

CLAIMS

What is claimed is:

- 1 1. A method of wireless communication comprising:
2 transmitting a registration message to a network to establish a secure
3 connection for at least non-access stratum (NAS) messages between the network and a
4 wireless device, the secure connection based at least in part on a wireless device identifier
5 and security capabilities of the wireless device included in the registration message; and
6 exchanging NAS messages with the network over the secure connection.
- 1 2. The method of claim 1, wherein exchanging NAS messages comprises:
2 transmitting an attach request to access the network.
- 1 3. The method of claim 2, wherein the attach request is piggybacked to a
2 security mode complete message transmitted to the network.
- 1 4. The method of claim 1, wherein the registration message is an attach
2 request message, a tracking area update (TAU) request message, or a service request
3 message.
- 1 5. The method of claim 1, further comprising:
2 performing, in response to the registration message, a mutual authentication
3 and key agreement with the network; and
4 encrypting subsequent NAS messages based in part on the key agreement
5 established as a result of a successful authentication with the network.
- 1 6. The method of claim 5, further comprising:
2 entering into a deregistered state with the network; and
3 transmitting, while in the deregistered state, an attach request, the attach
4 request being encrypted and integrity protected under the mutual authentication and key
5 agreement.
- 1 7. The method of claim 5, further comprising:
2 entering into a registered state with the network; and
3 transmitting, while in the registered state, the subsequent NAS messages with
4 encryption and integrity protection in accordance with the mutual authentication and key
5 agreement.

1 8. The method of claim 5, further comprising:
2 entering into an idle state with the network; and
3 transmitting, upon exiting the idle state, a service request that includes a first
4 portion of the service request having integrity protection based on a security context
5 established during the successful authentication with the network, and a second portion of the
6 service request having encryption and integrity protection based on the security context.

1 9. The method of claim 8, wherein the first portion includes at least one
2 of the wireless device identifier or a key set identifier.

1 10. The method of claim 5, further comprising:
2 transmitting an attach request, a service request, or a tracking area update
3 (TAU) message;
4 receiving a reject message associated with the transmitted attach request,
5 service request, or TAU message, wherein the reject message is not encrypted or integrity
6 protected based on a security context established during the successful authentication with the
7 network; and
8 transmitting a second registration message to the network to establish security
9 with the network based on the wireless device identifier and security capabilities of the
10 wireless device included in the second registration message.

1 11. The method of claim 10, further comprising:
2 waiting a predetermined amount of time after receiving the reject message;
3 and
4 re-transmitting the previously transmitted attach request, service request, or
5 TAU message prior to transmitting the second registration message.

1 12. The method of claim 5, further comprising:
2 transmitting an attach request, a service request, or a tracking area update
3 (TAU) message;
4 receiving a reject message associated with the transmitted attach request,
5 service request, or TAU message, wherein the reject message is not encrypted or integrity
6 protected based on a security context established during the successful authentication with the
7 network; and
8 transmitting a second registration message to a different network to establish

9 security with the network based on the wireless device identifier and security capabilities of
10 the wireless device included in the second registration message.

1 13. The method of claim 5, wherein performing the mutual authentication
2 and key agreement comprises:
3 communicating between the wireless device and a component of the network
4 that is configured for securing NAS messages.

1 14. The method of claim 1, further comprising:
2 calculating a hash of the registration request;
3 receiving a hash of the registration request from the network subsequent to the
4 transmitted registration message; and
5 determining whether the values of the calculated hash and the received hash
6 match.

1 15. The method of claim 14, further comprising:
2 retransmitting at least one information element contained within the
3 registration message upon determining that the calculated and received hash values do not
4 match.

1 16. The method of claim 14, further comprising:
2 retransmitting the registration message to the network upon determining that
3 the calculated and received hash values do not match.

1 17. A method of wireless communication comprising:
2 receiving a registration message from a wireless device to establish a secure
3 connection for at least non-access stratum (NAS) messages between the wireless device and
4 a network, the secure connection based at least in part on a wireless device identifier and
5 security capabilities of the wireless device included in the registration message; and
6 exchanging NAS messages with the wireless device over the secure
7 connection.

1 18. The method of claim 17, wherein exchanging NAS messages
2 comprises:
3 receiving an attach request from the wireless device to access the network.

1 19. The method of claim 18, wherein the attach request is piggybacked to a
2 security mode complete message transmitted to the network.

1 20. The method of claim 17, wherein the registration message is an attach
2 request message, a tracking area update (TAU) request message, or a service request
3 message.

