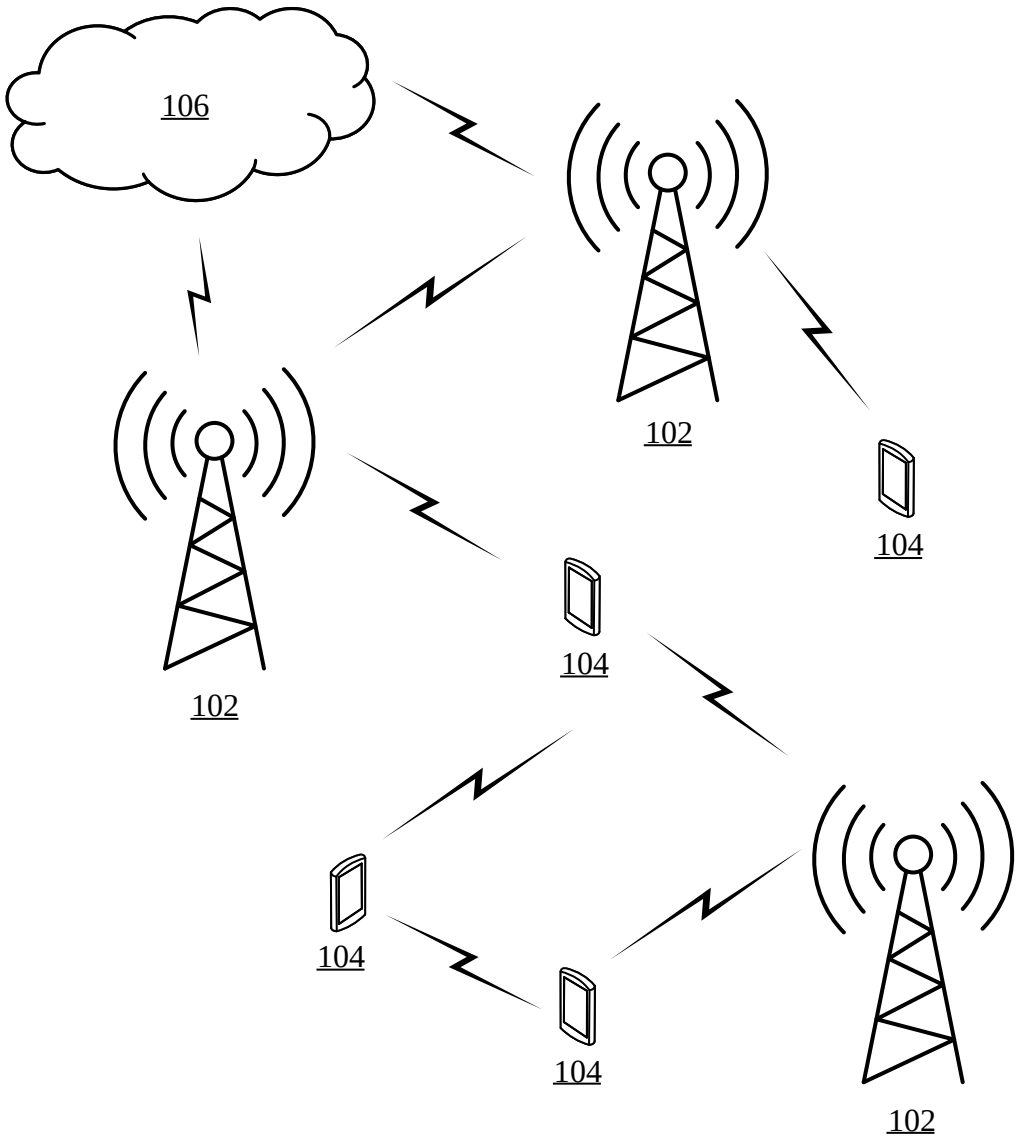



Figure 1

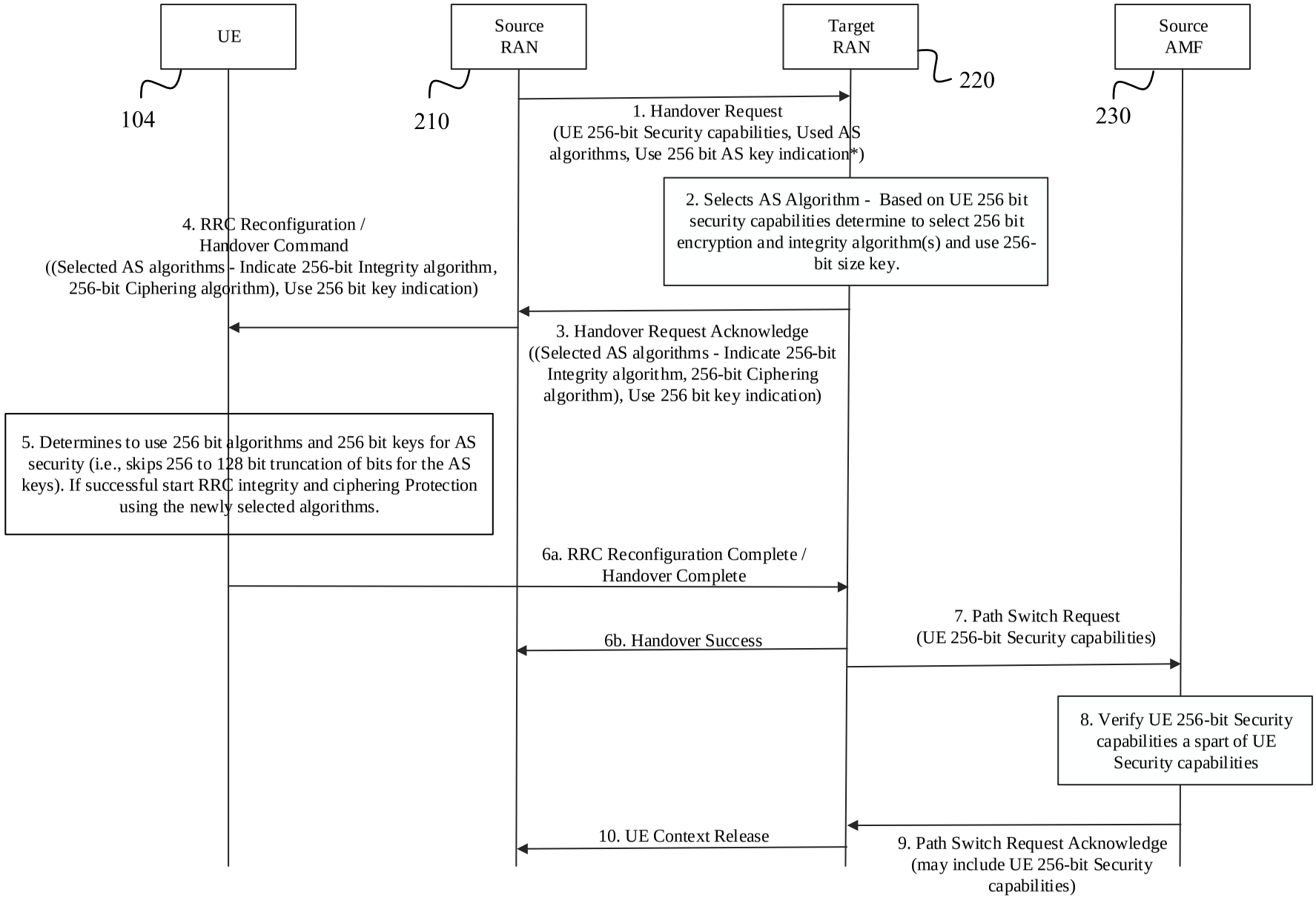

UE
Source RAN
Target RAN
Source AMF
104
210
220
230
1. Handover Request
(UE 256-bit Security capabilities, Used AS algorithms, Use 256 bit AS key indication*)
2. Selects AS Algorithm - Based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size key.
4. RRC Reconfiguration / Handover Command
((Selected AS algorithms - Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm), Use 256 bit key indication)
3. Handover Request Acknowledge
((Selected AS algorithms - Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm), Use 256 bit key indication)
5. Determines to use 256 bit algorithms and 256 bit keys for AS security (i.e., skips 256 to 128 bit truncation of bits for the AS keys). If successful start RRC integrity and ciphering Protection using the newly selected algorithms.
6a. RRC Reconfiguration Complete / Handover Complete
6b. Handover Success
7. Path Switch Request
(UE 256-bit Security capabilities)
8. Verify UE 256-bit Security capabilities a spart of UE Security capabilities
9. Path Switch Request Acknowledge
(may include UE 256-bit Security capabilities)
10. UE Context Release

Figure 2

200

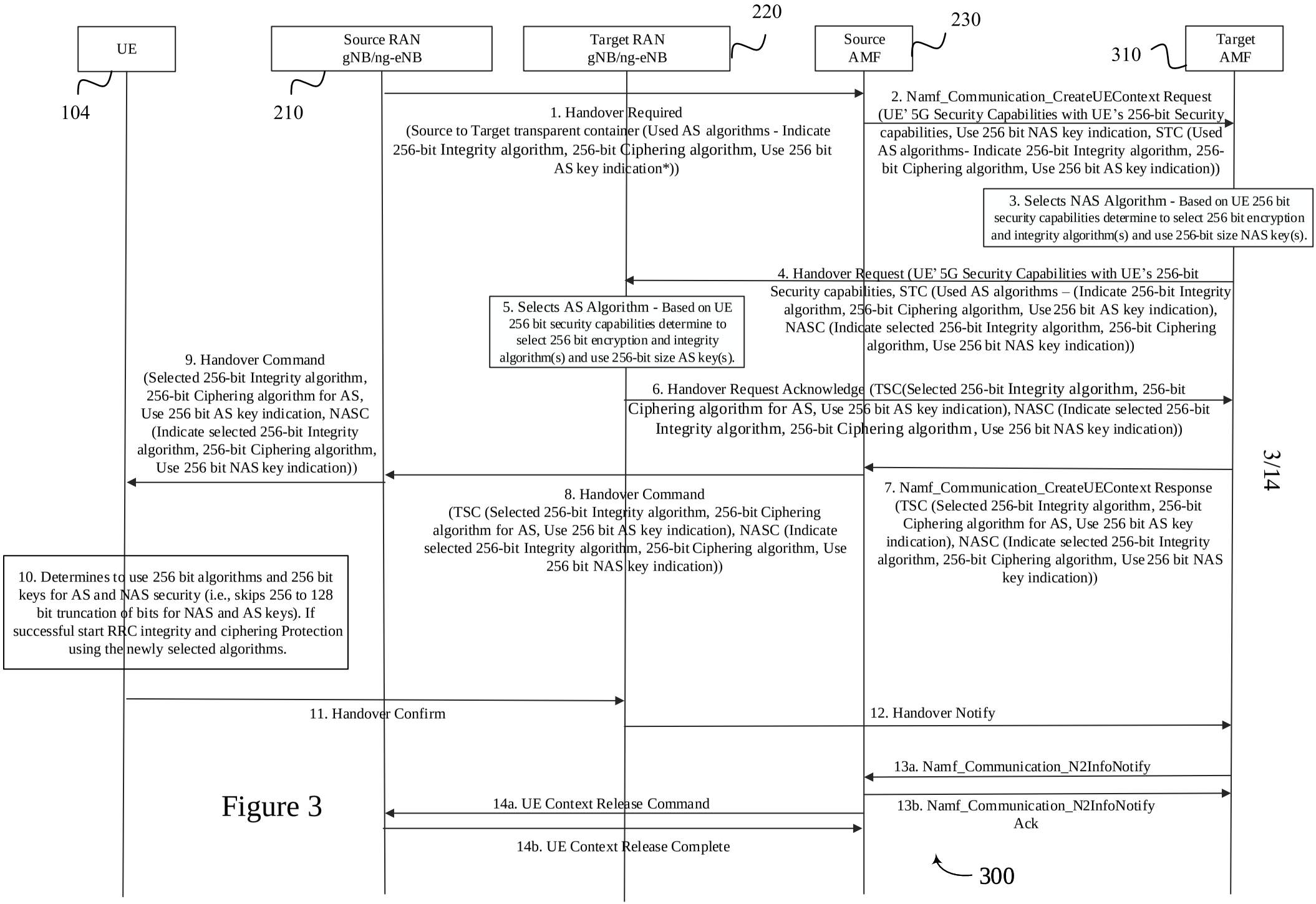

UE
104
Source RAN
gNB/ng-eNB
210
Target RAN
gNB/ng-eNB
220
Source
AMF
230
Target
AMF
310
1. Handover Required
(Source to Target transparent container (Used AS algorithms - Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication*))
2. Namf_Communication_CreateUEContext Request (UE' 5G Security Capabilities with UE's 256-bit Security capabilities, Use 256 bit NAS key indication, STC (Used AS algorithms- Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication))
3. Selects NAS Algorithm - Based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size NAS key(s).
4. Handover Request (UE' 5G Security Capabilities with UE's 256-bit Security capabilities, STC (Used AS algorithms – (Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication), NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit NAS key indication))
5. Selects AS Algorithm - Based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size AS key(s).
6. Handover Request Acknowledge (TSC(Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication), NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit NAS key indication))
7. Namf_Communication_CreateUEContext Response (TSC (Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication), NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit NAS key indication))
8. Handover Command
(TSC (Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication), NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit NAS key indication))
9. Handover Command
(Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication, NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit NAS key indication))
10. Determines to use 256 bit algorithms and 256 bit keys for AS and NAS security (i.e., skips 256 to 128 bit truncation of bits for NAS and AS keys). If successful start RRC integrity and ciphering Protection using the newly selected algorithms.
11. Handover Confirm
12. Handover Notify
13a. Namf_Communication_N2InfoNotify
13b. Namf_Communication_N2InfoNotify Ack
14a. UE Context Release Command
14b. UE Context Release Complete
300

