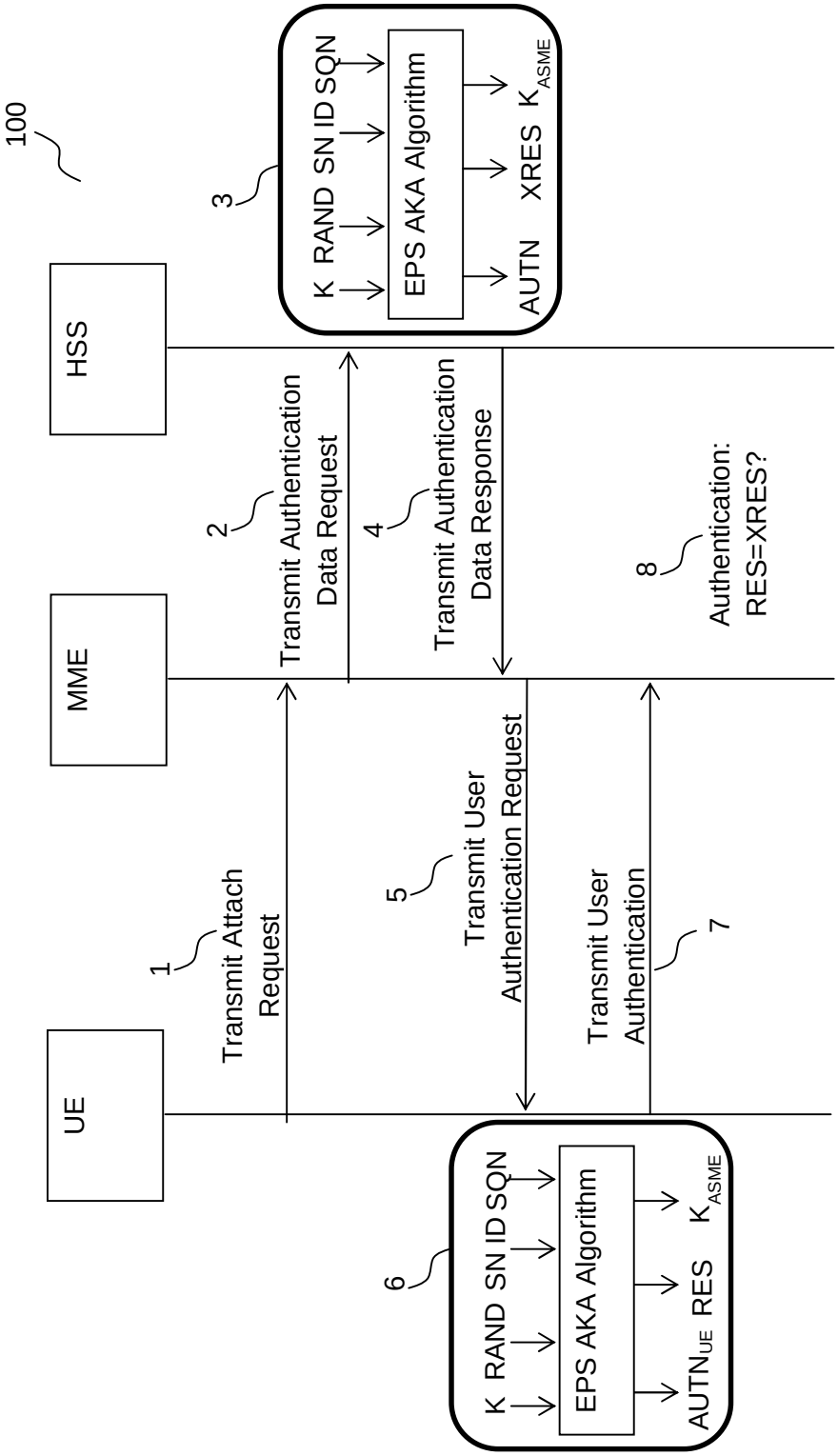
100
UE
MME
HSS
1
Transmit Attach Request
2
Transmit Authentication Data Request
3
K RAND SN ID SQN
EPS AKA Algorithm
AUTN XRES K_{ASME}
4
Transmit Authentication Data Response
5
Transmit User Authentication Request
6
K RAND SN ID SQN
EPS AKA Algorithm
$AUTN_{UE}$ RES K_{ASME}
7
Transmit User Authentication
8
Authentication: RES=XRES?

Figure 1

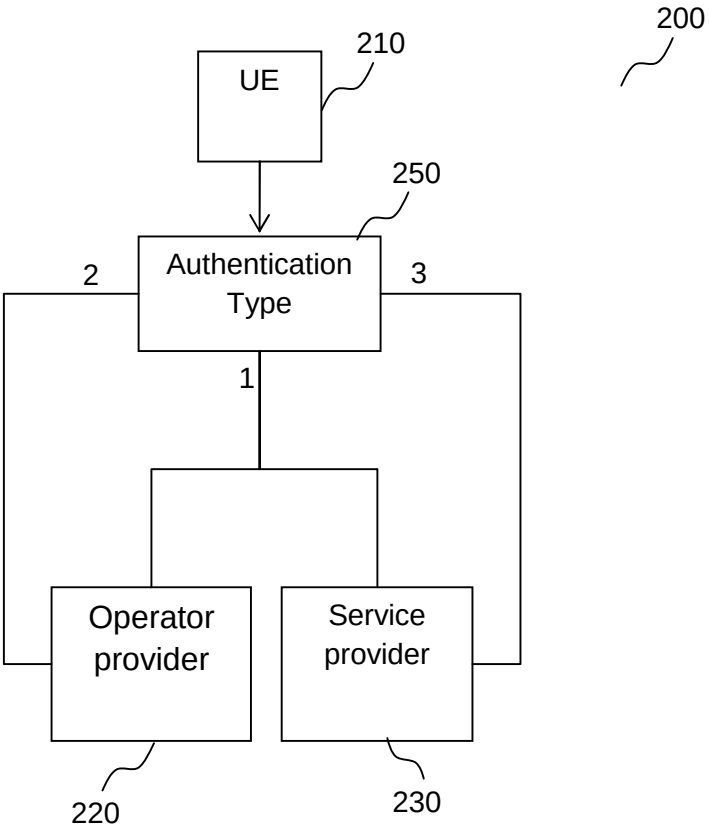
200
210
UE
250
Authentication Type
2
3
1
Operator provider
Service provider
220
230