1 21. The method of claim 17, further comprising:
2 performing, in response to the registration message, a mutual authentication
3 and key agreement with the wireless device; and
4 encrypting subsequent NAS messages based in part on the key agreement
5 established as a result of a successful authentication with the wireless device.

1 22. The method of claim 21, further comprising:
2 receiving an attach request, a service request, or a tracking area update (TAU)
3 message;
4 transmitting a reject message associated with the received attach request,
5 service request, or TAU message, wherein the reject message is not encrypted or integrity
6 protected based on a security context established during the successful authentication with the
7 wireless device; and
8 receiving a second registration message from the wireless device to establish
9 security with the wireless device based on the wireless device identifier and security
10 capabilities of the wireless device included in the second registration message.

1 23. The method of claim 21, wherein performing the mutual authentication
2 and key agreement comprises:
3 communicating between the wireless device and a component of the network
4 that is configured for securing NAS messages.

1 24. The method of claim 17, further comprising:
2 determining a hash of the received registration message in response to a
3 request contained within the registration message; and transmitting the hash to the wireless
4 device.

1 25. An apparatus for wireless communication comprising:
2 means for transmitting a registration message to a network to establish a
3 secure connection for at least non-access stratum (NAS) messages between the network and a

4 wireless device, the secure connection based at least in part on a wireless device identifier
5 and security capabilities of the wireless device included in the registration message; and
6 means for exchanging NAS messages with the network over the secure
7 connection.

1 26. The apparatus of claim 25, wherein the means for exchanging NAS
2 messages comprises:

3 means for transmitting an attach request to access the network.

1 27. The apparatus of claim 26, wherein the attach request is piggybacked
2 to a security mode complete message transmitted to the network.

1 28. The apparatus of claim 25, wherein the registration message is an
2 attach request message, a tracking area update (TAU) request message, or a service request
3 message.

1 29. The apparatus of claim 25, further comprising:

2 means for performing, in response to the registration message, a mutual
3 authentication and key agreement with the network; and

4 means for encrypting subsequent NAS messages based in part on the key
5 agreement established as a result of a successful authentication with the network.

1 30. The apparatus of claim 29, further comprising:

2 means for entering into a deregistered state with the network; and

3 means for transmitting, while in the deregistered state, an attach request, the
4 attach request being encrypted and integrity protected under the mutual authentication and
5 key agreement.

1 31. The apparatus of claim 29, further comprising:

2 means for entering into a registered state with the network; and

3 means for transmitting, while in the registered state, the subsequent NAS
4 messages with encryption and integrity protection in accordance with the mutual
5 authentication and key agreement.

1 32. The apparatus of claim 29, further comprising:

2 means for entering into an idle state with the network; and

3 means for transmitting, upon exiting the idle state, a service request that
4 includes a first portion of the service request having integrity protection based on a security

5 context established during the successful authentication with the network, and a second
6 portion of the service request having encryption and integrity protection based on the security
7 context.

1 33. The apparatus of claim 32, wherein the first portion includes at least
2 one of the wireless device identifier or a key set identifier.

1 34. The apparatus of claim 29, further comprising:
2 means for transmitting an attach request, a service request, or a tracking area
3 update (TAU) message;

4 means for receiving a reject message associated with the transmitted attach
5 request, service request, or TAU message, wherein the reject message is not encrypted or
6 integrity protected based on a security context established during the successful
7 authentication with the network; and

8 means for transmitting a second registration message to the network to
9 establish security with the network based on the wireless device identifier and security
10 capabilities of the wireless device included in the second registration message.

1 35. The apparatus of claim 34, further comprising:
2 means for waiting a predetermined amount of time after receiving the reject
3 message; and

4 means for re-transmitting the previously transmitted attach request, service
5 request, or TAU message prior to transmitting the second registration message.

1 36. The apparatus of claim 29, further comprising:
2 means for transmitting an attach request, a service request, or a tracking area
3 update (TAU) message;

4 means for receiving a reject message associated with the transmitted attach
5 request, service request, or TAU message, wherein the reject message is not encrypted or
6 integrity protected based on a security context established during the successful
7 authentication with the network; and

8 means for transmitting a second registration message to a different network to
9 establish security with the network based on the wireless device identifier and security
10 capabilities of the wireless device included in the second registration message.

1 37. The apparatus of claim 29, wherein the means for performing the
2 mutual authentication and key agreement comprises:

3 means for communicating between the wireless device and a component of the
4 network that is configured for securing NAS messages.

1 38. The apparatus of claim 25, further comprising:
2 means for calculating a hash of the registration request;
3 means for receiving a hash of the registration request from the network
4 subsequent to the transmitted registration message; and
5 means for determining whether the values of the calculated hash and the
6 received hash match.