Figure 3

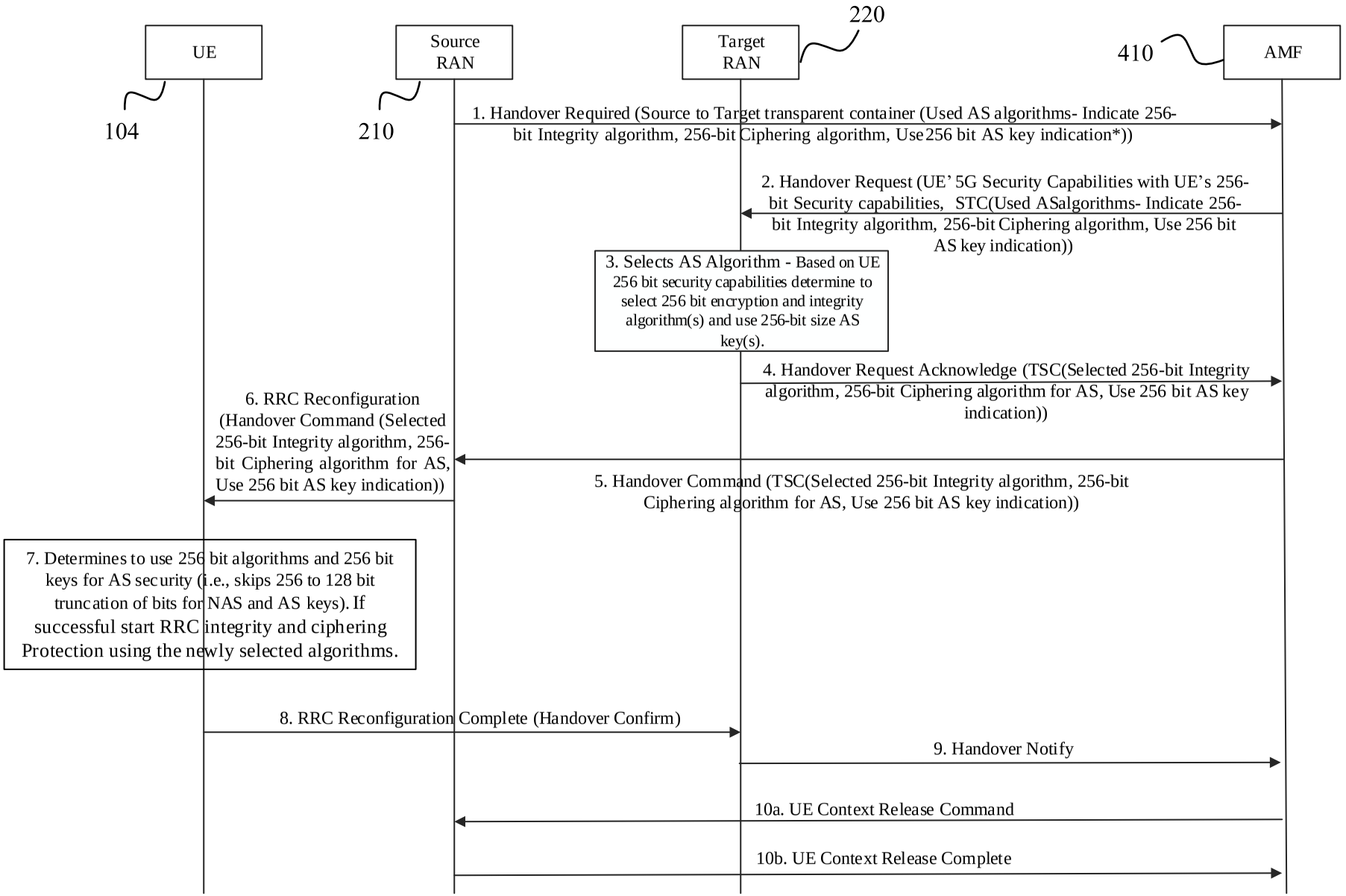

UE
104
Source RAN
210
Target RAN
220
AMF
410
1. Handover Required (Source to Target transparent container (Used AS algorithms- Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use256 bit AS key indication*))
2. Handover Request (UE' 5G Security Capabilities with UE's 256-bit Security capabilities, STC(Used ASalgorithms- Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication))
3. Selects AS Algorithm - Based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size AS key(s).
4. Handover Request Acknowledge (TSC(Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication))
5. Handover Command (TSC(Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication))
6. RRC Reconfiguration (Handover Command (Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, Use 256 bit AS key indication))
7. Determines to use 256 bit algorithms and 256 bit keys for AS security (i.e., skips 256 to 128 bit truncation of bits for NAS and AS keys). If successful start RRC integrity and ciphering Protection using the newly selected algorithms.
8. RRC Reconfiguration Complete (Handover Confirm)
9. Handover Notify
10a. UE Context Release Command
10b. UE Context Release Complete

