CLAIMS

WHAT IS CLAIMED IS:

1. A method operational in a device, comprising:

performing subscriber authentication with a network entity;

performing device authentication of the device with the network entity;

generating a security key that binds the subscriber authentication and the device authentication; and

using the security key to secure communications between the device and a serving network.

2. The method of claim 1, wherein subscriber authentication is based on an authentication key agreement exchange between the device and the network entity.

3. The method of claim 1, wherein device authentication is based on a challenge-response exchange between the device and the network entity.

4. The method of claim 1, wherein subscriber authentication is performed by a first authentication server that is part of the network entity, and device authentication is performed by a second authentication server that is part of the network entity.

5. The method of claim 1, wherein device authentication is performed by:

receiving data from the network entity that is encrypted with a public key of the device;

using a corresponding private key to decrypt the encrypted data; and

subsequently proving to the network entity that the device has knowledge of the data.

6. The method of claim 1, further comprising:

sending an attach request from the device to the network entity, the attach request including an indication of device authentication capabilities of the device.

7. The method of claim 1, wherein device authentication is secured by at least one key generated during the subscriber authentication.

8. The method of claim 1, wherein subscriber authentication and device authentication are concurrently performed in combined message exchanges.

9. The method of claim 1, wherein subscriber authentication is performed in an earlier and separate security exchange from the device authentication.

10. The method of claim 1, wherein the security key is generated as a function of at least a first key obtained from subscriber authentication and a second key obtained from device authentication.

11. The method of claim 10, wherein the security key is also a function of a network nonce and a device nonce.

12. The method of claim 1, wherein the device is a relay node that appears as an access terminal to the network entity and appears as a network device to one or more access terminals.

13. The method of claim 1, wherein the security key is separately generated by the device and the network entity.

14. The method of claim 1, further comprising:

provisioning a subscriber-specific key as part of a service agreement, where the subscriber-specific key is used for the subscriber authentication; and

provisioning a device-specific key in the device during manufacturing, where the device-specific key is used for the device authentication.

15. A device, comprising:

a communication interface; and

a processing circuit coupled to the communication interface, the processing circuit adapted to:

perform subscriber authentication with a network entity;

perform device authentication of the device with the network entity;

generate a security key that binds the subscriber authentication and the device authentication; and

use the security key to secure communications between the device and a serving network.

16. The device of claim 15, wherein subscriber authentication is based on an authentication key agreement exchange between the device and the network entity.

17. The device of claim 15, wherein device authentication is based on a challenge-response exchange between the device and the network entity.

18. The device of claim 15, wherein device authentication is performed by:

receiving data from the network entity that is encrypted with a public key of the device;

using a corresponding private key to decrypt the encrypted data; and

subsequently proving to the network entity that the device has knowledge of the data.

19. The device of claim 15, further comprising:

sending an attach request from the device to the network entity, the attach request including an indication of device authentication capabilities of the device.

20. The device of claim 15, wherein device authentication is secured by at least one key generated during the subscriber authentication.

21. The device of claim 15, wherein subscriber authentication and device authentication are concurrently performed in combined message exchanges.

22. The device of claim 15, wherein subscriber authentication is performed in an earlier and separate security exchange from the device authentication.

23. The device of claim 15, wherein the security key is generated as a function of at least a first key obtained from subscriber authentication and a second key obtained from device authentication.

24. The device of claim 15, wherein the device is a relay node that appears as an access terminal to the network entity and appears as a network device to one or more access terminals.

25. The device of claim 15, further comprising:

a removable storage device coupled to the processing circuit and storing a subscriber-specific key used for the subscriber authentication; and

a secure storage device coupled to the processing circuit and storing a device-specific key used for the device authentication.

26. A device, comprising:

means for performing subscriber authentication with a network entity;

means for performing device authentication of the device with the network entity;

means for generating a security key that binds the subscriber authentication and the device authentication; and

means for using the security key to secure communications between the device and a serving network.

27. The device of claim 26, further comprising:

means for storing a subscriber-specific key used for the subscriber authentication; and

means for storing a device-specific key used for the device authentication.

28. A processor-readable medium comprising instructions operational on a device, which when executed by a processor causes the processor to:

perform subscriber authentication with a network entity;

perform device authentication of the device with the network entity;

generate a security key that binds the subscriber authentication and the device authentication; and

use the security key to secure communications between the device and a serving network.

