Claims

1. A user equipment (UE) comprising a Mission-Critical Push-To-Talk (MCPTT) client equipped to be connected to a MCPTT node that serves the UE, comprising:

processing circuitry, memory, and transceiver circuitry collectively configured to:

receive a first message from the MCPTT node in unicast when activating a Multimedia Broadcast and Multicast Service (MBMS) bearer, wherein the first message comprises a MBMS Subchannel Control Key (MSCCK);

identify the MSCCK from the message;

receive an MBMS subchannel control message from the MCPTT node; and

apply integrity protection and/or confidentiality protection to the MBMS subchannel control message using the MSCCK.

2. The UE of claim 1, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises generating a message authentication code (MAC) value using the at least one MBMS subchannel control message and the MSCCK, and comparing the generated MAC value to a MAC value appended to the at least one MBMS subchannel control message.

3. The UE of claim 1, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises decrypting the MBMS subchannel control message using the MSCCK.

4. The UE of claim 1, wherein the at least one MBMS subchannel control message comprises a Map Group To Bearer message.

5. The UE of claim 1, wherein the at least one MBMS subchannel control message comprises an Unmap Group To Bearer message.

6. A method of operating a user equipment (UE) comprising a Mission-Critical Push-To-Talk (MCPTT) client equipped to be connected to a MCPTT node that serves the UE, comprising:

receiving a first message from the MCPTT node in unicast when activating a Multimedia Broadcast and Multicast Service (MBMS) bearer, wherein the first message comprises a MBMS Subchannel Control Key (MSCCK);

identifying the MSCCK from the message;

receiving an MBMS subchannel control message from the MCPTT node; and

applying integrity protection and/or confidentiality protection to the MBMS subchannel control message using the MSCCK.

7. The method of claim 6, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises generating a message authentication code (MAC) value using the at least one MBMS subchannel control message and the MSCCK, and comparing the generated MAC value to a MAC value appended to the at least one MBMS subchannel control message.

8. The method of claim 6, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises decrypting the MBMS subchannel control message using the MSCCK.

9. The method of claim 6, wherein the at least one MBMS subchannel control message comprises a Map Group To Bearer message.

10. The method of claim 6, wherein the at least one MBMS subchannel control message comprises an Unmap Group To Bearer message.

11. A method of operating a UE comprising a Mission-Critical Push-To-Talk (MCPTT) client connected to a MCPTT node that serves the UE, comprising:

receiving a first message from the MCPTT node in unicast when activating a MBMS bearer, wherein the first message comprises a Multimedia Broadcast and Multicast Service (MBMS) Subchannel Control Key (MSCCK);

identifying the MSCCK from the message;

receiving an MBMS subchannel control message from the MCPTT node; and

decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK.

12. The method of claim 11, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises generating a message authentication code (MAC) value using the at least one MBMS subchannel control message and the MSCCK, and comparing the generated MAC value to a MAC value appended to the at least one MBMS subchannel control message.

13. The method of claim 11, wherein decrypting and/or integrity checking the MBMS subchannel control message using the MSCCK comprises decrypting the MBMS subchannel control message using the MSCCK.

14. The method of claim 11, wherein the at least one MBMS subchannel control message comprises a Map Group To Bearer message.

15. The method of claim 11, wherein the at least one MBMS subchannel control message comprises an Unmap Group To Bearer message.