Figure 4

400

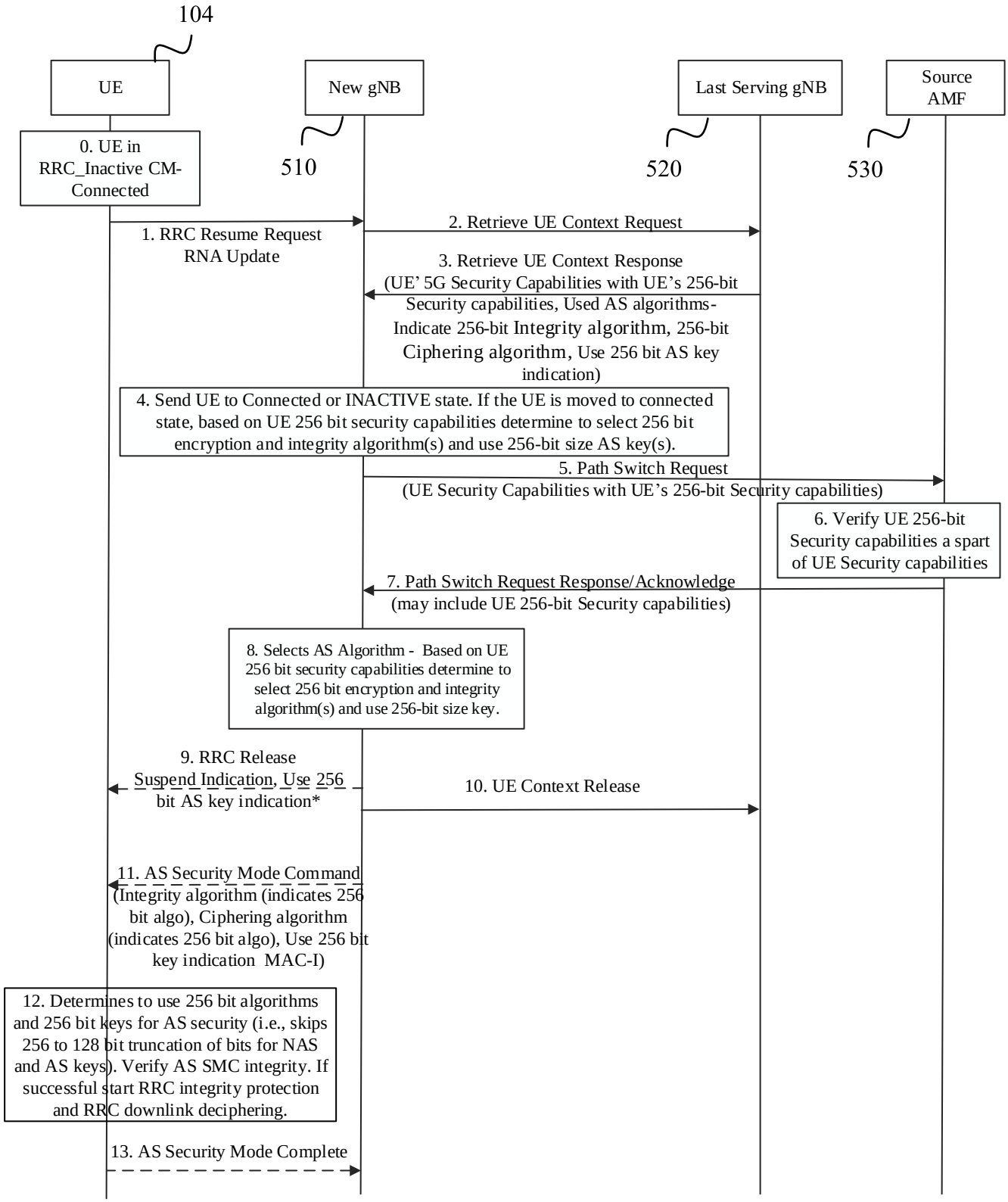

104
UE
New gNB
Last Serving gNB
Source AMF
0. UE in RRC_Inactive CM-Connected
510
520
530
1. RRC Resume Request RNA Update
2. Retrieve UE Context Request
3. Retrieve UE Context Response (UE' 5G Security Capabilities with UE's 256-bit Security capabilities, Used AS algorithms- Indicate 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication)
4. Send UE to Connected or INACTIVE state. If the UE is moved to connected state, based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size AS key(s).
5. Path Switch Request (UE Security Capabilities with UE's 256-bit Security capabilities)
6. Verify UE 256-bit Security capabilities a spart of UE Security capabilities
7. Path Switch Request Response/Acknowledge (may include UE 256-bit Security capabilities)
8. Selects AS Algorithm - Based on UE 256 bit security capabilities determine to select 256 bit encryption and integrity algorithm(s) and use 256-bit size key.
9. RRC Release Suspend Indication, Use 256 bit AS key indication*
10. UE Context Release
11. AS Security Mode Command (Integrity algorithm (indicates 256 bit algo), Ciphering algorithm (indicates 256 bit algo), Use 256 bit key indication MAC-I)
12. Determines to use 256 bit algorithms and 256 bit keys for AS security (i.e., skips 256 to 128 bit truncation of bits for NAS and AS keys). Verify AS SMC integrity. If successful start RRC integrity protection and RRC downlink deciphering.
13. AS Security Mode Complete
500