29. A method operational in a network entity, comprising:

performing subscriber authentication with a device;

performing device authentication of the device;

generating a security key that binds the subscriber authentication and the device authentication; and

using the security key to secure communications between the network entity and the device.

30. The method of claim 29, wherein subscriber authentication is based on an authentication key agreement exchange between the network entity and the device.

31. The method of claim 29, wherein device authentication is based on a challenge-response exchange between the network entity and the device.

32. The method of claim 29, wherein device authentication includes:

receiving a certificate from the device;

verifying the certificate associated with the device has not been revoked.

33. The method of claim 29, further comprising:

receiving an attach request from the device, the attach request including an indication of device authentication capabilities of the device.

34. The method of claim 29, wherein device authentication is secured by at least one key generated during the subscriber authentication.

35. The method of claim 29, wherein subscriber authentication and device authentication are concurrently performed in combined message exchanges.

36. The method of claim 29, wherein subscriber authentication is performed in an earlier and separate security exchange from the device authentication.

37. The method of claim 29, wherein the security key is generated as a function of at least a first key obtained from subscriber authentication and a second key obtained from device authentication.

38. The method of claim 29, wherein the security key is separately generated by the device and the network entity.

39. The method of claim 29, further comprising:

obtaining a subscriber-specific key as part of a service agreement, the subscriber-specific key used for the subscriber authentication; and

obtaining a device-specific key for the device, the device-specific key used for the device authentication.

40. A network entity, comprising:

a communication interface; and

a processing circuit coupled to the communication interface, the processing circuit adapted to:

perform subscriber authentication with a device;

perform device authentication of the device;

generate a security key that binds the subscriber authentication and the device authentication; and

use the security key to secure communications between the network entity and the device.

41. The network entity of claim 40, wherein subscriber authentication is based on an authentication key agreement exchange between the network entity and the device.

42. The network entity of claim 40, wherein device authentication is based on a challenge-response exchange between the network entity and the device.

43. The network entity of claim 40, wherein the processing circuit is further adapted to:

receive an attach request from the device, the attach request including an indication of device authentication capabilities of the device.

44. The network entity of claim 40, wherein device authentication is secured by at least one key generated during the subscriber authentication.

45. The network entity of claim 40, wherein subscriber authentication and device authentication are concurrently performed in combined message exchanges.

46. The network entity of claim 40, wherein subscriber authentication is performed in an earlier and separate security exchange from the device authentication.

47. The network entity of claim 40, wherein the security key is generated as a function of at least a first key obtained from subscriber authentication and a second key obtained from device authentication.

48. The network entity of claim 40, further comprising:

obtaining a subscriber-specific key as part of a service agreement, the subscriber-specific key used for the subscriber authentication; and

obtaining a device-specific key for the device, the device-specific key used for the device authentication.

49. A network entity, comprising

means for performing subscriber authentication with a device;

means for performing device authentication of the device;

means for generating a security key that binds the subscriber authentication and the device authentication; and

means for using the security key to secure communications between the network entity and the device.

50. A processor-readable medium comprising instructions operational on a network entity, which when executed by a processor causes the processor to:

perform subscriber authentication with a device;

perform device authentication of the device;

generate a security key that binds the subscriber authentication and the device authentication; and

use the security key to secure communications between the network entity and the device.

CLAIMS

1. A method operational in a device, including:

performing subscriber authentication with a network entity based on a subscriber authentication key;

performing device authentication of the device with the network entity and obtaining device authentication data;

generating a security key based on the subscriber authentication key and the device authentication data that binds the subscriber authentication and the device authentication; and

using the security key to secure communications between the device and a serving network.

2. The method of claim 1, wherein subscriber authentication is based on an authentication key agreement exchange between the device and the network entity.

3. The method of claim 1, wherein device authentication is based on a challenge-response exchange between the device and the network entity.

4. The method of claim 1, wherein subscriber authentication is performed by a first authentication server that is part of the network entity, and device authentication is performed by a second authentication server that is part of the network entity.

5. The method of claim 1, wherein device authentication is performed by:

receiving data from the network entity that is encrypted with a public key of the device;

using a corresponding private key to decrypt the encrypted data; and

subsequently proving to the network entity that the device has knowledge of the data.

