CLAIMS

1. A method for establishing a first security context between a remote station and a serving network, the first security context having a security property that is not supported by a second security context, the method comprising:

the remote station forwarding a first message to the serving network, wherein the first message includes an information element signaling that the remote station supports the first security context;

the remote station generating at least one session key, in accordance with the first security context, using the information element;

the remote station receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and

the remote station, in response to the second message, having wireless communications protected by the at least one session key.

2. A method for establishing a first security context as defined in claim 1, wherein the information element comprises a count value updated for a session.

3. A method for establishing a first security context as defined in claim 1, wherein the serving network is a UMTS serving network.

4. A method for establishing a first security context as defined in claim 3, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

5. A method for establishing a first security context as defined in claim 1, wherein the serving network is a GERAN serving network.

6. A method for establishing a first security context as defined in claim 1, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

7. A method for establishing a first security context as defined in claim 1, wherein the remote station comprises a mobile user equipment.

8. A remote station, comprising:

means for forwarding a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

means for generating at least one session key, in accordance with the first security context, using the information element;

means for receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and

means for having wireless communications, in response to the second message, protected by the at least one session key.

9. A remote station as defined in claim 8, wherein the information element comprises a count value updated for a session.

10. A remote station as defined in claim 8, wherein the serving network is a UMTS serving network.

11. A remote station as defined in claim 10, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

12. A remote station as defined in claim 8, wherein the serving network is a GERAN serving network.

13. A remote station as defined in claim 8, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

14. A remote station as defined in claim 8, wherein the remote station comprises a mobile user equipment.

15. A remote station, comprising:

a processor configured to:

forward a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

generate at least one session key, in accordance with the first security context, using the information element;

receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

have wireless communications, in response to the second message, protected by the at least one session key.

16. A remote station as defined in claim 15, wherein the information element comprises a count value updated for a session.

17. A remote station as defined in claim 15, wherein the serving network is a UMTS serving network.

18. A remote station as defined in claim 17, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

19. A remote station as defined in claim 15, wherein the serving network is a GERAN serving network.

20. A remote station as defined in claim 15, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

21. A remote station as defined in claim 15, wherein the remote station comprises a mobile user equipment.

22. A computer program product, comprising:

computer-readable storage medium, comprising:

code for causing a computer to forward a first message to a serving network, wherein the first message includes an information element signaling that the computer supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

code for causing a computer to generate at least one session key, in accordance with the first security context, using the information element;

code for causing a computer to receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

code for causing a computer to have wireless communications, in response to the second message, protected by the at least one session key.

23. A computer program product as defined in claim 22, wherein the information element comprises a count value updated for a session.

24. A computer program product as defined in claim 22, wherein the serving network is a UMTS serving network.

25. A computer program product as defined in claim 24, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

26. A computer program product as defined in claim 22, wherein the serving network is a GERAN serving network.

27. A computer program product as defined in claim 22, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the received information element.

CLAIMS

1. A method for establishing a first security context between a remote station and a serving network, the first security context having a security property that is not supported by a second security context, the method including:

the remote station forwarding a first message to the serving network, wherein the first message includes an information element signaling that the remote station supports the first security context;

the remote station generating at least one session key, in accordance with the first security context, using the information element;

the remote station receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and

the remote station, in response to the second message, having wireless communications protected by the at least one session key.

2. A method for establishing a first security context as defined in claim 1, wherein the information element includes a count value updated for a session.

3. A method for establishing a first security context as defined in claim 1 or 2, wherein the serving network is a UMTS serving network.

4. A method for establishing a first security context as defined in claim 3, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

5. A method for establishing a first security context as defined in claim 1 or 2, wherein the serving network is a GERAN serving network.

6. A method for establishing a first security context as defined in any one of claims 1 to 5, wherein the indication that the serving network supports the first security context includes an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

7. A method for establishing a first security context as defined in any one of claims 1 to 6, wherein the remote station includes a mobile user equipment.

8. A remote station, including:

means for forwarding a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

means for generating at least one session key, in accordance with the first security context, using the information element;

means for receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and

means for having wireless communications, in response to the second message, protected by the at least one session key.

9. A remote station as defined in claim 8, wherein the information element includes a count value updated for a session.

10. A remote station as defined in claim 8 or 9, wherein the serving network is a UMTS serving network.

11. A remote station as defined in claim 10, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

12. A remote station as defined in claim 8 or 9, wherein the serving network is a GERAN serving network.

13. A remote station as defined in any one of claims 8 to 12, wherein the indication that the serving network supports the first security context includes an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

14. A remote station as defined in any one of claims 8 to 13, wherein the remote station includes a mobile user equipment.

15. A remote station, including:

a processor configured to:

forward a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

generate at least one session key, in accordance with the first security context, using the information element;

receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

have wireless communications, in response to the second message, protected by the at least one session key.

16. A remote station as defined in claim 15, wherein the information element includes a count value updated for a session.

17. A remote station as defined in claim 15 or 16, wherein the serving network is a UMTS serving network.

18. A remote station as defined in claim 17, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

19. A remote station as defined in claim 15 or 16, wherein the serving network is a GERAN serving network.

20. A remote station as defined in any one of claims 15 to 19, wherein the indication that the serving network supports the first security context includes an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

21. A remote station as defined in any one of claims 15 to 20, wherein the remote station includes a mobile user equipment.

22. A computer program product, including:

computer-readable storage medium, including:

code for causing a computer to forward a first message to a serving network, wherein the first message includes an information element signaling that the computer supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

code for causing a computer to generate at least one session key, in accordance with the first security context, using the information element;

code for causing a computer to receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

code for causing a computer to have wireless communications, in response to the second message, protected by the at least one session key.

23. A computer program product as defined in claim 22, wherein the information element includes a count value updated for a session.

24. A computer program product as defined in claim 22 or 23, wherein the serving network is a UMTS serving network.

25. A computer program product as defined in claim 24, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

26. A computer program product as defined in claim 22 or 23, wherein the serving network is a GERAN serving network.

27. A computer program product as defined in any one of claims 22 to 26, wherein the indication that the serving network supports the first security context includes an authentication code generated based on a corresponding at least one session key generated by the serving network using the received information element.