Figure 2

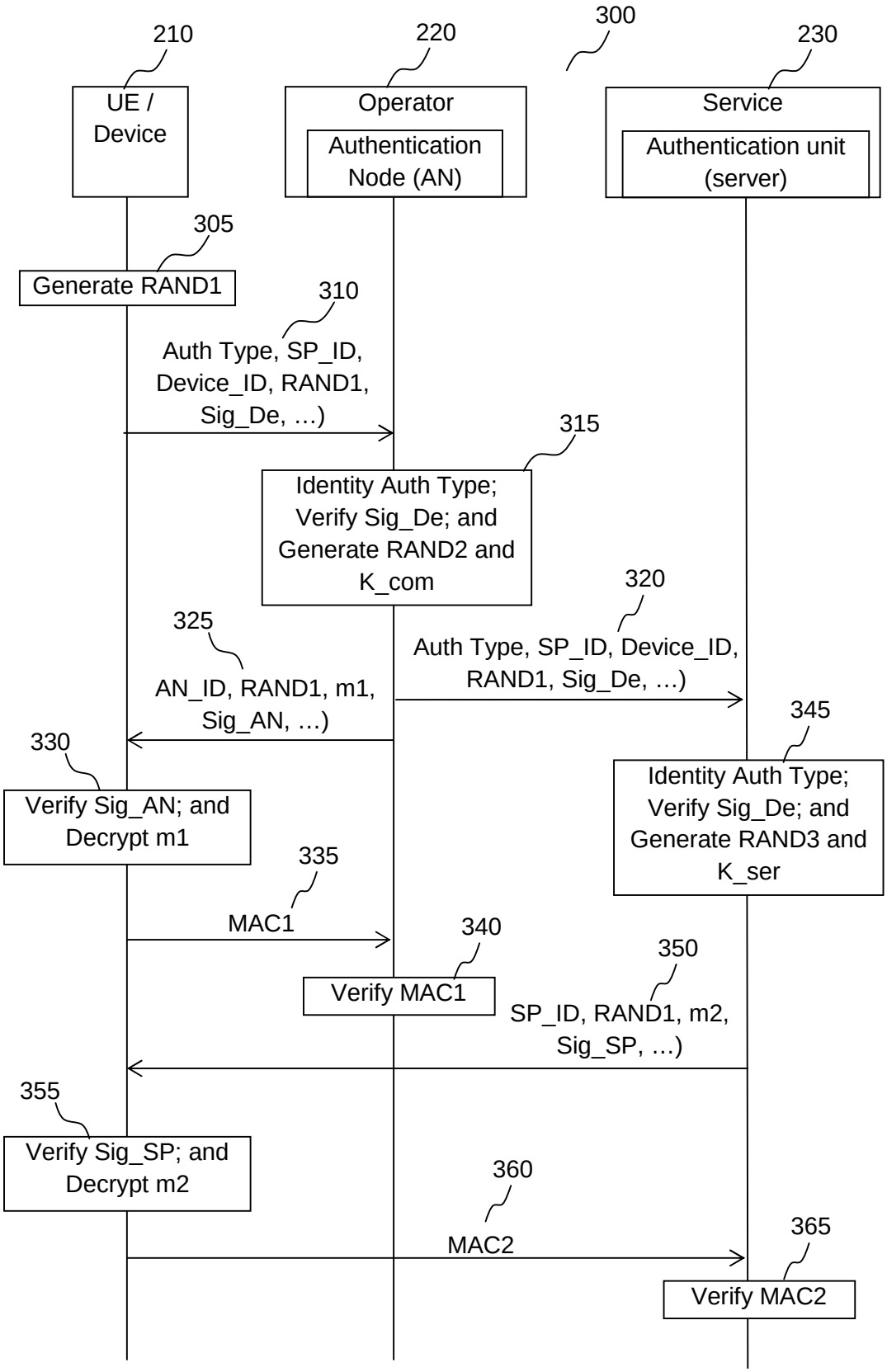
210
220
300
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
305
Generate RAND1
310
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
315
Identity Auth Type; Verify Sig_De; and Generate RAND2 and K_com
320
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
325
AN_ID, RAND1, m1, Sig_AN, …)
345
330
Verify Sig_AN; and Decrypt m1
Identity Auth Type; Verify Sig_De; and Generate RAND3 and K_ser
335
MAC1
340
Verify MAC1
350
SP_ID, RAND1, m2, Sig_SP, …)
355
Verify Sig_SP; and Decrypt m2
360
MAC2
365
Verify MAC2

