

Secure Short Message Service

Field of the Invention

[0001] The present invention relates to short message service (SMS). In particular, the invention relates to a system and method for transmitting secured SMS message between two communication devices.

Background

[0002] Short Messaging Service (SMS) is one of the most used features of mobile phones, which allow communications to be carried out in text form. SMS messages are sent from a device to another via a communication network formed by a group of service providers. The SMS messages are not only stored on the sender and recipient devices, but they are also stored as a “copy” at the service providers’ side.

[0003] The SMS messages generally are transmitted with little or no protection along the transmission route. In many cases, these SMS messages can easily be stolen by those who can access to the locations where the messages are stored or even from the air where the SMS messages are transmitted. The lack of security in SMS messages generally discourages users to transmit personal information through SMS.

Summary

[0004] The present invention provides a method for transmitting SMS message from a sender device to a recipient device. The SMS message is encrypted before transmission. Upon receiving the encrypted SMS, the recipient performs a multiple-validation process. In the multiple-validation process, sender and recipient identities are validated and the encryption is validated.

[0005] In accordance with one aspect, there is provided a method for transmitting an encrypted SMS message composed on a sender device under a secure mode to a recipient device. The method comprises receiving the encrypted SMS

message on the recipient device; validating a presence of a compatible platform; validating a cryptography key; validating an identity of user of the recipient device; validating encryption of the encrypted SMS message; and decrypting the SMS message to show text readable to the user.

[0006] In accordance with one embodiment, the method may further comprise discarding the SMS message if any one of the validating steps fails.

[0007] In yet another embodiment, validating the identity of user of the recipient device includes verifying biometric data of the user or matching a password.

[0008] In another embodiment, the cryptography key be a public key or a private key.

[0009] In yet another embodiment, the method may comprise restoring the SMS message to the encrypted SMS message for storing on the recipient device.

[0010] In another aspect, there is provided a system for composing and transmitting an encrypted SMS message, the system comprising a platform operable to perform the aforesaid method.

Brief Description of the Drawings

[0011] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0012] **FIG. 1** illustrates method for transmitting a SMS message between a sender device and a recipient device in accordance with an embodiment of the present invention; and

[0013] **FIG. 2** is a diagram showing a data validation flow between a sender device and a recipient device in accordance with another embodiment of the present invention.

Detailed Description

[0014] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0015] The present invention provides a secured SMS message transmission between a secured sender device and one or more secured recipient device. The sender and recipient devices are communication devices that are able to communicate with each other according to industrial standard protocols of the communication channels. The sender and recipient devices are adapted to provide additional security features over the standard communication protocol for protecting SMS messages sent between the sender and recipient devices. In normal operating mode, the sender and recipient devices are operated as the general communication devices and the SMS messages are sent according to the standard communication protocols, such as GSM protocols. When the sender device is switched to a secured mode, all SMS messages composed by the sender device are added with additional security features where the recipient device required having the associated security features to receive the SMS messages. The SMS can still be sending over the standard communication protocols under the secured mode. As a result of the additional security features, the SMS message transmission provides the following advantages: the SMS message can be created by the intended sender; the SMS message is encrypted for transmission; the SMS message only reaches the intended recipient; and the SMS message is opened by the intended recipient.

[0016] **FIG. 1** illustrates a method for transmitting an SMS message for transmission in accordance with one embodiment of the present invention. The method for transmitting the SMS message starts from a sender end and ends with a recipient end. At the sender end, the method comprises activating a secured mode in step **100**; composing the SMS message in step **102**, encrypting the SMS message in step **104** and

transmitting the SMS message in step **106**. Optionally, the method may further comprise verifying user identity **108**. At start, the user needs to activate the secure mode for composing and transmitting the SMS message in step **100**. In the step **102**, the SMS message is composed with the secured sender device with the standard SMS application provided by the sender device. Once the SMS message is composed, it is encrypted with a prescribed encryption algorithm in the step **104** and subsequently sent out in the step **106**. A public key can be included in the encrypted SMS message. Before sending the SMS message, the secured sender device may prompt to verify the composer identity in the step **108**. The composer verification can be carried out between the steps **102** to **108**. When desired, the secured sender device can be adapted to perform the composer verification when the secure mode is activated. Such verification is to ensure that the composer is a rightful user to the secured sender device. There may be many ways of verifying the composer identity, for example, by password verification, biometric verification and etc.

