We Claim:

1) A user equipment configured to support dual connectivity operation towards a master node and a secondary node of a radio access network, the user equipment comprising at least one processor and at least one memory, the at least one memory storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least the following:

- establishing a connection towards the master node;
- receiving configuration information from the master node, wherein the configuration information comprises key counter information which defines a sequence of at least two different key counter values to generate at least two different security keys for at least two different target secondary nodes; wherein a first target secondary node is configured for a first conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the first target secondary node, and wherein a second target secondary node is configured for a subsequent conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the second target secondary node.

2) The user equipment according to claim 1, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least one of the following:

- generating a first security key using a first key counter value derived from the key counter information;
- using the first security key for integrity protection and/or ciphering of data exchanged between the user equipment and a first target secondary node;
- processing the key counter information such that the user equipment is enabled to derive, from the processed key counter information, at least a second key counter value, which is different from the first key counter value.

3) The user equipment according to claim 2, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least one of the following:

- generating a second security key, which is different from the first security key, using the second key counter value derived from the processed key counter information;
- using the second security key for integrity protection and/or ciphering of data exchanged between the user equipment and a second target secondary node, which is different from the first target secondary node;

- further processing the key counter information such that the user equipment is enabled to derive, from the further processed key counter information, at least a further key counter value, which is different from the first key counter value and different from the second key counter value.

4) The user equipment according to claim 1, wherein the key counter information received from the master node defines a list of at least two different key counter values.

5) The user equipment according to claim 2, wherein generating the first security key comprises using the first list element in the list of key counter values as the first key counter value, wherein processing the key counter information comprises removing the first list element from the list of key counter values.

6) The user equipment according to claim 3, wherein generating the second security key comprises using the presently first list element in the list of key counter values as the second key counter value, wherein further processing the key counter information comprises removing the presently first list element from the list of key counter values.

7) The user equipment according to claim 6,
wherein the configuration information comprises key counter information which defines a list of at least two different SN counter values to generate at least two different K_{SN} security keys for at least two different target secondary nodes,
wherein the first key counter value is a first SN counter value, wherein the second key counter value is a second SN counter value, wherein the first security key is a first K_{SN} security key, wherein the second security key is a second K_{SN} security key,
wherein the configuration information further comprises a radio resource control reconfiguration request,
wherein the configuration information further comprises information which is related to a conditional addition or change of a primary cell of a secondary cell group associated with the first target secondary node or related to a conditional handover towards the first target secondary node,
wherein the configuration information further comprises information which is related to a conditional addition or change of a primary cell of a secondary cell group associated with the second target secondary node or related to a conditional handover towards the second target secondary node,
the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least one of the following:

- determining whether at least one condition for a conditional addition or change of a primary cell of a secondary cell group associated with the first target secondary node or at least one condition for a conditional handover towards the first target secondary node is fulfilled;
- initiating, via a random access channel, a random access procedure towards the first target secondary node using the first K_{SN} security key;

- determining whether at least one condition for a conditional addition or change of a primary cell of a secondary cell group associated with the second target secondary node or at least one condition for a conditional handover towards the second target secondary node is fulfilled;
- initiating, via a random access channel, a random access procedure towards the second target secondary node using the second K_{SN} security key.

8) The user equipment according to claim 4, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least the following:
- receiving at least one additional list element for the list of key counter values from the master node.

9) The user equipment according to claim 1, wherein the key counter information received from the master node comprises a key counter value and an instruction to maintain the key counter value.

10) The user equipment according to claim 2, wherein generating the first security key comprises using the key counter value received from the master node as the first key counter value, wherein processing the key counter information comprises adding a predefined step value to the key counter value received from the master node.

11) The user equipment according to claim 3, wherein generating the second security key comprises using the present key counter value as the second key counter value, wherein further processing the key counter information comprises adding the predefined step value to the present key counter value.

12) The user equipment according to claim 11,
wherein the configuration information comprises key counter information which defines a sequence of at least two different SN counter values to generate at least two different K_{SN} security keys for at least two different target secondary nodes,
wherein the key counter information received from the master node comprises an SN counter value and an instruction to maintain the SN counter value,
wherein the first key counter value is a first SN counter value, wherein the second key counter value is a second SN counter value, wherein the first security key is a first K_{SN} security key, wherein the second security key is a second K_{SN} security key,
wherein the configuration information further comprises a radio resource control reconfiguration request,
wherein the configuration information further comprises information which is related to a conditional addition or change of a primary cell of a secondary cell group associated with the first target secondary node or related to a conditional handover towards the first target secondary node,
wherein the configuration information further comprises information which is related to a conditional addition or change of a primary cell of a secondary cell group associated with the second target secondary node or related to a conditional handover towards the second target secondary node,

the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least one of the following:

- determining whether at least one condition for a conditional addition or change of a primary cell of a secondary cell group associated with the first target secondary node or at least one condition for a conditional handover towards the first target secondary node is fulfilled;
- initiating, via a random access channel, a random access procedure towards the first target secondary node using the first K_{SN} security key;
- determining whether at least one condition for a conditional addition or change of a primary cell of a secondary cell group associated with the second target secondary node or at least one condition for a conditional handover towards the second target secondary node is fulfilled;
- initiating, via a random access channel, a random access procedure towards the second target secondary node using the second K_{SN} security key.

13) The user equipment according to claim 10, wherein the key counter information received from the master node defines a maximum allowed number of additions of the predefined step value to the key counter value received from the master node, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least the following:

- determining whether the maximum allowed number of additions has been reached;
- in response to determining that the maximum allowed number of additions has been reached, preventing further additions of the predefined step value to the present key counter value.