1 39. The apparatus of claim 38, further comprising:
2 means for retransmitting at least one information element contained within the
3 registration message upon determining that the calculated and received hash values do not
4 match.

1 40. The apparatus of claim 38, further comprising:
2 means for retransmitting the registration message to the network upon
3 determining that the calculated and received hash values do not match.

1 41. An apparatus for wireless communication comprising:
2 means for receiving a registration message from a device to establish a secure
3 connection for at least non-access stratum (NAS) messages between the wireless device and
4 a network, the secure connection based at least in part on a wireless device identifier and
5 security capabilities of the wireless device included in the registration message; and
6 means for exchanging NAS messages with the wireless device over the secure
7 connection.

1 42. The apparatus of claim 41, wherein the means for exchanging NAS
2 messages comprises:
3 means for receiving an attach request from the wireless device to access the
4 network.

1 43. The apparatus of claim 42, wherein the attach request is piggybacked
2 to a security mode complete message transmitted to the network.

1 44. The apparatus of claim 41, wherein the registration message is an
2 attach request message, a tracking area update (TAU) request message, or a service request
3 message.

1 45. The apparatus of claim 41, further comprising:
2 means for performing, in response to the registration message, a mutual
3 authentication and key agreement with the wireless device; and
4 means for encrypting subsequent NAS messages based in part on the key
5 agreement established as a result of a successful authentication with the wireless device.

1 46. The apparatus of claim 45, further comprising:
2 means for receiving an attach request, a service request, or a tracking area
3 update (TAU) message;
4 means for transmitting a reject message associated with the received attach
5 request, service request, or TAU message, wherein the reject message is not encrypted or
6 integrity protected based on a security context established during the successful
7 authentication with the wireless device; and
8 means for receiving a second registration message from the wireless device to
9 establish security with the wireless device based on the wireless device identifier and
10 security capabilities of the wireless device included in the second registration message.

1 47. The apparatus of claim 45, wherein the means for performing the
2 mutual authentication and key agreement comprises:
3 means for communicating between the wireless device and a component of
4 the network that is configured for securing NAS messages.

1 48. The apparatus of claim 41, further comprising:
2 means for determining a hash of the received registration message in response
3 to a request contained within the registration message; and transmitting the hash to the
4 wireless device.

1 49. An apparatus for wireless communication, comprising:
2 a processor;
3 memory in electronic communication with the processor; and
4 instructions stored in the memory and operable, when executed by the
5 processor, to cause the apparatus to:

6 transmit a registration message to a network to establish a secure connection
7 for at least non-access stratum (NAS) messages between the network and a wireless device,
8 the secure connection based at least in part on a wireless device identifier and security
9 capabilities of the wireless device included in the registration message; and
10 exchange NAS messages with the network over the secure connection.

1 50. The apparatus of claim 49, wherein the instructions operable to cause
2 the apparatus to exchange NAS messages comprise instructions operable to cause the
3 apparatus to:

4 transmit an attach request to access the network.

1 51. The apparatus of claim 50, wherein the attach request is piggybacked
2 to a security mode complete message transmitted to the network.

1 52. The apparatus of claim 49, wherein the registration message is an
2 attach request message, a tracking area update (TAU) request message, or a service request
3 message.

1 53. The apparatus of claim 49, wherein the instructions are operable to
2 cause the processor to:
3 perform, in response to the registration message, a mutual authentication and
4 key agreement with the network; and
5 encrypt subsequent NAS messages based in part on the key agreement
6 established as a result of a successful authentication with the network.

1 54. The apparatus of claim 53, wherein the instructions are operable to
2 cause the processor to:
3 enter into a deregistered state with the network; and
4 transmit, while in the deregistered state, an attach request, the attach request
5 being encrypted and integrity protected under the mutual authentication and key agreement.

1 55. The apparatus of claim 53, wherein the instructions are operable to
2 cause the processor to:
3 enter into a registered state with the network; and
4 transmit, while in the registered state, the subsequent NAS messages with
5 encryption and integrity protection in accordance with the mutual authentication and key
6 agreement.

1 56. The apparatus of claim 53, wherein the instructions are operable to
2 cause the processor to:
3 enter into an idle state with the network; and
4 transmit, upon exiting the idle state, a service request that includes a first
5 portion of the service request having integrity protection based on a security context
6 established during the successful authentication with the network, and a second portion of the
7 service request having encryption and integrity protection based on the security context.