Figure 3

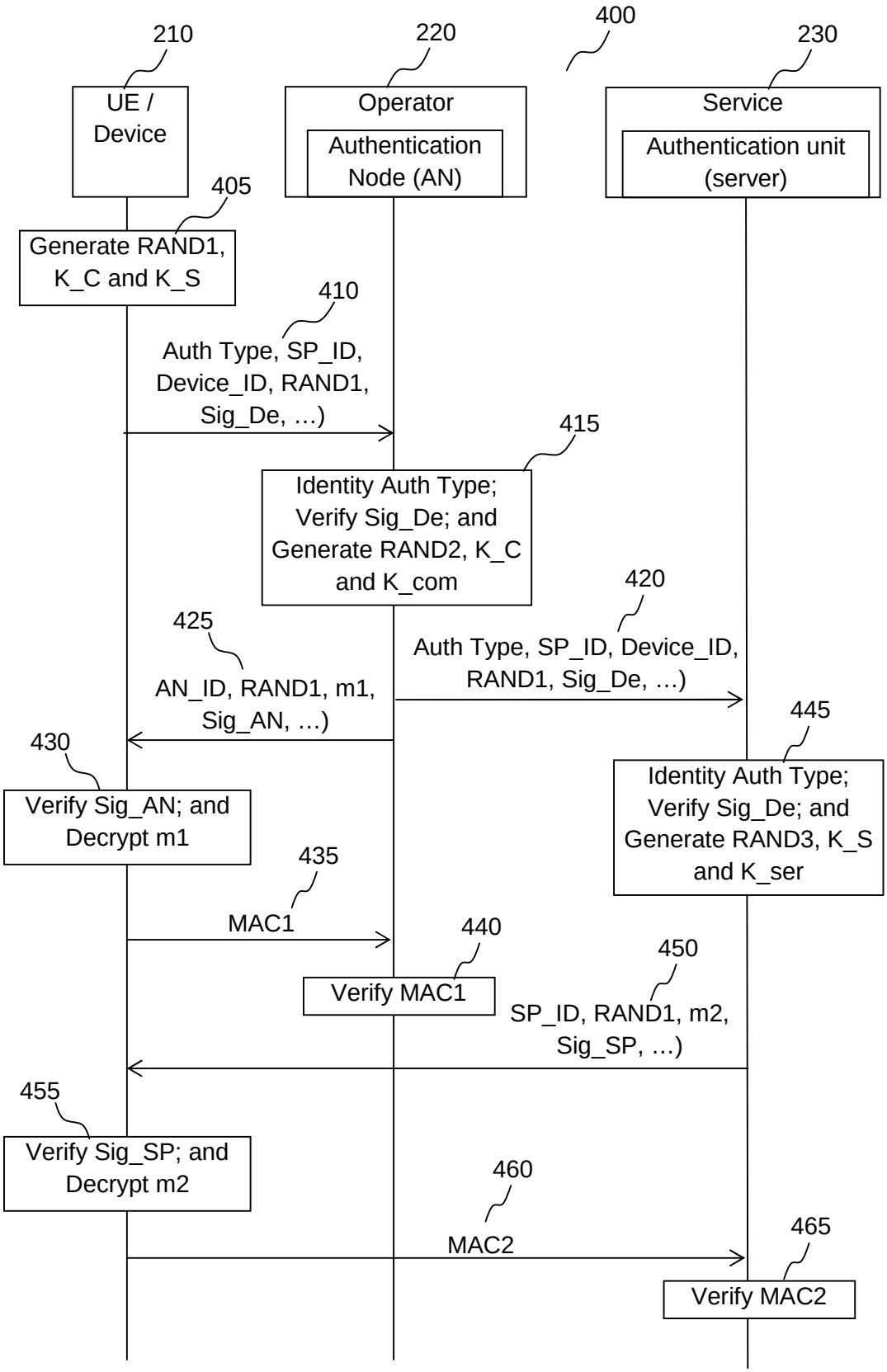
400
210
220
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
405
Generate RAND1, K_C and K_S
410
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
415
Identity Auth Type; Verify Sig_De; and Generate RAND2, K_C and K_com
420
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
425
AN_ID, RAND1, m1, Sig_AN, …)
430
Verify Sig_AN; and Decrypt m1
445
Identity Auth Type; Verify Sig_De; and Generate RAND3, K_S and K_ser
435
MAC1
440
Verify MAC1
450
SP_ID, RAND1, m2, Sig_SP, …)
455
Verify Sig_SP; and Decrypt m2
460
MAC2
465
Verify MAC2

Figure 4

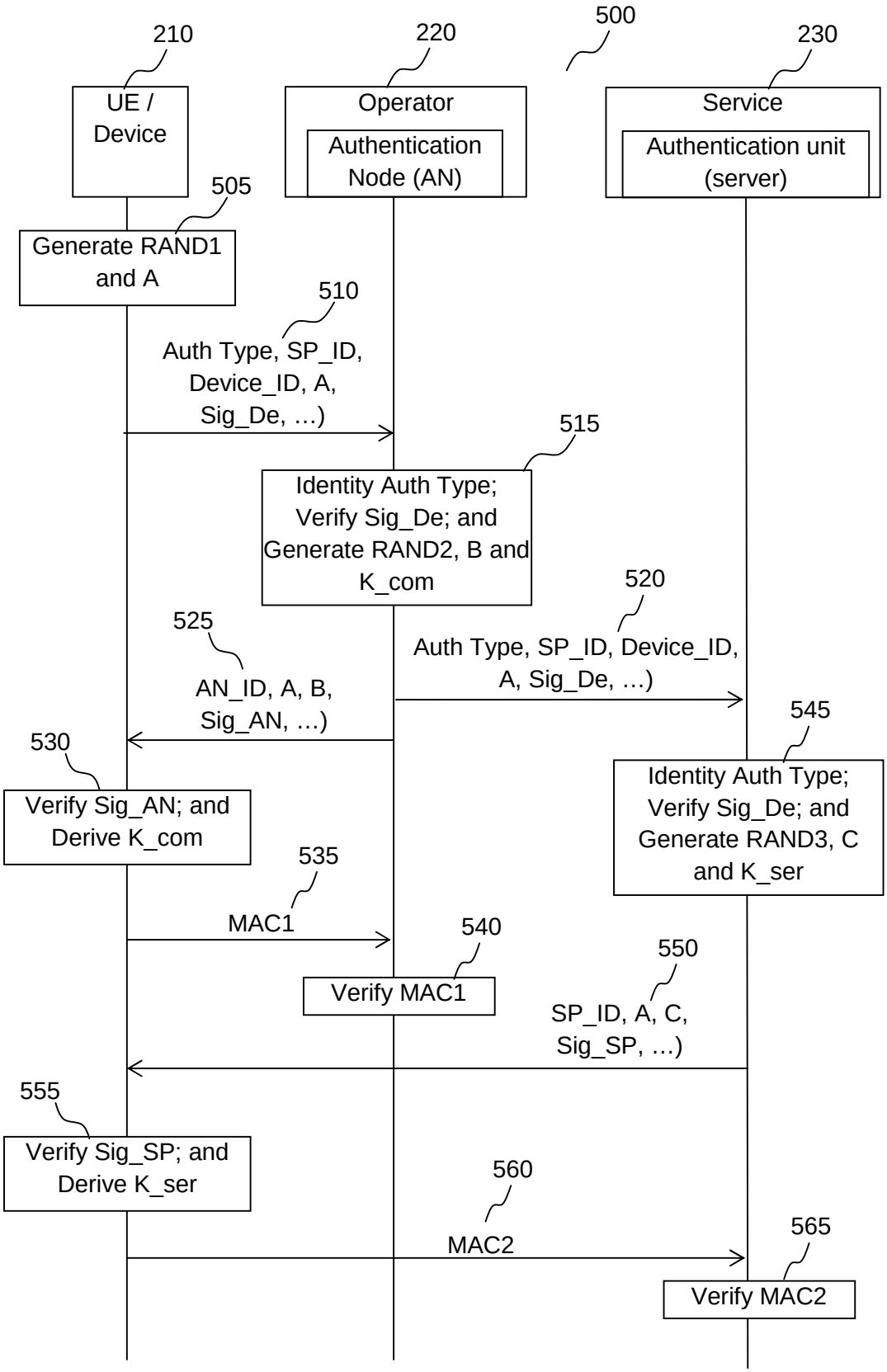
500
210
220
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
505
Generate RAND1 and A
510
Auth Type, SP_ID, Device_ID, A, Sig_De, …)
515
Identity Auth Type; Verify Sig_De; and Generate RAND2, B and K_com
520
Auth Type, SP_ID, Device_ID, A, Sig_De, …)
525
AN_ID, A, B, Sig_AN, …)
530
Verify Sig_AN; and Derive K_com
545
Identity Auth Type; Verify Sig_De; and Generate RAND3, C and K_ser
535
MAC1
540
Verify MAC1
550
SP_ID, A, C, Sig_SP, …)
555
Verify Sig_SP; and Derive K_ser
560
MAC2
565
Verify MAC2

