CLAIMS

1. A method, in a network node, for security key generation for secured communications between a wireless terminal and an anchor base station and between the wireless terminal and an assisting base station, wherein the wireless terminal is or is about to be dually connected to the anchor base station and the assisting base station, the method comprising:

generating (810) an assisting security key for the assisting base station, based, at least in part, on an anchor base station key;

sending (820), to the assisting base station, the generated assisting security key, for use by the assisting base station in encrypting data traffic sent to the wireless terminal or in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station while the wireless terminal is dually connected to the anchor base station and the assisting base station; and

using (830) the anchor base station key, or a key derived from the anchor base station key, for encrypting data sent to the wireless terminal by the anchor base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.

2. The method of claim 1, wherein the generated assisting security key comprises a base assisting security key for use in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station.

~~3. The method of claim 2, wherein using (830) the anchor base station key comprises deriving an encryption key, or an integrity key, or both, from the anchor base station key, and using the derived key or keys for protecting data sent to the wireless terminal by the anchor base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.~~

~~4. The method of any of claims 1-3, wherein generating (810) the assisting security key comprises deriving the assisting security key from the anchor base station key using a one-way function.~~

~~5. The method of claim 4, wherein the one-way function is an HMAC-SHA-256 cryptographic function.~~

~~6. The method of any of claims 1-5, wherein generating (810) the assisting security key is further based on a freshness parameter.~~

~~7. The method of any of claims 1-6, further comprising:~~

~~detecting that a Packet Data Convergence Protocol, PDCP, COUNT parameter in the assisting base station is about to wrap around;~~

~~in response to said detecting, initiating a refresh of the anchor base station key and re-calculating the assisting security key.~~

~~8. The method of any of claims 1-7, wherein the network node is a Long-Term Evolution, LTE, eNodeB.~~

~~9. The method of any of claims 1-8, wherein said generating (810)is repeated for each of a plurality of Data Radio Bearers established between the wireless terminal and the assisting base station, such that the resulting assisting security keys differ for each Data Radio Bearer.~~

1~~0~~. A method, in an anchor base station ~~network node~~, for security key generation for secure~~d~~ communications between a wireless terminal ~~and an anchor base station and between the wireless terminal~~ and an assisting base station, wherein the wireless terminal is or is about to be dually connected to the anchor base station and the assisting base station, wherein a primary security key is known to the anchor base station and the wireless terminal, the method comprising:

~~sharing (910) a primary security key with the wireless terminal;~~

generating (920) an assisting security key for the assisting base station, based, at least in part, on the primary security key;

sending (930), to the assisting base station, the generated assisting security key, for use by the assisting base station ~~in encrypting data traffic sent to the wireless terminal or~~ in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.

2~~1~~. The method of claim 1~~0~~, wherein the generated assisting security key comprises a base assisting security key for use in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station.

312. The method of claim 10 or 211, wherein generating (920) the assisting security key comprises deriving the assisting security key from the anchor base stationprimary key using a one-way function.

413. The method of claim 312, wherein the one-way function is an HMAC-SHA-256 cryptographic function.

514. The method of any of claims 10-413, wherein generating (920) the assisting security key is further based on a freshness parameter.

15. The method of any of claims 10-14, wherein sending (930) the generated assisting security key to the assisting base station comprises sending the generated assisting security key to the assisting base station indirectly, via the anchor base station.

16. The method of any of claims 10-15, wherein the network node is a mobility management node.

17. A network node (401A) for security key generation for secured communications between a wireless terminal and an assisting base station, wherein the wireless terminal is, or is about to be, dually connected to the anchor base station and the assisting base station, the network node (401A) comprising interface circuitry (440A) configured to communicate with the assisting base station and further comprising processing circuitry (420A, 430A), characterized in that the processing circuitry (420A, 430A) is configured to:

generate an assisting security key for the assisting base station, based, at least in part, on an anchor base station key;

send to the assisting base station, using the interface circuitry, the generated assisting security key, for use by the assisting base station in encrypting data traffic sent to the wireless terminal or in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station while the wireless terminal is dually connected to the anchor base station and the assisting base station; and

use the anchor base station key, or a key derived from the anchor base station key, for encrypting data sent to the wireless terminal by the anchor base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.

