CLAIMS

We claim:

1. A short messaging service (SMS) system configured for secure communications, said SMS system comprising:

a software module configured for use on a mobile device, wherein the software module is configured to encrypt an SMS message via a first encryption; and

a gateway configured to communicate with the mobile device, wherein the gateway is configured to receive the encrypted SMS message from the mobile device.

2. The system of claim 1, wherein the gateway is configured to decrypt the encrypted SMS message received from the mobile device.

3. The system of claim 2, wherein the gateway is configured to re-encrypt the decrypted SMS message via a second encryption.

4. The system of claim 3, wherein the first encryption and the second encryption are different.

5. The system of claim 4, wherein the gateway is configured to transmit the re-encrypted SMS message to a mobile device.

6. A method of securing short messaging service (SMS) communications, the method comprising:

encrypting, at a mobile device, an SMS message;

transmitting the encrypted SMS message to a gateway;

decrypting, at the gateway, the encrypted SMS message;

re-encrypting, at the gateway, the decrypted SMS message; and

transmitting the re-encrypted SMS message to a recipient.

7. The method of claim 6, wherein the message is encrypted at a mobile device via a first encryption, and wherein the decrypted message is re-encrypted at the gateway via a second encryption different from the first encryption.

8. The method of claim 6, further comprising transmitting, to a mobile device, a delivery confirmation responsive to delivery of the re-encrypted SMS message to a recipient.

9. The method of claim 6, further comprising transmitting, to a mobile device, an open confirmation responsive to the re-encrypted SMS message being accessed by a recipient.

10. The method of claim 6, wherein, at the mobile device, information identifying the recipient of the message is encrypted with the message.

11. The method of claim 10, wherein the decrypting, at the gateway, further comprises determining a recipient of the encrypted message.

12. The method of claim 6, further comprising dividing, at the mobile device, the encrypted message into at least two encrypted sub-messages, wherein the at least two encrypted sub-messages are configured according to an SMS protocol for transmittal to the gateway.

13. The method of claim 12, further comprising assembling, at the gateway, the at least two encrypted sub-messages to reconstitute the encrypted message.

14. The method of claim 6, further comprising updating, at the mobile device, an encryption key associated with the mobile device, wherein the updating is responsive to a key update command transmitted by the gateway.

15. The method of claim 14, further comprising queuing, at the gateway, at least one message associated with the mobile device, wherein the queuing is responsive to a key update command transmitted by the gateway.

16. The method of claim 15, further comprising processing, at the gateway, the at least one queued message, wherein the processing is responsive to a key change acknowledgement message transmitted from the mobile device to the gateway.

18. A communication system for securely delivering a message to a mobile device, the system comprising:

a first software module configured as a gateway, wherein the first software module is configured to encrypt at least one of a short messaging service (SMS) message or a multimedia messaging service (MMS) message for delivery to the mobile device; and

a second software module configured for use on the mobile device, wherein the second software module is further configured to decrypt at least one of the encrypted SMS message or the encrypted MMS message received from the first software module, and wherein the information in at least one of the encrypted SMS message or the encrypted MMS message was received at the first software module from a third party.

19. The system of claim 18, wherein the second software module comprises an encrypted address book.

20. The system of claim 18, wherein the second software module is configured to be locked after a period of inactivity.

21. The system of claim 18, wherein access to the second software module is protected by a password.

22. The system of claim 18, wherein the second software module is configured to delete at least one item of information, wherein the deletion is responsive to a selected number of failed authentication attempts.

23. A method of securely delivering a message to a mobile device, the method comprising:

dividing the message into at least two sub-messages, wherein the at least two sub-messages are configured according to at least one of a short messaging service (SMS) protocol or a multimedia messaging service (MMS protocol);

encrypting the at least two sub-messages;

transmitting the at least two encrypted sub-messages to a mobile device according to at least one of an SMS protocol or a MMS protocol;

decrypting, at the mobile device, the at least two encrypted sub-messages; and

combining, at the mobile device, the at least two decrypted sub-messages to form the message.

24. A method of securely delivering a message to a mobile device, the method comprising:

encrypting the message;

dividing the encrypted message into at least two sub-messages;

transmitting the at least two sub-messages to a mobile device according to at least one of an SMS protocol or an MMS protocol;

combining, at the mobile device, the at least two sub-messages to form an encrypted message; and

decrypting, at the mobile device, the encrypted message.

25. A method of deleting information on a mobile device, comprising:

transmitting, to a mobile device, an encrypted short messaging service (SMS) message comprising a wipe instruction; and

deleting, at the mobile device, at least one item of information responsive to the wipe instruction.

26. The method of claim 25, further comprising transmitting, from the mobile device, a message confirming deletion of the at least one item of information.

27. The method of claim 25, wherein the at least one item of information is a database of at least one of SMS messages or MMS messages.

CLAIMS

1. A short messaging service (SMS) system or multimedia messaging service (MMS) system configured for secure communications, the system comprising:

a software module configured to run as a user application on a mobile device, wherein the software module can be protected by at least one of a password and biometric and wherein the software module is configured to encrypt an SMS or MMS message via a first encryption on the mobile device; and

a gateway configured to communicate with the mobile device, wherein the

gateway is configured to receive the encrypted SMS or MMS message from the mobile device.