Figure 5

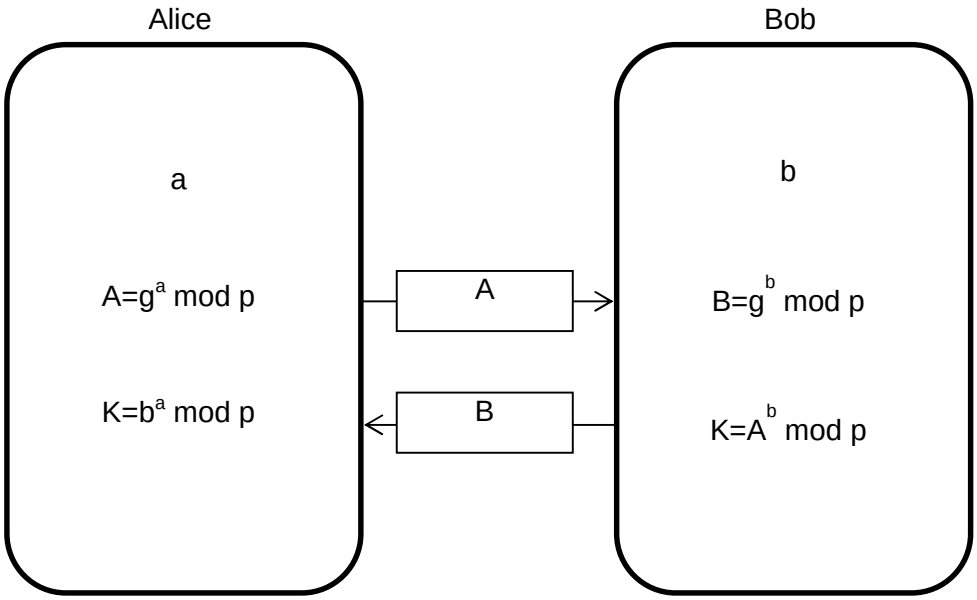

Figure 6

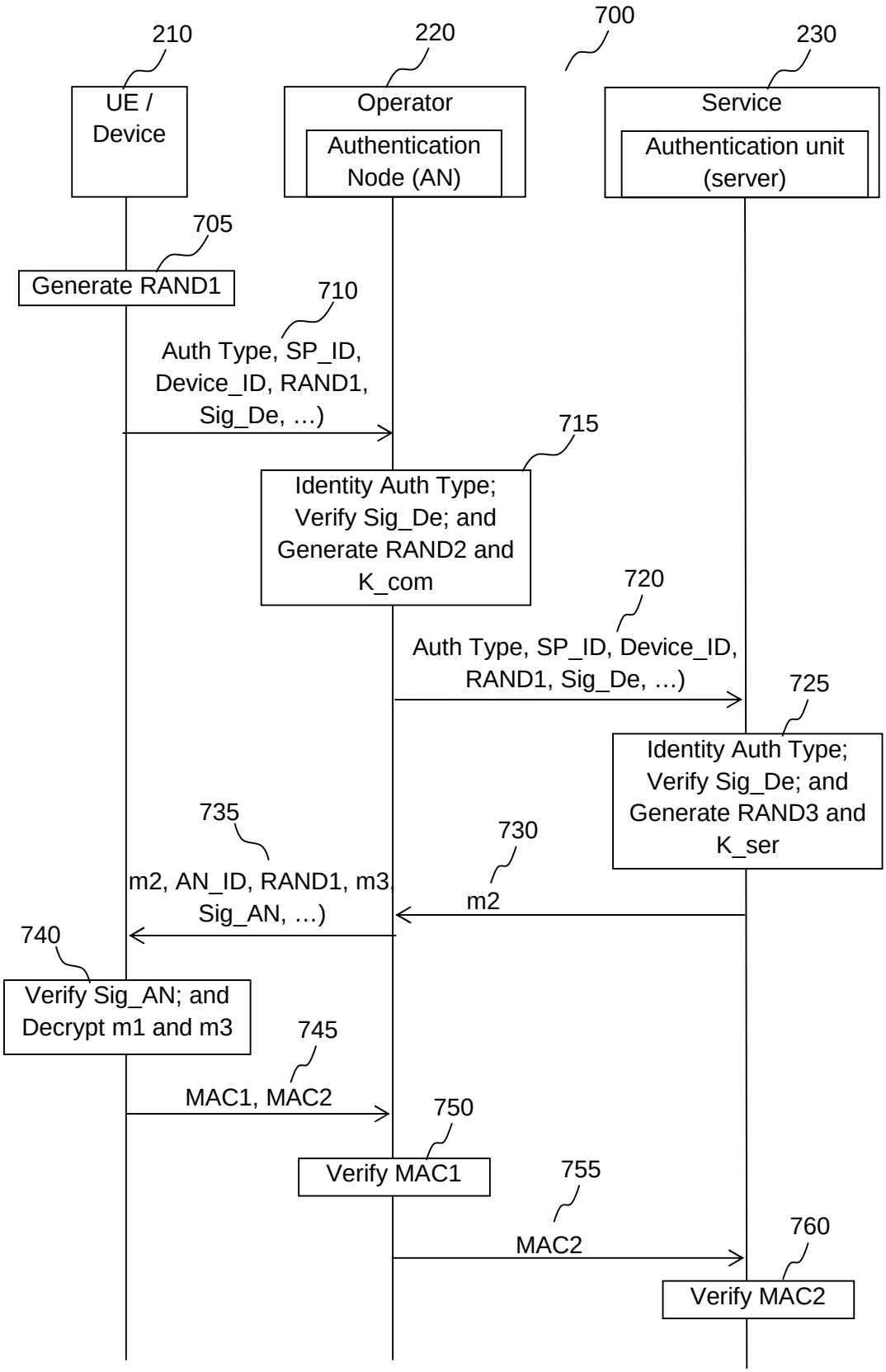
700
210
220
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
705
Generate RAND1
710
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
715
Identity Auth Type; Verify Sig_De; and Generate RAND2 and K_com
720
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
725
Identity Auth Type; Verify Sig_De; and Generate RAND3 and K_ser
735
m2, AN_ID, RAND1, m3, Sig_AN, …)
730
m2
740
Verify Sig_AN; and Decrypt m1 and m3
745
MAC1, MAC2
750
Verify MAC1
755
MAC2
760
Verify MAC2

