CLAIMS

1. A method for wireless communications by a user equipment, UE (120), comprising:

receiving (802), from an anchor base station (110), a first message integrity protected with a first integrity protection key and encrypted with a first encryption key, wherein the first integrity protection key and the first encryption key are derived from a first key, and the first message comprises information for deriving a second key;

entering, based on an indication in the first message, a first state with no dedicated resources allocated to the UE;

transmitting (804), to a serving base station (110), a second message integrity protected with the first integrity protection key, wherein the second message comprises a request to transition from the first state to a second state with dedicated resources allocated to the UE;

receiving (806), from the serving base station, a third message comprising one or more indications;

determining (808) a third key based in part on at least one of the one or more indications in the third message or a blind detection procedure;

processing (810) the third message based on the third key; and

remaining in the first state in response to receiving the third message;

wherein the second message is sent for a radio access network, RAN, notification area, RNA, update.

2. The method of claim 1, wherein determining (808) the third key comprises determining whether the third key is the first key or the second key based in part on the one or more indications.

3. The method of claim 2,wherein:

the third message comprises a packet data convergence protocol, PDCP, header; and

the one or more indications comprise a count value in the PDCP header.

4. The method of claim 3, wherein the determination is that the third key is the first key if the count value is a non-initial value, wherein the non-initial count value in particular indicates anchor non-relocation.

5. The method of claim 2, wherein the one or more indications comprise at least one of an indication of whether the third key is the first key or the second key, or an indication of whether one or more parameters for deriving the third key are associated with the anchor base station or the serving base station.

6. The method of claim 5, wherein the one or more indications indicate:

that the third key is the first key and that the one or more parameters are associated with the anchor base station; or

that the third key is the first key and that the one or more parameters are associated with the serving base station; or

that the third key is the second key and that the one or more parameters are associated with the anchor base station; or

that the third key is the second key and that the one or more parameters are associated with the serving base station.

7. The method of claim 5, wherein the one or more indications are provided in a medium access control, MAC, control element, CE, or a packet data convergence protocol, PDCP, control protocol data unit, PDU; or

wherein the one or more parameters comprise at least one of an absolute radio frequency channel number, ARFCN, or a physical cell identifier, PCI.

8. The method of claim 1, wherein determining (808) the third key comprises at least one of:

assuming that the third key is always the second key; or

assuming that one or more parameters for deriving the third key are always associated with the serving base station.

9. The method of claim 1, further comprising:

deriving a second integrity protection key and a second encryption key from the third key;

wherein processing (810) the third message in particular comprises:

decrypting the third message using the second encryption key; and

verifying the third message using the second integrity protection key; or

wherein the third message in particular further comprises information for deriving a fourth key.

10. The method of claim 1, wherein the blind detection procedure comprises at least one of:

detecting whether the third key is the first key;

detecting whether the third key is the second key;

detecting whether one or more parameters for deriving the third key are associated with the anchor base station; or

detecting whether the one or more parameters are associated with the serving base station; or

further comprising determining after the blind detection procedure that:

the third key is the second key and the one or more parameters are associated with the anchor base station; or

the third key is the first key and the one or more parameters are associated with the anchor base station.

11. An apparatus for wireless communications at a user equipment, UE (120; 2200), comprising:

a receiver (2212) configured to receive (802), from an anchor base station (110), a first message integrity protected with a first integrity protection key and encrypted with a first encryption key, wherein the first integrity protection key and the first encryption key are derived from a first key, and the first message comprises information for deriving a second key;

a transmitter (2212) configured to transmit (804), to a serving base station (110), a second message integrity protected with the first integrity protection key,

wherein the receiver is further configured to receive (806), from the serving base station, a third message comprising one or more indications,

wherein the apparatus further comprises:

at least one processor (2208) configured to:

enter, based on an indication in the first message, a first state with no dedicated resources allocated to the UE;

determine (808) a third key based in part on at least one of the one or more indications in the third message or a blind detection procedure;

process (810) the third message based on the third key; and

remain in the first state in response to receiving the third message; and

a memory coupled to the at least one processor,

wherein the second message comprises a request to transition from the first state to a second state with dedicated resources allocated to the UE, and

wherein the second message is sent for a radio access network, RAN, notification area, RNA, update.

12. The apparatus of claim 11, wherein the at least one processor (2208) is further configured to perform the method of any one of claims 2 to 10.

13. An apparatus (110) for wireless communication at an anchor base station, comprising:

a transmitter (2212) configured to transmit (702), to a user equipment, UE (120), a first message encrypted with a first key, the first message comprising information for deriving a second key and an indication triggering the UE to enter a state with no dedicated resources allocated to the UE;

at least one processor (2208) configured to:

determine (704), during a context retrieval procedure with a serving base station, a third key for encrypting communications between the UE and the serving base station; and

determine whether to perform anchor relocation based on a type of radio access network, RAN, notification area, RNA, update procedure;

wherein the transmitter is further configured to transmit (706), to the serving base station, a second message encrypted with the second key, the second message comprising

an indication of the third key and an indication triggering the UE to enter a state with no dedicated resources allocated to the UE.

14. The apparatus of claim 13, wherein in the context retrieval procedure:

the receiver is further configured to receive, from the serving base station, a third message comprising information derived from the first key, the third message comprising a request for a context of the UE; and

the transmitter is further configured to transmit the second message to the serving base station in response to the third message; or

wherein the second message comprises a radio resource control, RRC, release message.

15. The apparatus of claim 13, wherein the at least one processor is configured to:

determine the third key by performing a horizontal key derivation; or

determine the third key by performing a vertical key derivation; or

derive the second key based on one or more parameters associated with the serving base station; or

derive the second key based on one or more parameters associated with the anchor base station;

wherein the one or more parameters in particular comprise at least one of an absolute radio frequency channel number, ARFCN, or a physical cell identifier, PCI, or wherein the second message further in particular comprises an indication that the one or more parameters are associated with the anchor base station.

16. The apparatus of claim 13, wherein the information for deriving the second key comprises a next hop chaining counter, NCC, or

wherein the at least one processor is configured to:

determine the third key during the context retrieval procedure while the UE is in a state with dedicated resources allocated to the UE; or

determine whether to perform anchor relocation based on a third message received from the serving base station, wherein the third message in particular indicates whether the UE has an uplink packet available for transmission.

17. The apparatus of claim 13,

wherein the type of RNA update procedure is determined based on at least one of a radio access network notification area code, RANAC, cell identity, tracking area identity, TAI, UE configured radio access network, RAN, notification area update, RNA, list, or routing area update, RAU, timer associated with the serving base station.

18. The apparatus of claim 13, wherein the at least one processor is configured to determine the third key during the context retrieval procedure with anchor non-relocation;

wherein the anchor non-relocation is in particular associated with at least one of an uplink transmission in a radio resource control, RRC, resume request message, a downlink transmission in a RRC release message, a periodic radio access network, RAN, notification area, RNA, update, or a location report triggered RAN paging procedure.