2. The system of claim 1, wherein the gateway is configured to decrypt the encrypted SMS or MMS message received from the mobile device.

3. The system of claim 2, wherein the gateway is configured to re-encrypt the decrypted SMS or MMS message via a second encryption.

4. The system of claim 3, wherein the first encryption and the second encryption are different.

5. The system of claim 4, wherein the gateway is configured to transmit the re-encrypted SMS or MMS message to a mobile device.

6. A method of securing short messaging service (SMS) or multimedia messaging service (MMS) communications, the method comprising:

encrypting, at a mobile device at a user application that is configured to run on the mobile device and that can be protected by at least one of a password and biometric, an SMS or MMS message;

transmitting the encrypted SMS or MMS message to a gateway;

decrypting, at the gateway, the encrypted SMS or MMS message;

re-encrypting, at the gateway, the decrypted SMS or MMS message; and

transmitting the re-encrypted SMS or MMS message to a recipient.

7. The method of claim 6, wherein the message is encrypted at a mobile device via a first encryption, and wherein the decrypted message is re-encrypted at the gateway via a second encryption different from the first encryption.

8. The method of claim 6, further comprising transmitting, to a mobile device, a delivery confirmation responsive to delivery of the re-encrypted SMS or MMS message to a recipient.

9. The method of claim 6, further comprising transmitting, to a mobile device, an open confirmation responsive to the re-encrypted SMS or MMS message being accessed by a recipient.

10. The method of claim 6, wherein, at the mobile device, information identifying the recipient of the message is encrypted with the message.

11. The method of claim 10, wherein the decrypting, at the gateway, further comprises determining a recipient of the encrypted message.

12. The method of claim 6, further comprising updating, at the mobile device, an encryption key associated with the mobile device, wherein the updating is responsive to a key update command transmitted by the gateway.

13. The method of claim 12, further comprising queuing, at the gateway, at least one message associated with the mobile device, wherein the queuing is responsive to a key update command transmitted by the gateway.

14. The method of claim 13, further comprising processing, at the gateway, the at least one queued message, wherein the processing is responsive to a key change acknowledgement message transmitted from the mobile device to the gateway.

15. A communication system for securely delivering a message to a mobile device, the system comprising:

a first software module configured as a gateway, wherein the first software module is configured to encrypt at least one of a short messaging service (SMS) message or a multimedia messaging service (MMS) message for delivery to the mobile device;

and

a second software module configured to run as a user application on a mobile device, wherein the second software module is further configured to decrypt the encrypted message received from the first software module, and wherein the information in the encrypted message received at the first software module was provided to the first software module via a method other than SMS.

16. The system of claim 15, wherein the second software module comprises an encrypted address book.

17. The system of claim 15, wherein the second software module is configured to be locked after a period of inactivity.

18. The system of claim 15, wherein access to the second software module is protected by a password.

19. The system of claim 15, wherein the second software module is configured to delete at least one item of information, wherein the deletion is responsive to a selected number of failed authentication attempts.

20. A method of deleting information on a mobile device, comprising: transmitting, to a mobile device, an encrypted short messaging service (SMS) message comprising a wipe instruction; and

deleting, at the mobile device, at least one item of information responsive to the wipe instruction.

21. The method of claim 20, further comprising transmitting, from the mobile device, a message confirming deletion of the at least one item of information.

22. The method of claim 20, wherein the at least one item of information is a database of at least one of SMS messages or MMS messages.

23. The system of claim 3, wherein the gateway is configured to transmit the re-encrypted SMS or MMS message to two or more mobile devices.

24. The system of claim 23 wherein the gateway is configured to re-encrypt the at least one of the SMS message or the MMS message using a different encryption for each of at least two of the two or more mobile devices.

25. The method of claim 6 wherein the step of transmitting the re-encrypted SMS or MMS message to a recipient comprises transmitting the re-encrypted message to two or more mobile devices.

26. The method of claim 25 wherein the re-encrypted message is re-encrypted using a different encryption for each of at least two of the two or more mobile devices.

27. The system of claim 15, wherein the first software module is configured to encrypt at least one of a short messaging service (SMS) message or a multimedia messaging service (MMS) message for delivery to two or more mobile devices.

28. The system of claim 27, wherein the first software module is configured to encrypt the at least one of the SMS message or the MMS message using a different encryption for each of at least two of the two or more mobile devices.

29. The system of claim 15, wherein the third party comprises a server.

30. A method for allowing third parties or data provider to communicate with customers. The method comprising in any order:

configuring a first software module on a server; and

configuring a second software module on a mobile device wherein the second software module is capable of communicating with the first software module via an encrypted short messaging service (SMS) or multimedia messaging service (MMS);

wherein the first software module on the server can route a communication between the second software module on mobile device and a third party capable of communicating with the first software module on the server via an Internet protocol.

31. A method of claim 30 wherein the second software module is downloaded onto the mobile device via at least one of the Internet and a mobile network.

32. A method of claim 30 wherein the communication between the second software module on mobile device and the third party comprises a message that requires immediate action.

33. A method of claim 32 the communication between the second software module on mobile device and the third party comprises priority notification.