Figure 7

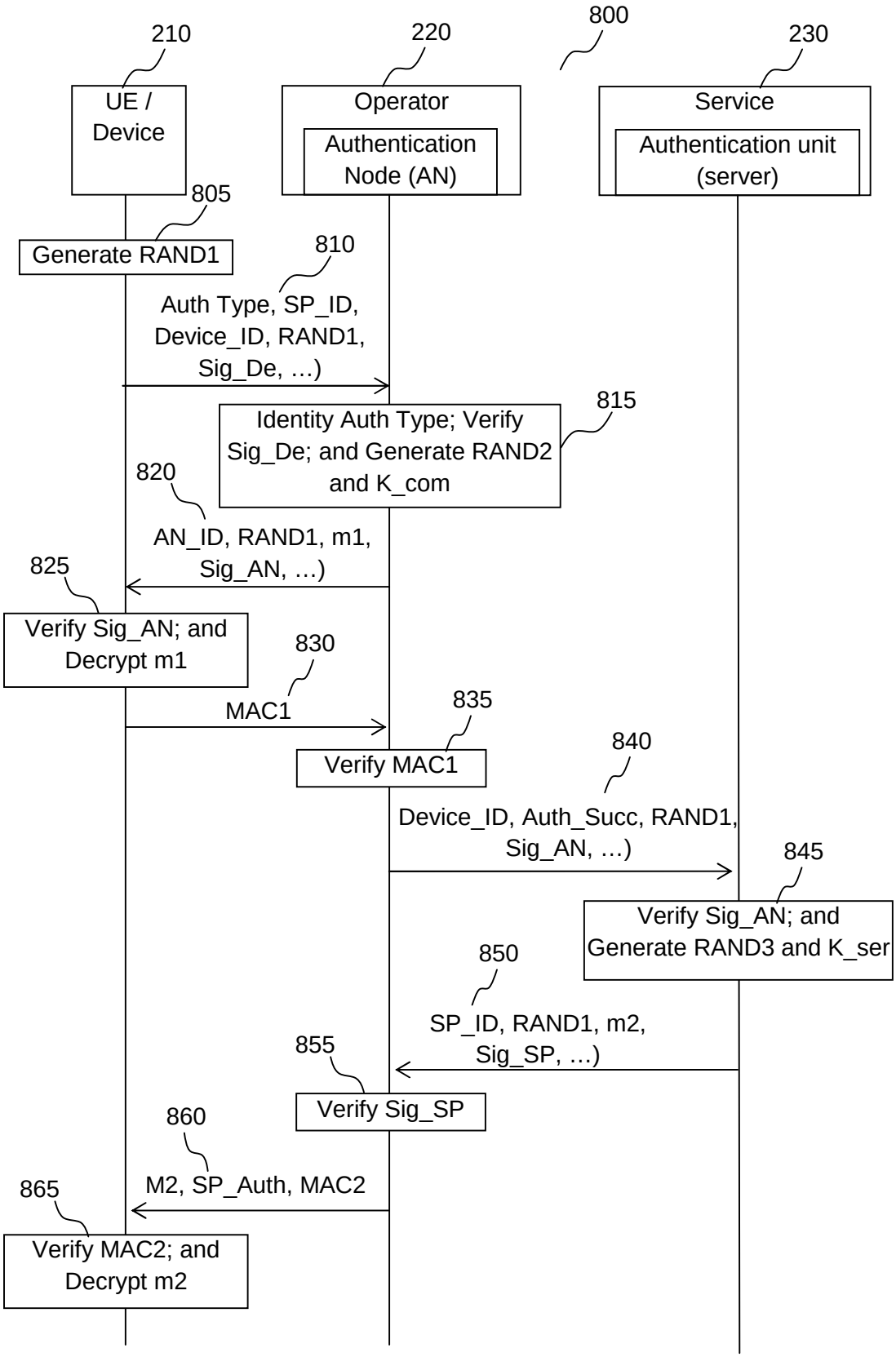
800
210
220
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
805
Generate RAND1
810
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
815
Identity Auth Type; Verify Sig_De; and Generate RAND2 and K_com
820
AN_ID, RAND1, m1, Sig_AN, …)
825
Verify Sig_AN; and Decrypt m1
830
MAC1
835
Verify MAC1
840
Device_ID, Auth_Succ, RAND1, Sig_AN, …)
845
Verify Sig_AN; and Generate RAND3 and K_ser
850
SP_ID, RAND1, m2, Sig_SP, …)
855
Verify Sig_SP
860
M2, SP_Auth, MAC2
865
Verify MAC2; and Decrypt m2