Figure 5

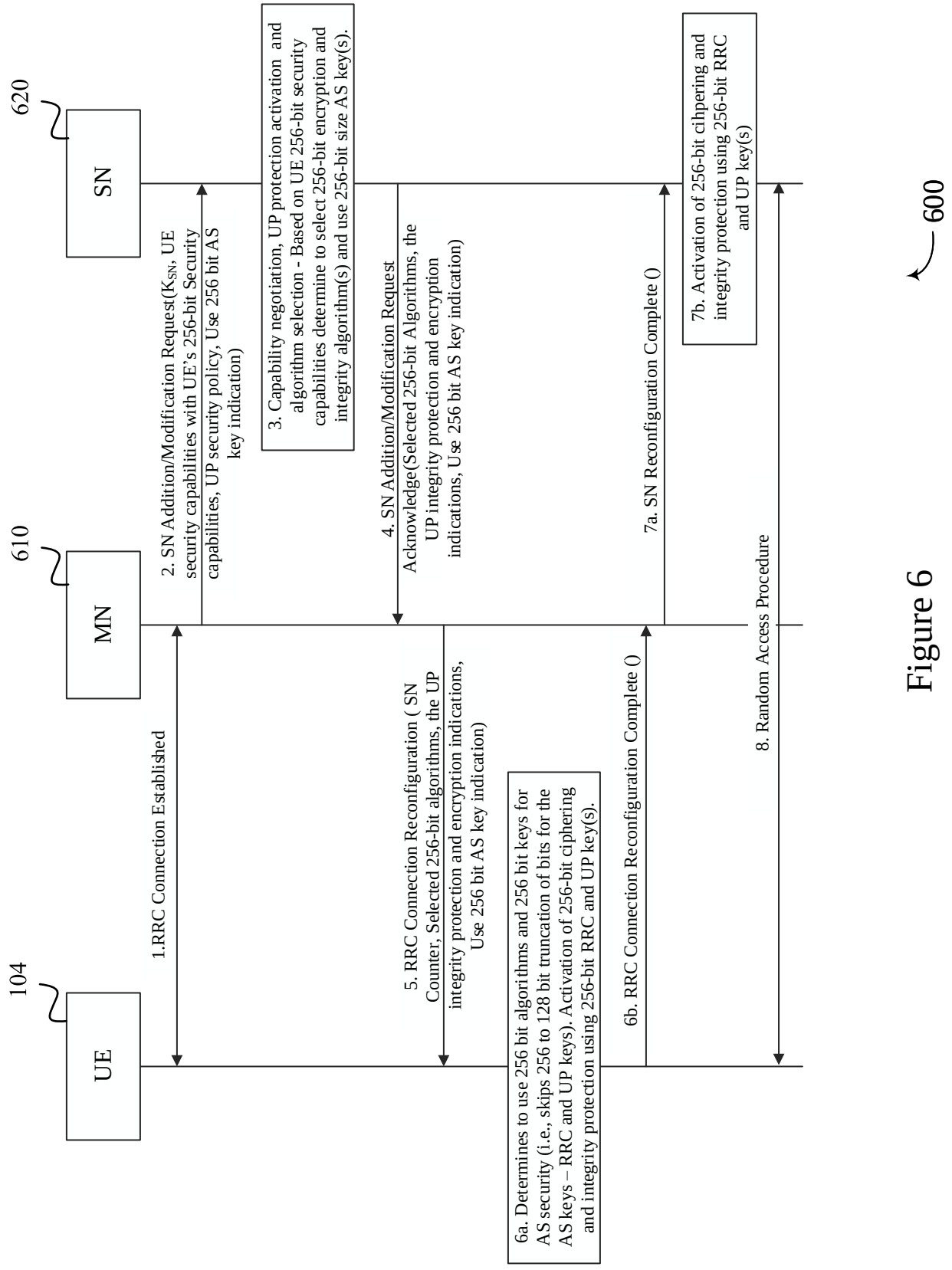

104
UE
610
MN
620
SN
1.RRC Connection Established
2. SN Addition/Modification Request($K_{SN}$, UE security capabilities with UE's 256-bit Security capabilities, UP security policy, Use 256 bit AS key indication)
3. Capability negotiation, UP protection activation and algorithm selection - Based on UE 256-bit security capabilities determine to select 256-bit encryption and integrity algorithm(s) and use 256-bit size AS key(s).
4. SN Addition/Modification Request Acknowledge(Selected 256-bit Algorithms, the UP integrity protection and encryption indications, Use 256 bit AS key indication)
5. RRC Connection Reconfiguration ( SN Counter, Selected 256-bit algorithms, the UP integrity protection and encryption indications, Use 256 bit AS key indication)
6a. Determines to use 256 bit algorithms and 256 bit keys for AS security (i.e., skips 256 to 128 bit truncation of bits for the AS keys – RRC and UP keys). Activation of 256-bit ciphering and integrity protection using 256-bit RRC and UP key(s).
6b. RRC Connection Reconfiguration Complete ()
7a. SN Reconfiguration Complete ()
7b. Activation of 256-bit cihpering and integrity protection using 256-bit RRC and UP key(s)
8. Random Access Procedure
600

Figure 6

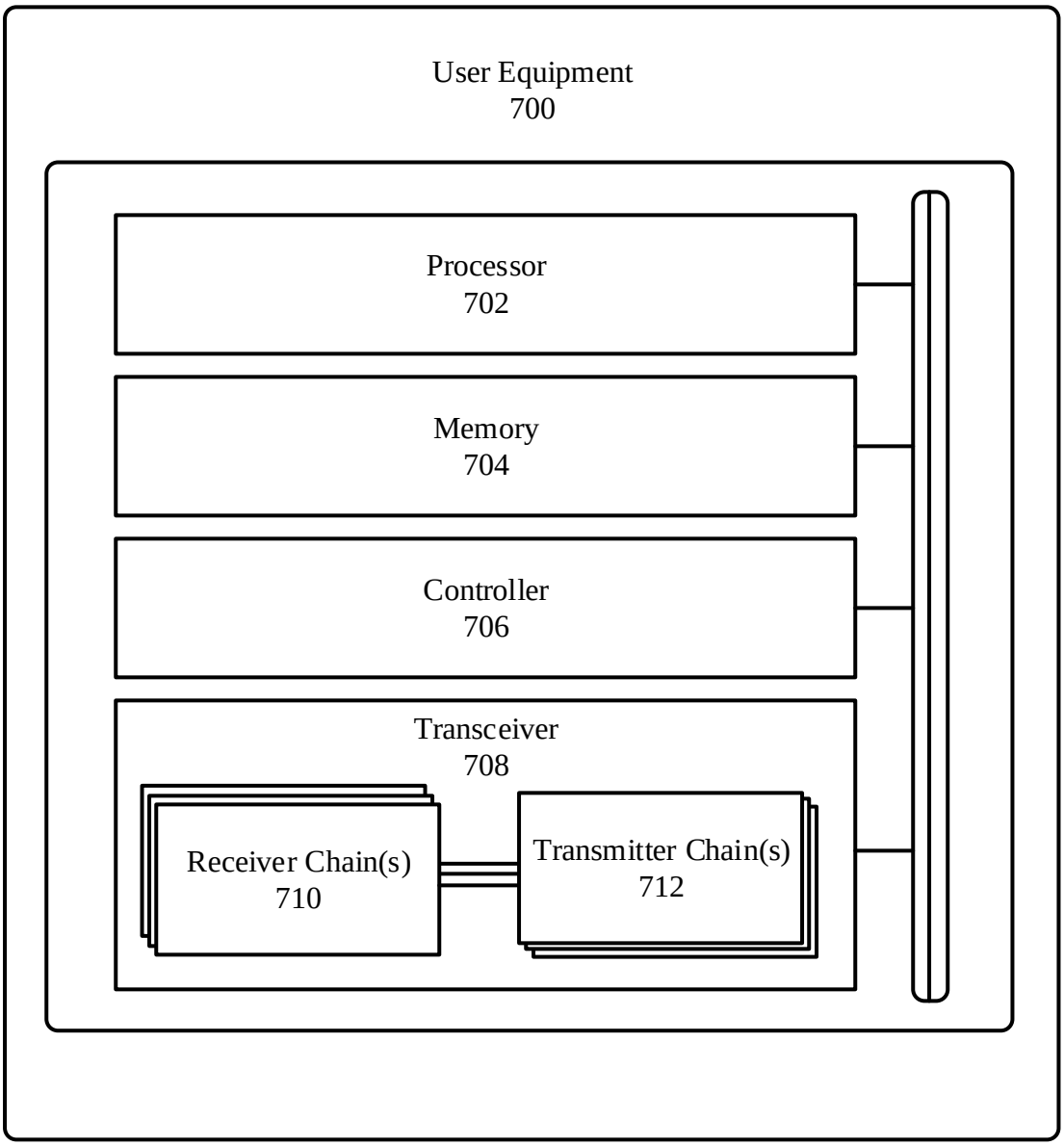

User Equipment
700
Processor
702
Memory
704
Controller
706
Transceiver
708
Receiver Chain(s)
710
Transmitter Chain(s)
712