[0017] Still referring to **FIG. 1**, after the SMS message is sent from the sender device and reached the recipient device(s), i.e. at the recipient end, the recipient device(s) performs a security validation before opening the SMS message. The security validation not only ensures that the SMS message is transmitted to an intended recipient, it also ensure that only the intended recipient is able to read the SMS message, thus achieving a higher level of trust and confidence between sender and recipient. At the recipient end, the method of transmitting the SMS message comprises: receiving the encrypted SMS message in step **110**; performing a first validation in step **112**; performing a second validation in step **114**; performing a third validation in step **116**; performing a fourth validation in step **118**; and reading the SMS message in step **120**. In the step **110**, when the recipient device receives the SMS message, it shall perform a check to determine if the SMS message is encrypted in accordance with the present invention. If the received SMS message is an ordinary SMS message, the recipient device simply prompts the user to read the SMS message as other SMS messages. When the SMS message is determined to be an encrypted SMS message in accordance with the present invention, the recipient device activates a secure mode to open the encrypted SMS message. In the step **112**, the first validation is carried out to check against the presence of appropriate device processor and/or

platform for rendering the encrypted SMS message. The secured SMS message requires a compatible device processor and/or platform to decode and parse the text contain in the encrypted SMS message. Further, the device processor and/or platform is adapted to prevent the encrypted SMS message be copied or duplicated to other device without the compatible processor and/or platform. The first validation prevents other from extracting the encrypted SMS message through other devices. In the step 114, the second validation is carried out to validate a public key and a private key in accordance with the known key infrastructure used in the transmitting messages. The second validation provides another layer of protections to the encrypted SMS message. The public key is used to ensure that the encrypted SMS message is sent to the right recipient with a valid private key to open the encrypted SMS message. In the even that the encrypted SMS message is being duplicated to other device, the others cannot decrypt the SMS message without the private key. In the step 116, the third validation is carried out to verify the rightfulness of the user of the recipient device. The third validation may include password verifications, biometric verification or the like. Such verification is ensured that the user operating the recipient device is the rightful owner to read the SMS message. In the step 118, the fourth validation is carried out to decrypt the encrypted SMS message. It is understood that the decryption requires a corresponding algorithm to decrypt the encrypted SMS message. Once the SMS message is decrypted successfully, the SMS message can be read accordingly in the step 120. If any of the above validation processes 112 to 118 fails due to any doubt on data ownership and data originality, the SMS message is discarded.

[0018] FIG. 2 is a diagram showing a validation flow between a sender device and a recipient device in accordance with another embodiment of the present invention. Once an SMS message is composed on the sender device, the sender device sends a request to the recipient device to verify if the recipient device has an appropriate platform to receive the SMS message. If the recipient device is equipped with the appropriate platform, the recipient device responds to the sender device to affirm the presence of the appropriate platform. Meanwhile, the recipient device also sets itself into a secure mode and awaits the arrival of the SMS message. When the sender device receives the response, the composed SMS message is encrypted on the sender device and sent to the recipient device via an appropriate communication channel. When the

recipient device receives the encrypted SMS message, the recipient device decrypts the SMS message. If the platform validation fails, i.e. the recipient device does not equipped with the same or compatible platform, the SMS message will not be sent.

[0019] Still referring to **FIG. 2**, the platform of the present invention relates to an instrument provided for handling secured transmissions at the sender and recipient ends. It can be any of a dedicated security processor for the mobile communication device, a secured platform/operating system, a relevant validation processor and the combinations thereof. The platform can be a hardware based or software based platform.

[0020] It is understood that when the SMS message is transmitted from the sender end to the recipient end, it may be sent through a common communications channel, with or without any security protection.

[0021] In accordance with the present invention, the sender and the recipient devices may provide additional features to enhance the privacy and security of the SMS transmission. In one embodiment, the sender device can be configured to hide sender identify automatically. In another embodiment, the devices include a black listed sender for blocking SMS messages from the black listed sender.

[0022] In yet another embodiment, the devices can be configured to delete SMS automatically at a prescribed time or period. For example, the sender can set the valid period for the SMS message, and if such validity period is defined, the recipient device will delete the SMS message upon expiry of prescribed period.

[0023] In yet another embodiment, the recipient device can be configured to have all SMS messages stored on the device remains encrypted at all time. Thus, the SMS message cannot be viewed properly the normal operating mode. To view the SMS message, the device has to be switched to a secure mode and one or more of the validation processes described above are executed to decrypt the SMS message for viewing.

[0024] In yet another embodiment, the SMS messages can be configured to be invisible under the normal operating mode, and it is only shown under the secure mode. That protects the privacy of the rightful device owner as the device may only allow the rightful owner to activate the secure mode.

[0025] In yet another embodiment, the SMS messages may be SIM lock SMS where the SMS message will be rendered unreadable with a different SIM card on the device.

[0026] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A method for transmitting an encrypted SMS message composed on a sender device under a secure mode to a recipient device, the method comprising:
 - receiving the encrypted SMS message on the recipient device;
 - validating a presence of a compatible platform;
 - validating a cryptography key;
 - validating an identity of user of the recipient device;
 - validating encryption of the encrypted SMS message; and
 - decrypting the SMS message to show text readable to the user.
2. The method according to claim 1, further comprising discarding the SMS message if any one of the validating steps fails.
3. The method according to claim 1, wherein validating the identity of user of the recipient device includes verifying biometric data of the user.
4. The method according to claim 1, wherein validating the identity of the user of the recipient device includes matching a password.
5. The method according to claim 1, wherein the cryptography key includes a public key.
6. The method according to claim 1, wherein the cryptography key includes a private key.
7. The method according to claim 1, further comprising restoring the SMS message to the encrypted SMS message for storing on the recipient device.
8. A system for composing and transmitting an encrypted SMS message, the system comprising a platform operable to perform the step in accordance with any one of the preceding claims.