Figure 8

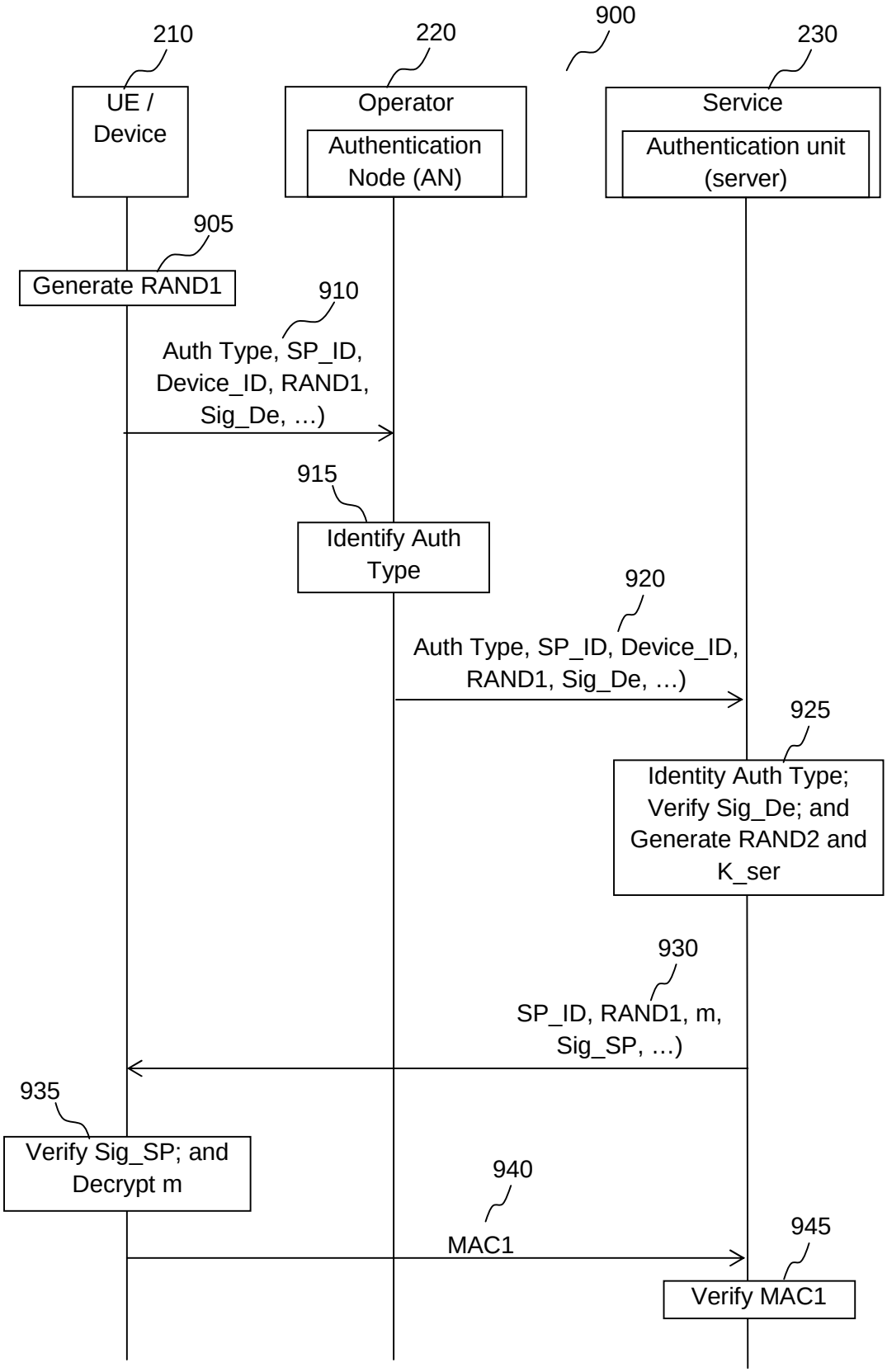
210
220
900
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
905
Generate RAND1
910
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
915
Identify Auth Type
920
Auth Type, SP_ID, Device_ID, RAND1, Sig_De, …)
925
Identity Auth Type; Verify Sig_De; and Generate RAND2 and K_ser
930
SP_ID, RAND1, m, Sig_SP, …)
935
Verify Sig_SP; and Decrypt m
940
MAC1
945
Verify MAC1

Figure 9

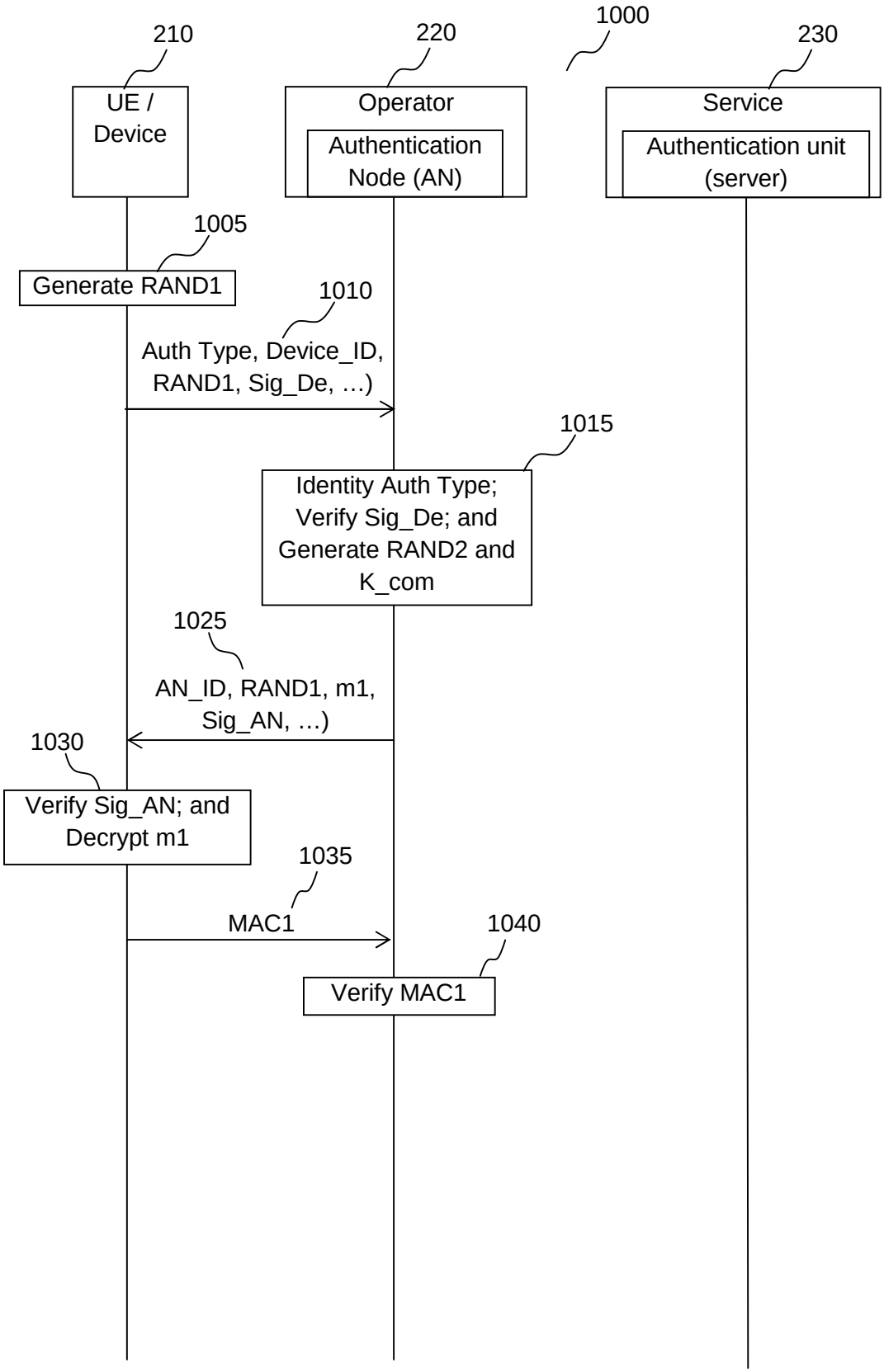
210
220
1000
230
UE / Device
Operator
Authentication Node (AN)
Service
Authentication unit (server)
1005
Generate RAND1
1010
Auth Type, Device_ID, RAND1, Sig_De, …)
1015
Identity Auth Type; Verify Sig_De; and Generate RAND2 and K_com
1025
AN_ID, RAND1, m1, Sig_AN, …)
1030
Verify Sig_AN; and Decrypt m1
1035
MAC1
1040
Verify MAC1