Figure 7

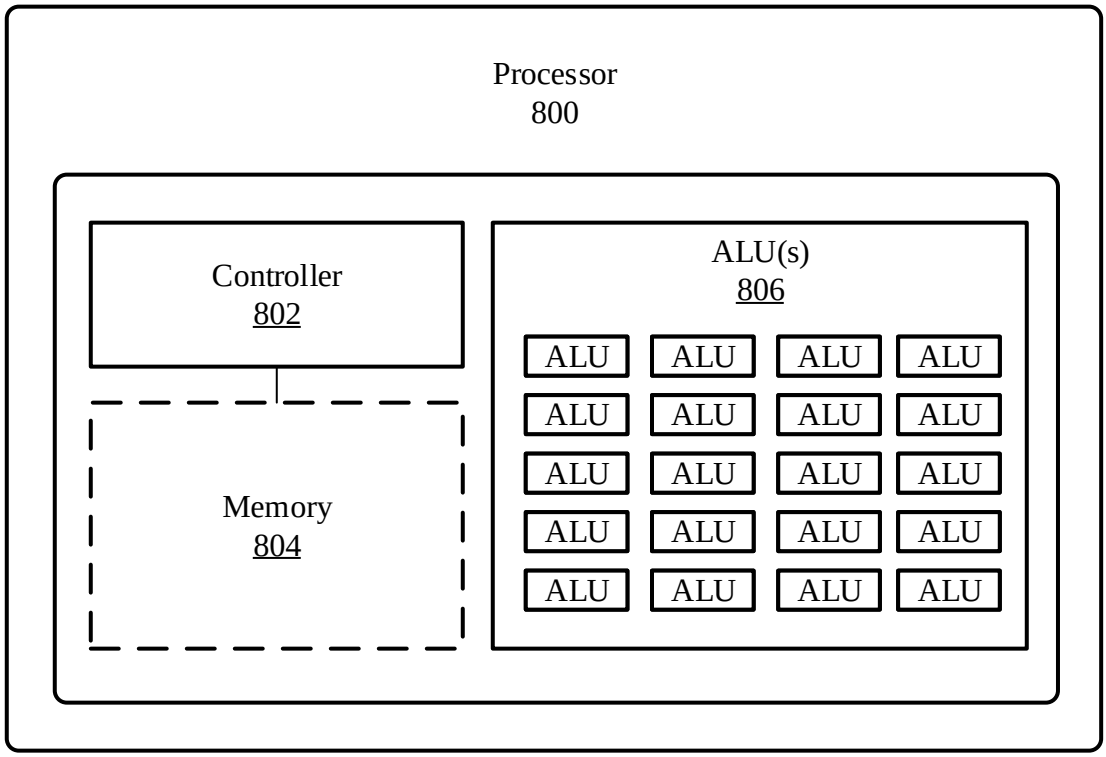

Processor
800
Controller
802
Memory
804
ALU(s)
806
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU
ALU

Figure 8

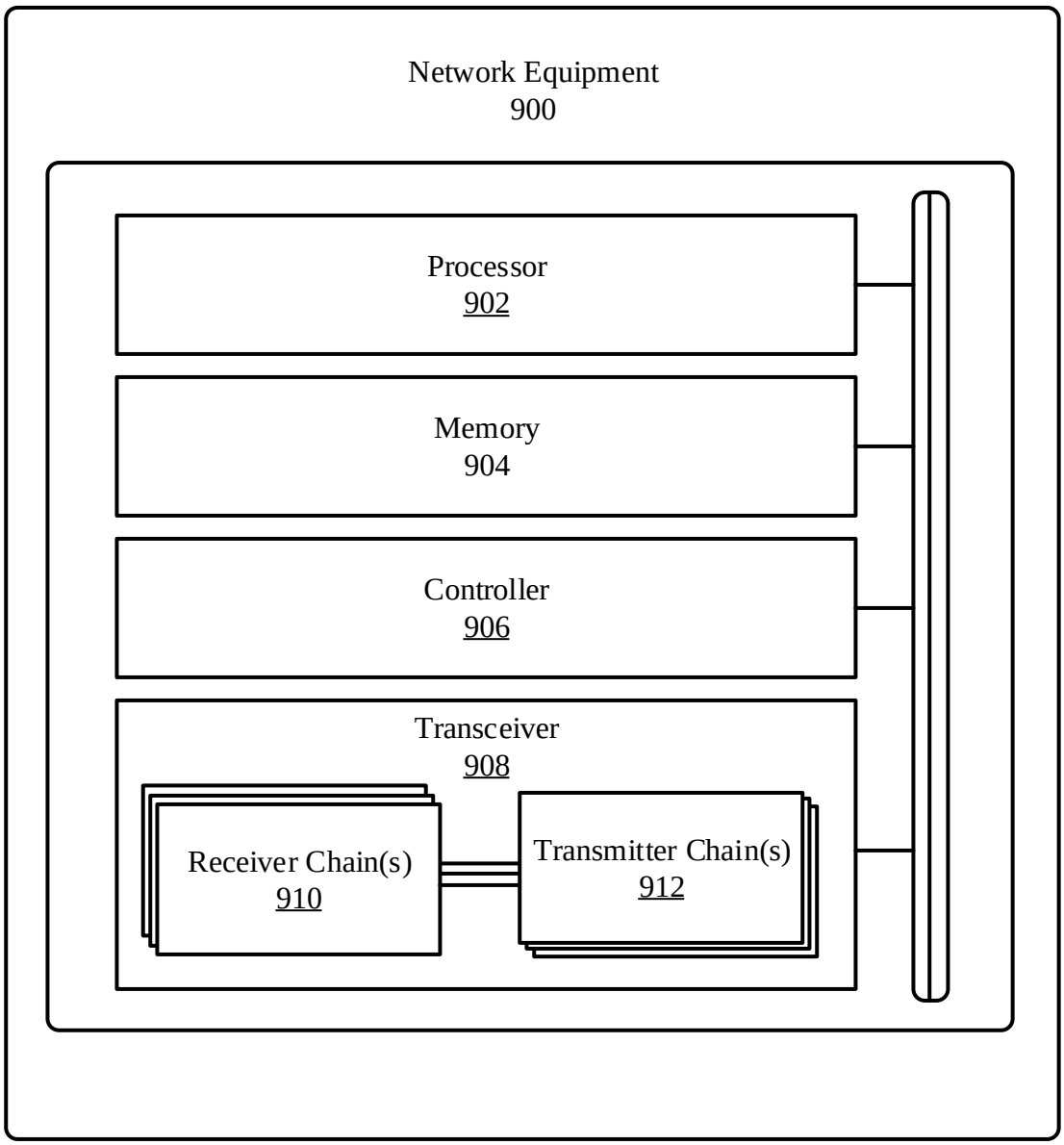

Network Equipment
900
Processor
902
Memory
904
Controller
906
Transceiver
908
Receiver Chain(s)
910
Transmitter Chain(s)
912

