

CLAIMS

1. A method for transmitting ~~a an encrypted message, received from a sender computer,~~ from a messaging server to a handset comprising the steps:

receiving, at the messaging server and from the sender computer, a message to be sent to the handset and a handset identifier associated with the handset, the handset identifier being a public network address ~~from a sender computer;~~

in response to receiving the message from the sender computer, determining that the handset is not registered with the messaging server;

facilitating the registration of the handset by:

sending, from the messaging server, a notification to the handset requesting registration using the public network address of the handset identifier;

receiving, from the handset, a handset encryption key associated with the handset identifier; and

storing the handset encryption key against the handset identifier at the messaging server; and

encrypting the ~~received message~~ received from the sender computer using the handset encryption key and sending the encrypted message to the handset.

2. A method as claimed in claim 1 wherein determining that the handset is not registered comprises determining that the handset identifier does not have an associated handset encryption key stored at the messaging server.

3. A method as claimed in claim 1 or claim 2 further comprising performing intermediate encryption of the message to create an intermediate encrypted message and storing the intermediate encrypted message at the messaging server.

4. A method as claimed in claim 3 wherein the intermediate encryption uses a messaging server encryption key.

5. A method as claim in claim 3 or claim 4 wherein the method further comprises decrypting the intermediate encrypted message before encrypting the message with the handset encryption key.

6. A method as claimed in any one of claims 1 to 5 wherein the step of facilitating the registration of the handset further comprises, at the messaging server, authenticating the handset prior to accepting from the handset the received handset encryption key.

7. A method as claimed in any one of claims 1 to 6 wherein the encryption key is generated by a handset application installed on or native to the handset.

8. A method as claimed in claim 7 wherein the encryption key is a public key generated during asymmetric key generation by the handset application and wherein the handset application also generates a private key, which is stored in the handset application on the handset and used to decrypt the encrypted message after receipt thereof.

9. A method as claimed in claim 8 wherein the asymmetric keys are generated by a random number generator of the handset application, seeded by the handset's identifier.

10. A method as claimed in ~~any one of claims 1 to 9~~ 6 wherein the step of authenticating the handset comprises:

providing a temporary password to the handset;

receiving a return password back from the handset; and

comparing the temporary password and the return password thereby to authenticate the handset.

11. A method as claimed in claim 10 wherein different communication channels are used for providing the temporary password to the handset and receiving the return password back from the handset.

12. A method as claimed in claim 11 wherein the temporary password is sent to the handset as part of an SMS, while the return password is received from the handset using a public mobile network supporting data communication.

13. A method as claimed in any one of claims 10 to 12 wherein the step of comparing the passwords further comprises comparing a handset identifier received with the return password, with the handset identifier to which the temporary password was sent.

14. A method as claimed in ~~any one of claims 61 to 9~~ wherein the step of authenticating the handset comprises:

receiving a first temporary password from the handset;

receiving a second temporary password from the handset; and

comparing the two temporary passwords thereby to authenticate the handset.

15. A method as claimed in claim 14 wherein different communication channels are used for receiving the first and second temporary password from the handset, with the one channel being a public mobile network supporting data communication and the other channel being an SMS channel.

16. A method as claimed in claim 15 wherein the first temporary password is automatically transmitted over a public mobile network supporting data communication from the handset once it has been generated by the handset application program, and is transmitted with the handset identifier entered by the user through the handset application.

17. A method as claimed in claim 16 wherein the second temporary password is obtained along with the handset identifier as an SMS sent to the messaging server from the handset application, the SMS being sent automatically, without user interaction, from the handset application.

18. A computer system comprising:

a memory with instructions for performing the steps of the method as claimed in any one of claims 1 to 17; and

a processor configured to execute the instructions.

~~19. A method for registering a handset to enable the secure sending of a message to the handset, the method comprising the steps:~~

generating, at the messaging server, a temporary password;

transmitting the temporary password to the handset;

~~receiving a return password back from the handset; comparing the temporary password with the return password;~~

~~in the event that they match, transmitting an authentication acknowledgement back to the handset; and~~

~~receiving a handset encryption key from the handset which is stored at the messaging server against an identification number of the handset.~~

20. — A method for registering a handset to enable the secure sending of a message to the handset, the method comprising the steps:

~~receiving, at the messaging server, a first temporary password from the handset through a public mobile network supporting data communication;~~

~~receiving a second temporary password from the handset as part of an SMS;~~

~~comparing the first and second temporary passwords with each other;~~

~~in the event of a match, transmitting an authentication acknowledgement back to the handset; and~~

~~receiving a handset encryption key from the handset which is stored at the messaging server against an identification number of the handset.~~

2419. A method for sending a secure message from a sender computer to a handset via a messaging server~~for transmitting an encrypted message from a messaging server to a handset~~ comprising the steps:

receiving, at the messaging server and from the sender computer, a message to be sent to the handset and a handset identifier associated with the handset~~from a sender computer~~;

in response to receiving the message from the sender computer, determining that the handset is not registered with the messaging server by determining that the handset identifier does not have an associated handset encryption key stored at the messaging server;

performing intermediate encryption of the message to create an intermediate encrypted message and storing the intermediate encrypted message at the messaging server;

facilitating the registration of the handset by sending, from the messaging server, a notification to the handset requesting registration using the handset identifier as a public network address;

~~after registration,~~ obtaining a handset encryption key from the handset;

decrypting the stored intermediate encrypted message; and

encrypting the message with the handset encryption key prior to sending the encrypted message to the handset.