Figure 10

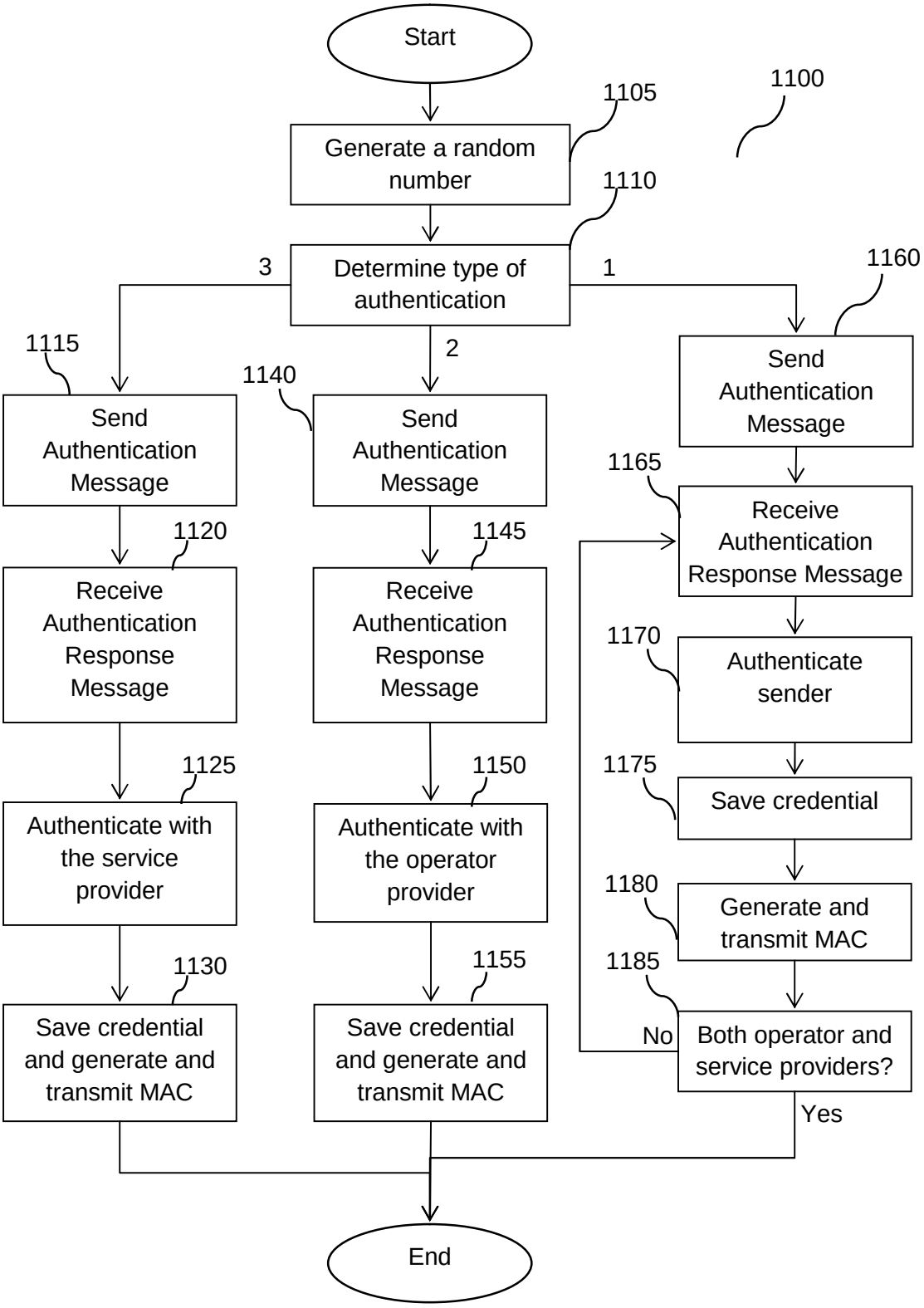
Start
1100
1105
Generate a random number
1110
Determine type of authentication
3
2
1
1160
1115
1140
Send Authentication Message
Send Authentication Message
Send Authentication Message
1165
1120
1145
Receive Authentication Response Message
Receive Authentication Response Message
Receive Authentication Response Message
1170
Authenticate sender
1125
1150
1175
Authenticate with the service provider
Authenticate with the operator provider
Save credential
1180
Generate and transmit MAC
1130
1155
1185
Save credential and generate and transmit MAC
Save credential and generate and transmit MAC
No
Both operator and service providers?
Yes
End