Figure 9

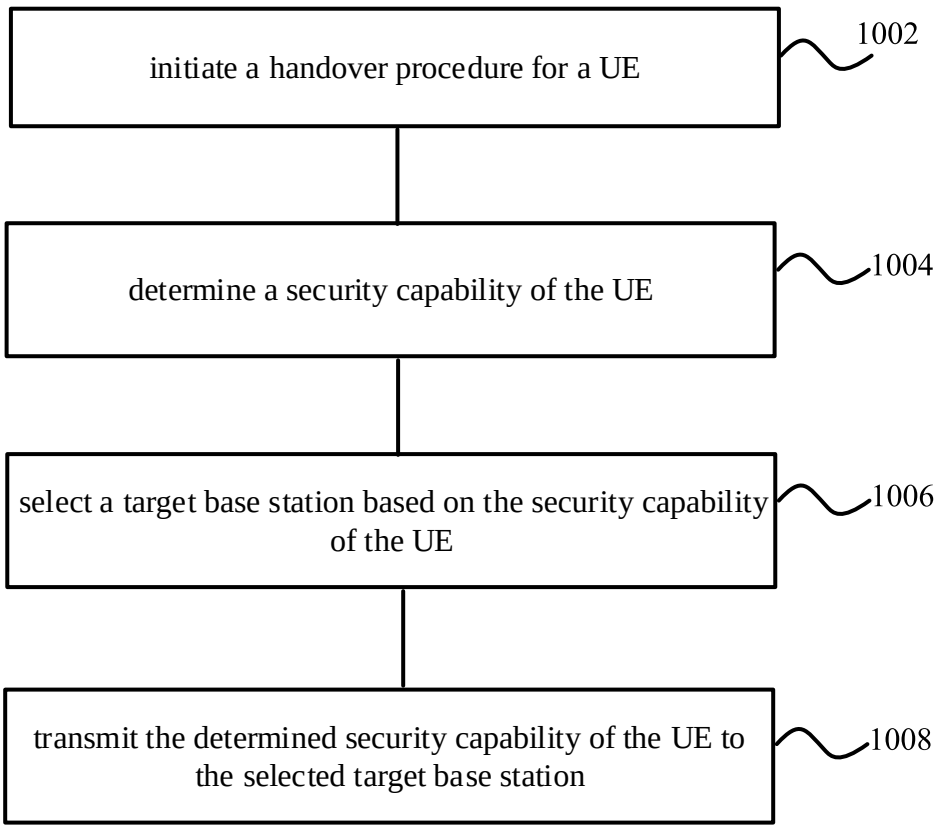

initiate a handover procedure for a UE
1002
determine a security capability of the UE
1004
select a target base station based on the security capability of the UE
1006
transmit the determined security capability of the UE to the selected target base station
1008

Figure 10

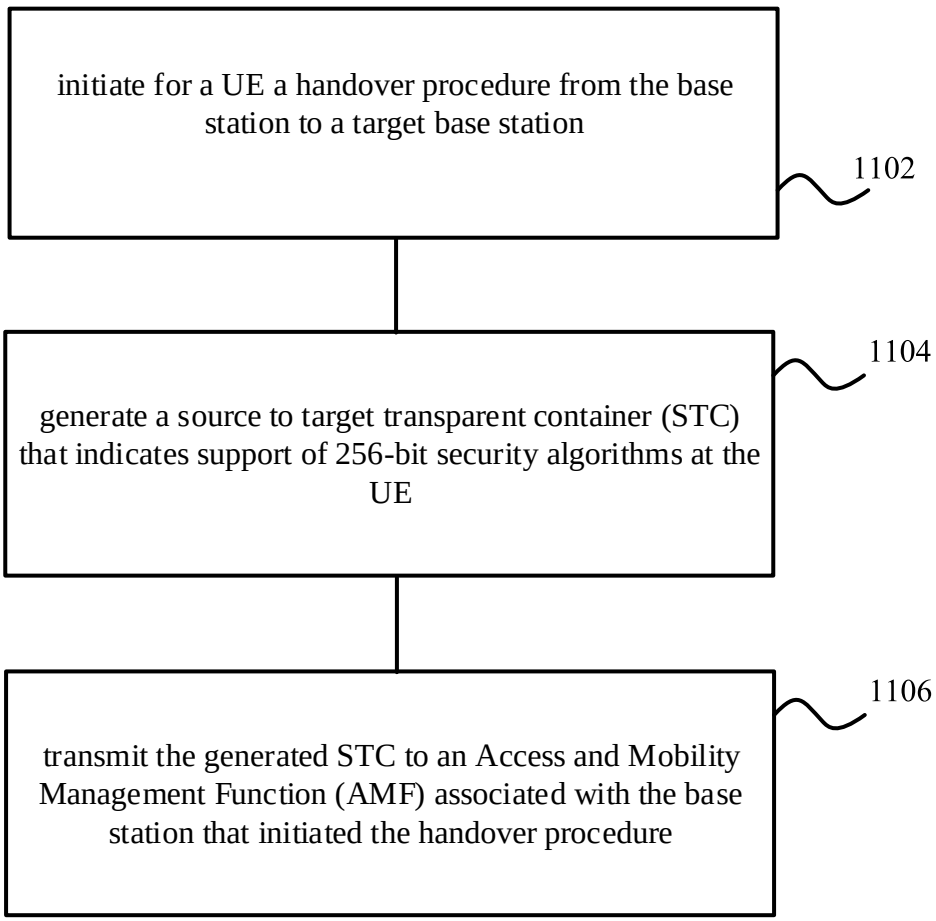

initiate for a UE a handover procedure from the base station to a target base station
1102
generate a source to target transparent container (STC) that indicates support of 256-bit security algorithms at the UE
1104
transmit the generated STC to an Access and Mobility Management Function (AMF) associated with the base station that initiated the handover procedure
1106