6. The method of claim 1, further including:

sending an attach request from the device to the network entity, the attach request including an indication that the device is capable of device authentication .

7. The method of claim 1, wherein device authentication is secured by at least one key generated during the subscriber authentication.

8. The method of claim 1, wherein subscriber authentication and device authentication are concurrently performed in message exchanges in which subscriber authentication and device authentication are combined.

9. The method of claim 1, wherein subscriber authentication is performed in an earlier and separate security exchange from the device authentication.

10. The method of claim 1, wherein the security key is generated as a function of at least a first key obtained from subscriber authentication and a second key obtained from device authentication.

11. The method of claim 10, wherein the security key is also a function of a network nonce and a device nonce.

12. The method of claim 1, wherein the device is a relay node that appears as an access terminal to the network entity and appears as a network device to one or more access terminals.

13. The method of claim 1, wherein the security key is separately generated by the device and the network entity.

14. The method of claim 1, further including:

provisioning a subscriber-specific key as part of a service agreement, where the subscriber-specific key is used for the subscriber authentication; and

provisioning a device-specific key in the device during manufacturing, where the device-specific key is used for the device authentication.

15. A device, including:

a communication interface; and

a processing circuit coupled to the communication interface, the processing circuit adapted to perform a method according to any one of claims 1 to 14.

16. A device, including:

means for performing subscriber authentication with a network entity based on a subscriber authentication key;

means for performing device authentication of the device with the network entity and obtaining device authentication data;

means for generating a security key based on the subscriber authentication key and the device authentication data that binds the subscriber authentication and the device authentication; and

means for using the security key to secure communications between the device and a serving network.

17. The device of claim 16, further including:

means for storing a subscriber-specific key used for the subscriber authentication; and

means for storing a device-specific key used for the device authentication.

18. A method operational in a network entity, including:

performing subscriber authentication with a device based on a subscriber authentication key;

performing device authentication of the device and obtaining device authentication data;

generating a security key based on the subscriber authentication key and the device authentication data that binds the subscriber authentication and the device authentication; and

using the security key to secure communications between the network entity and the device.

19. The method of claim 18, wherein device authentication includes:

receiving a certificate from the device;

verifying the certificate associated with the device has not been revoked.

20. The method of claim 18, further including:

receiving an attach request from the device, the attach request including an indication that the device is capable of device authentication .

21. The method of claim 18, wherein device authentication is secured by at least one key generated during the subscriber authentication.

22. The method of claim 18, wherein subscriber authentication and device authentication are concurrently performed in message exchanges.

23. The method of claim 18, further including:

obtaining a subscriber-specific key as part of a service agreement, the subscriber-specific key used for the subscriber authentication; and

obtaining a device-specific key for the device, the device-specific key used for the device authentication.

24. A network entity, including:

a communication interface; and

a processing circuit coupled to the communication interface, the processing circuit adapted to:

perform subscriber authentication with a device entity based on a subscriber authentication key;

perform device authentication of the device entity and obtain device authentication data;

generate a security key based on the subscriber authentication key and the device authentication data that binds the subscriber authentication and the device authentication; and

use the security key to secure communications between the network entity and the device.

25. The network entity of claim 24, wherein the processing circuit is further adapted to:

receive an attach request from the device, the attach request including an indication of device authentication capabilities of the device.

26. The network entity of claim 24, wherein device authentication is secured by at least one key generated during the subscriber authentication.

27. The network entity of claim 24, wherein subscriber authentication and device authentication are concurrently performed in combined message exchanges.

28. The network entity of claim 24, further including:

obtaining a subscriber-specific key as part of a service agreement, the subscriber-specific key used for the subscriber authentication; and

obtaining a device-specific key for the device, the device-specific key used for the device authentication.

29. A network entity, including:

means for performing subscriber authentication with a device based on a subscriber authentication key;

means for performing device authentication of the device and obtaining device authentication data;

means for generating a security key based on the subscriber authentication key and the device authentication data that binds the subscriber authentication and the device authentication; and

means for using the security key to secure communications between the network entity and the device.

30. A processor-readable medium including instructions operational on a network entity, which when executed by a processor causes the processor to perform a method according to any one of claims 1 to 14 or 18 to 23.