Figure 11

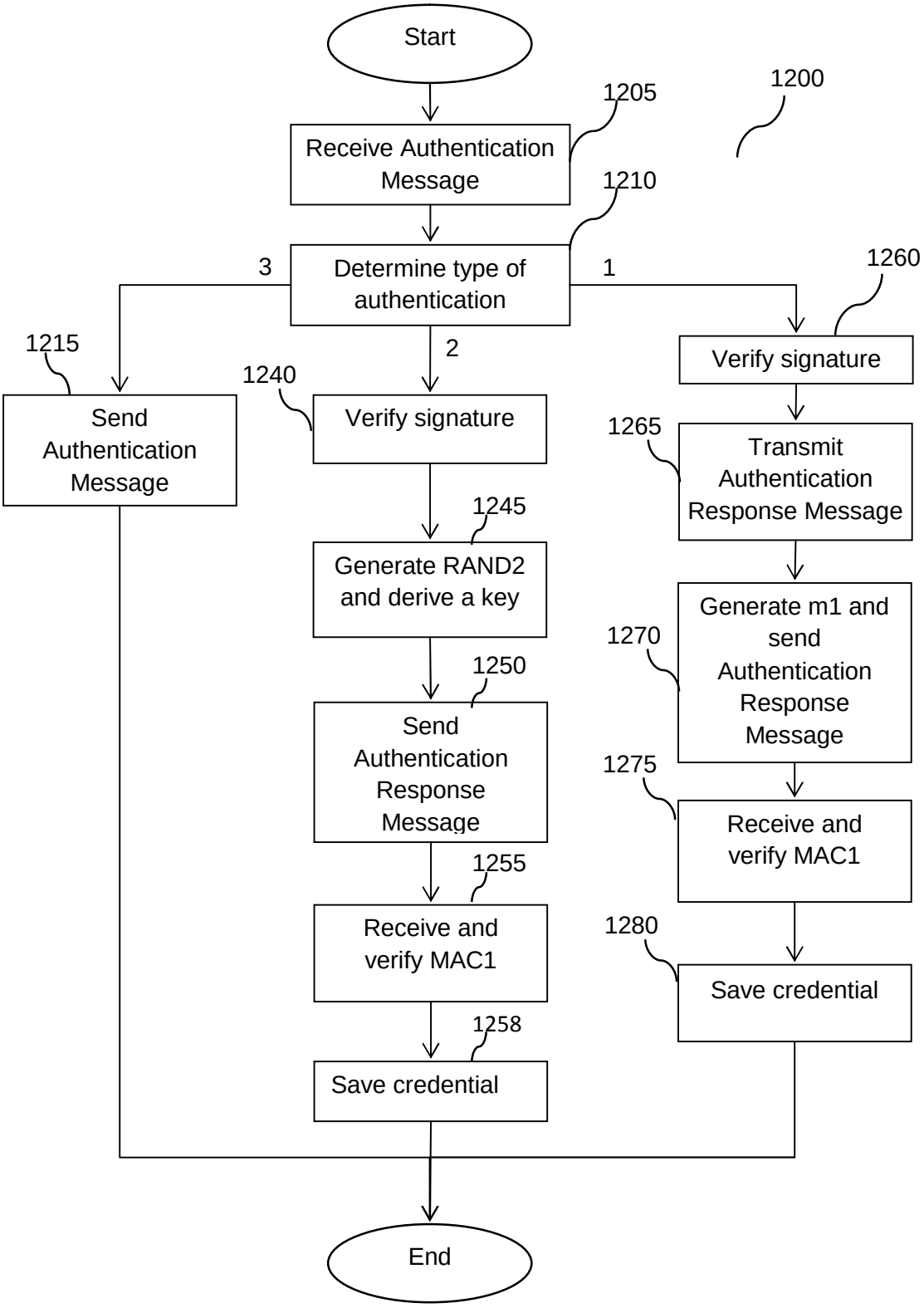
Start
1200
1205
Receive Authentication Message
1210
Determine type of authentication
3
1
2
1260
Verify signature
1215
Send Authentication Message
1240
Verify signature
1265
Transmit Authentication Response Message
1245
Generate RAND2 and derive a key
1270
Generate m1 and send Authentication Response Message
1250
Send Authentication Response Message
1275
Receive and verify MAC1
1255
Receive and verify MAC1
1280
Save credential
1258
Save credential
End

Figure 12

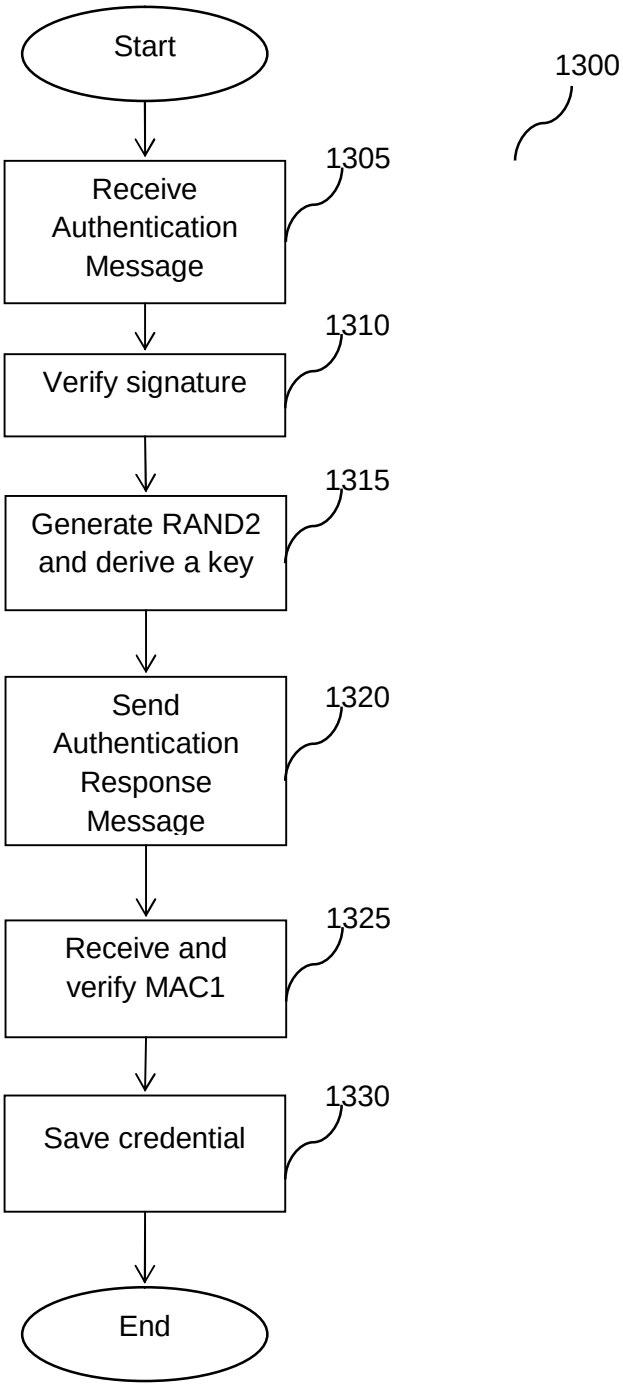
Start
1300
Receive Authentication Message
1305
Verify signature
1310
Generate RAND2 and derive a key
1315
Send Authentication Response Message
1320
Receive and verify MAC1
1325
Save credential
1330
End

Figure 13