Figure 11

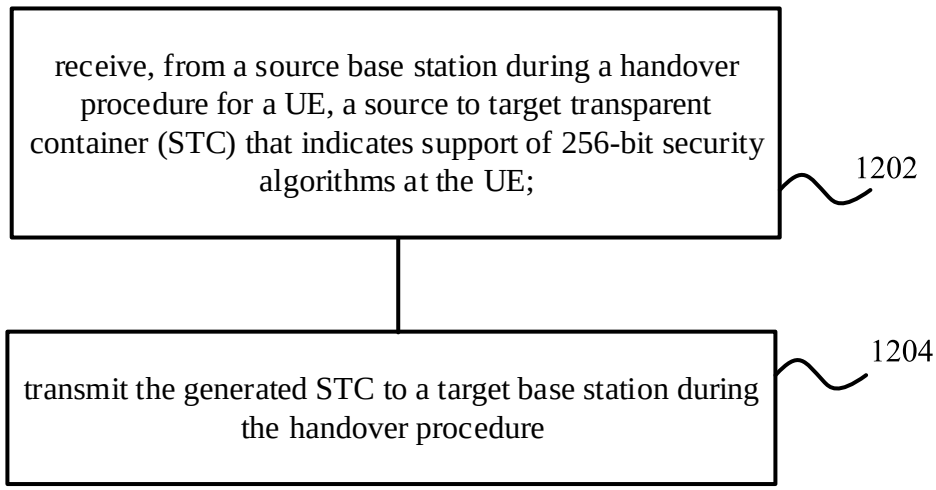

receive, from a source base station during a handover procedure for a UE, a source to target transparent container (STC) that indicates support of 256-bit security algorithms at the UE;
1202
transmit the generated STC to a target base station during the handover procedure
1204

Figure 12

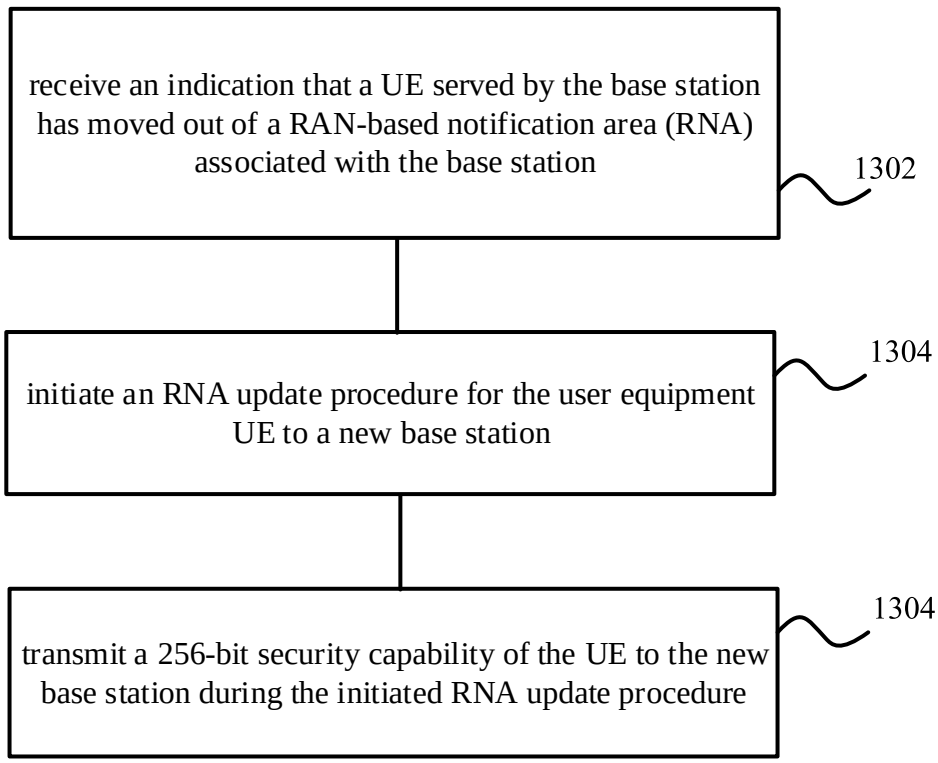

receive an indication that a UE served by the base station has moved out of a RAN-based notification area (RNA) associated with the base station
1302
initiate an RNA update procedure for the user equipment UE to a new base station
1304
transmit a 256-bit security capability of the UE to the new base station during the initiated RNA update procedure
1304

Figure 13

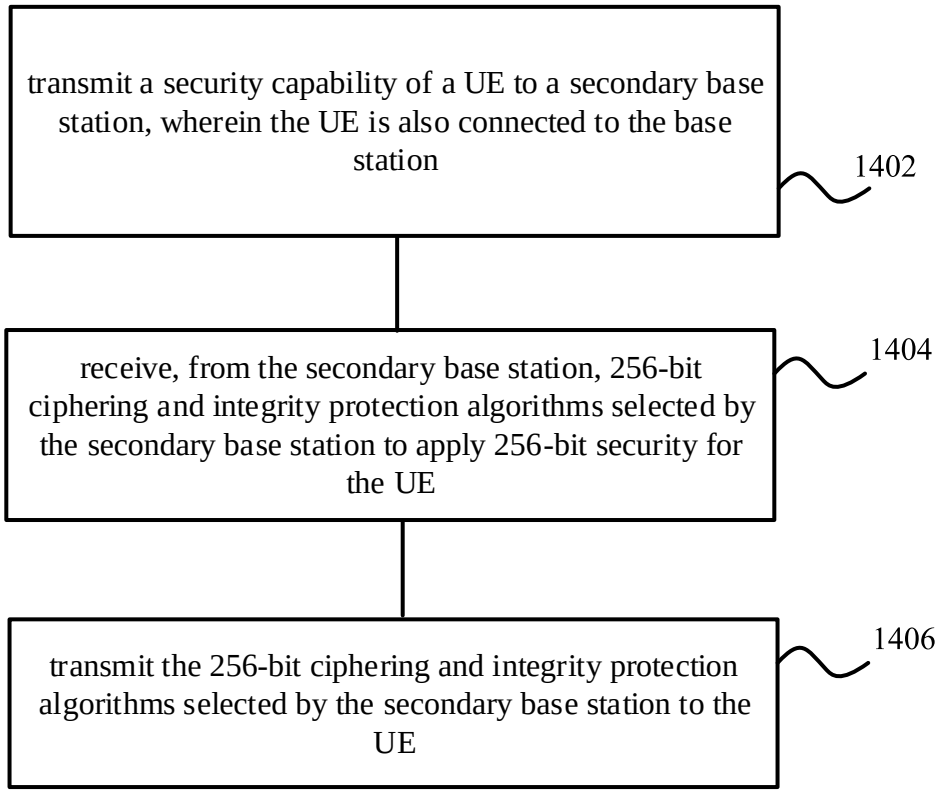

transmit a security capability of a UE to a secondary base station, wherein the UE is also connected to the base station
1402
receive, from the secondary base station, 256-bit ciphering and integrity protection algorithms selected by the secondary base station to apply 256-bit security for the UE
1404
transmit the 256-bit ciphering and integrity protection algorithms selected by the secondary base station to the UE
1406

Figure 14