18. The network node (401A) of claim 17, wherein the generated assisting security key comprises a base assisting security key for use in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station.

19. The network node (401A) of claim 18, wherein the processing circuitry (420A, 430A) is configured to use the anchor base station key to derive an encryption key, or an integrity key, or both, from the anchor base station key, and to use the derived key or keys for protecting data sent to the wireless terminal by the anchor base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.

~~20. The network node (401A) of any of claims 17-19, wherein the processing circuitry (420A, 430A) is configured to generate the assisting security key by deriving the assisting security key from the anchor base station key using a one-way function.~~

~~21. The network node (401A) of claim 20, wherein the one-way function is an HMAC-SHA-256 cryptographic function.~~

~~22. The network node (401A) of any of claims 17-21, wherein the processing circuitry (420A, 430A) is configured to generate the assisting security key based further on a freshness parameter.~~

~~23. The network node (401A) of any of claims 17-22, wherein the processing circuitry (420A, 430A) is further configured to:~~

~~detect that a Packet Data Convergence Protocol, PDCP, COUNT parameter in the assisting base station is about to wrap around;~~

~~in response to said detecting, initiate a refresh of the anchor base station key and re-calculate the assisting security key.~~

~~24. The network node (401A) of any of claims 17-23, wherein the network node (401A) is a Long-Term Evolution, LTE, eNodeB.~~

~~25. The network node (401A) of any of claims 17-24, wherein the processing circuitry (420A, 430A) is configured to repeat said generating for each of a plurality of Data Radio Bearers established between the wireless terminal and the assisting base station, such that the resulting assisting security keys differ for each Data Radio Bearer.~~

~~2~~6. An anchor base station ~~network node~~ (505A) for security key generation for secure~~d~~ communications between a wireless terminal and an assisting base station, wherein the wireless terminal is, or is about to be, dually connected to the anchor base station and the assisting base station, and wherein a primary security key is known to the anchor base station (505A) and the wireless terminal, the ~~network node~~anchor base station (505A) comprising interface circuitry (510A) configured to communicate with the assisting base station and further comprising processing circuitry (520A, 530A), characterized in that the processing circuit is configured to:

~~share a primary security key with the wireless terminal;~~

generate an assisting security key for the assisting base station, based, at least in part, on the primary security key;

send to the assisting base station, via the interface circuitry (510A), the generated assisting security key, for use by the assisting base station in ~~encrypting data traffic sent to the wireless terminal or in~~ generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station while the wireless terminal is dually connected to the anchor base station and the assisting base station.

~~2~~7. The ~~network node~~anchor base station (505A) of claim ~~2~~6, wherein the generated assisting security key comprises a base assisting security key for use in generating one or more additional assisting security keys for encrypting data traffic sent to the wireless terminal by the assisting base station.

~~2~~8. The ~~network node~~anchor base station (505A) of claim ~~2~~6 or ~~2~~7, wherein the processing circuitry (520A, 530A) is configured to generate the assisting security key by deriving the assisting security key from the ~~anchor base station~~primary key using a one-way function.

~~2~~9. The ~~network node~~anchor base station (505A) of claim ~~2~~8, wherein the one-way function is an HMAC-SHA-256 cryptographic function.

1~~3~~0. The ~~network node~~anchor base station (505A) of any of claims ~~2~~6-~~2~~9, wherein the processing circuitry (520A, 530A) is configured to generate the assisting security key based further on a freshness parameter.

~~31. The network node (505A) of any of claims 26-30, wherein the processing circuitry (520A, 530A) is configured to send the generated assisting security key to the assisting base station indirectly, via the anchor base station.~~

~~32. The network node (505A) of any of claims 26-31, wherein the network node (505A) is a mobility management node.~~