1 57. The apparatus of claim 56, wherein the first portion includes at least
2 one of the wireless device identifier or a key set identifier.

1 58. The apparatus of claim 53, wherein the instructions are operable to
2 cause the processor to:
3 transmit an attach request, a service request, or a tracking area update (TAU)
4 message;
5 receive a reject message associated with the transmitted attach request, service
6 request, or TAU message, wherein the reject message is not encrypted or integrity protected
7 based on a security context established during the successful authentication with the network;
8 and
9 transmit a second registration message to the network to establish security
10 with the network based on the wireless device identifier and security capabilities of the
11 wireless device included in the second registration message.

1 59. The apparatus of claim 58, wherein the instructions are operable to
2 cause the processor to:
3 wait a predetermined amount of time after receiving the reject message; and
4 re-transmit the previously transmitted attach request, service request, or TAU
5 message prior to transmitting the second registration message.

1 60. The apparatus of claim 53, wherein the instructions are operable to
2 cause the processor to:
3 transmit an attach request, a service request, or a tracking area update (TAU)
4 message;
5 receive a reject message associated with the transmitted attach request, service
6 request, or TAU message, wherein the reject message is not encrypted or integrity protected
7 based on a security context established during the successful authentication with the network;

8 and

9 transmit a second registration message to a different network to establish
10 security with the network based on the wireless device identifier and security capabilities of
11 the wireless device included in the second registration message.

1 61. The apparatus of claim 53, wherein the instructions operable to cause
2 the apparatus to perform the mutual authentication and key agreement comprise instructions
3 operable to cause the apparatus to:

4 communicate between the wireless device and a component of the network
5 that is configured for securing NAS messages.

1 62. The apparatus of claim 49, wherein the instructions are operable to
2 cause the processor to:

3 calculate a hash of the registration request;

4 receive a hash of the registration request from the network subsequent to the
5 transmitted registration message; and

6 determine whether the values of the calculated hash and the received hash
7 match.

1 63. The apparatus of claim 62, wherein the instructions are operable to
2 cause the processor to:

3 retransmit at least one information element contained within the registration
4 message upon determining that the calculated and received hash values do not match.

1 64. The apparatus of claim 62, wherein the instructions are operable to
2 cause the processor to:

3 retransmit the registration message to the network upon determining that the
4 calculated and received hash values do not match.

1 65. An apparatus for wireless communication, comprising:

2 a processor;

3 memory in electronic communication with the processor; and

4 instructions stored in the memory and operable, when executed by the
5 processor, to cause the apparatus to:

6 receive a registration message from a wireless device to establish a secure
7 connection for at least non-access stratum (NAS) messages between the wireless device and

8 a network, the secure connection based at least in part on a wireless device identifier and
9 security capabilities of the wireless device included in the registration message; and
10 exchange NAS messages with the wireless device over the secure connection.

1 66. The apparatus of claim 65, wherein the instructions operable to cause
2 the apparatus to exchange NAS messages comprise instructions operable to cause the
3 apparatus to:
4 receive an attach request from the wireless device to access the network.

1 67. The apparatus of claim 66, wherein the attach request is piggybacked
2 to a security mode complete message transmitted to the network.

1 68. The apparatus of claim 65 wherein the registration message is an attach
2 request message, a tracking area update (TAU) request message, or a service request
3 message.

1 69. The apparatus of claim 65, wherein the instructions are operable to
2 cause the processor to:
3 perform, in response to the registration message, a mutual authentication and
4 key agreement with the wireless device; and
5 encrypt subsequent NAS messages based in part on the key agreement
6 established as a result of a successful authentication with the wireless device.

1 70. The apparatus of claim 69, wherein the instructions are operable to
2 cause the processor to:
3 receive an attach request, a service request, or a tracking area update (TAU)
4 message;
5 transmit a reject message associated with the received attach request, service
6 request, or TAU message, wherein the reject message is not encrypted or integrity protected
7 based on a security context established during the successful authentication with the wireless
8 device; and
9 receive a second registration message from the wireless device to establish
10 security with the wireless device based on the wireless device identifier and security
11 capabilities of the wireless device included in the second registration message.

1 71. The apparatus of claim 69, wherein the instructions operable to cause
2 the apparatus to perform the mutual authentication and key agreement comprise instructions
3 operable to cause the apparatus to:

4 communicate between the wireless device and a component of the network
5 that is configured for securing NAS messages.

1 72. The apparatus of claim 71, wherein the instructions are operable to
2 cause the processor to:

3 determine a hash of the received registration message in response to a request
4 contained within the registration message; and

5 transmit the hash to the wireless device.