14) The user equipment according to claim 3, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least one of the following:

- generating a further security key, which is different from the first security key and different from the second security key, using the further key counter value derived from the further processed key counter information;
- using the further security key for integrity protection and/or ciphering of data exchanged between the user equipment and a further target secondary node, which is different from the second target secondary node;
- further processing the key counter information such that the user equipment is enabled to derive, from the further processed key counter information, at least one further key counter value, which is different from the first key counter value, different from the second key counter value, and different from any other key counter value derived previously from the non-processed, processed or further processed key counter information.

15) The user equipment according to claim 1, wherein the configuration information further comprises information indicative of at least one target secondary cell for which generating a security key is not required.

16) The user equipment according to claim 1, the at least one memory further storing instructions that, when executed by the at least one processor, cause the user equipment to further perform: establishing a connection towards the secondary node; and

- wherein the first target secondary node is configured for a first conditional PSCell addition or change (CPAC) or a conditional handover (CHO) from the secondary node the UE is connected to towards the first target secondary node, and wherein a second target secondary node is configured for a subsequent conditional PSCell addition or change (CPAC) or a conditional handover (CHO) from the first target secondary node the UE is connected to after the first CPAC or CHO towards the second target secondary node.

17) A non-transitory computer-readable medium comprising program instructions that, when executed by a user equipment configured to support dual connectivity operation towards a master node and a secondary node of a radio access network, cause the user equipment to perform at least the following:

- establishing a connection towards the master node;
- receiving configuration information from the master node, wherein the configuration information comprises key counter information which defines a sequence of at least two different key counter values to generate at least two different security keys for at least two different target secondary nodes; wherein a first target secondary node is configured for a first conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the first target secondary node, and wherein a second target secondary node is configured for a subsequent conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the second target secondary node.

18) A master node of a radio access network, the master node configured to support dual connectivity operation towards a secondary node of the radio access network and a user equipment, the master node comprising at least one processor and at least one memory, the at least one memory storing instructions that, when executed by the at least one processor, cause the master node to perform at least the following:

- establishing a connection towards the user equipment;
- transmitting configuration information to the user equipment, wherein the configuration information comprises key counter information which defines a sequence of at least two different key counter values to generate at least two different security keys for at least two different target secondary nodes; wherein a first target secondary node is configured for a first conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the first target secondary node, and wherein a second target secondary node is configured for a subsequent conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the second target secondary node.

19) The master node according to claim 18, wherein the key counter information transmitted to the user equipment defines a list of at least two different key counter values.

20) The master node according to claim 19, the at least one memory further storing instructions that, when executed by the at least one processor, cause the master node to perform at least the following:

- generating a list of at least two different security keys which corresponds to the list of at least two different key counter values defined by the key counter information transmitted to the user equipment;
- transmitting request information to at least one target secondary node, wherein the request information comprises the generated list of security keys.

21) The master node according to claim 20, the at least one memory further storing instructions that, when executed by the at least one processor, cause the master node to perform at least one of the following:

- receiving, from a first target secondary node, information indicative of a security key switch;
- transmitting, to at least one other target secondary node, an instruction to remove the first list element from the list of security keys, wherein the at least one other target secondary node is different from the first target secondary node.

22) The master node according to claim 21, the at least one memory further storing instructions that, when executed by the at least one processor, cause the master node to perform at least one of the following:

- receiving, from a second target secondary node, information indicative of a security key switch, wherein the second target secondary node is different from the first target secondary node;
- transmitting, to at least one further target secondary node, an instruction to remove the presently first list element from the list of security keys, wherein the at least one further target secondary node is different from the second target secondary node.

23) The master node according to claim 20, the at least one memory further storing instructions that, when executed by the at least one processor, cause the master node to perform at least the following:

- transmitting at least one additional list element for the list of key counter values to the user equipment;
- transmitting at least one additional list element for the list of security keys to at least one target secondary node.

24) The master node according to claim 18, wherein the key counter information transmitted to the user equipment comprises a key counter value and an instruction to maintain the key counter value.

25) The master node according to claim 18, wherein the master node comprises a gNB-CU-CP node comprising at least one processor and at least one memory, wherein the instructions are stored on the at

least one memory of the gNB-CU-CP node to be executed by the at least one processor of the gNB-CU-CP node.

26) The master node according to claim 18, wherein the configuration information further comprises information indicative of at least one target secondary cell for which generating a security key is not required.

27) A non-transitory computer-readable medium comprising program instructions that, when executed by a master node of a radio access network, the master node configured to support dual connectivity operation towards a secondary node of the radio access network and a user equipment, cause the master node to perform at least the following:

- establishing a connection towards the user equipment;
- transmitting configuration information to the user equipment, wherein the configuration information comprises key counter information which defines a sequence of at least two different key counter values to generate at least two different security keys for at least two different target secondary nodes; wherein a first target secondary node is configured for a first conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the first target secondary node, and wherein a second target secondary node is configured for a subsequent conditional PSCell addition or change (CPAC) or a conditional handover (CHO) towards the second target secondary node.

28)

ABSTRACT

SECURITY KEY MANAGEMENT IN DUAL CONNECTIVITY OPERATION

The disclosure inter alia relates to a user equipment configured to support dual connectivity operation towards a master node and a secondary node of a radio access network, the user equipment comprising at least one processor and at least one memory, the at least one memory storing instructions that, when executed by the at least one processor, cause the user equipment to perform at least the following: establishing a connection towards the master node; receiving configuration information from the master node, wherein the configuration information comprises key counter information which defines a sequence of at least two different key counter values to generate at least two different security keys for at least two different target secondary nodes.

FIG. 1 is proposed for publication.