

extended header may include information related to the sending user (e.g., the sending user's phone number or wireless handset identifier) and may be supplemented with additional information based on identification information related to the sending user.

[0031] An alert is generated that is based on the extended header. For example, and as is shown in UI ("User Interface") **100** in FIG. 1, the receiving user USER_NAME receives a MMS message from TRUSTED_INTERMEDIARY. TRUSTED_INTERMEDIARY represents an intermediary system that exchanges alerts and reports with a recipient user in order to determine whether the message should be delivered. UI **100** indicates that a user with handset identifier 202-555-1212 wants to send the second user a text message. The second user then has different options with which the recipient second user may respond. The second user can interact with one or more different hyperlinked options, for example, to accept, deny, or validate the text message. The recipient second user may respond to the alert by accepting the message, which will deliver the message to the second user without additional processing. The recipient second user also may deny the message to instruct the intermediary system to not deliver the message. The recipient user also may respond by instructing the intermediary system to validate the message.

[0032] Thus, in response to receiving the response to the alert from the second user, a validation request is generated. The validation request is processed using a certificate authority, for example, associated with the sending user and/or operated by a wireless carrier or other business entity (e.g., an online business certificate server).

[0033] A report is generated that reflects the results of processing the validation request. FIG. 2 illustrates a UI **200** of a report that includes one or more processing options. UI **200** is sent by TRUSTED_INTERMEDIARY and indicates that the user has requested to validate the message from 202-555-1212. The report indicates that TRUSTED_INTERMEDIARY has validated the message. UI **200** then presents options to accept the message, deny the message, or to accept the message and cache the certificate locally. The second user then may select one of the options in order to instruct the trusted intermediary. If the second user has instructed the intermediary system to deliver the message, the intermediary system will deliver the message. In FIG. 3, UI **300** illustrates how the message may be presented to the second user. Specifically, UI **300** indicates that the message is from 202-555-1212, in contrast to the alert and report indicating origination from the TRUSTED_INTERMEDIARY (as was shown previously in UIs **100** and **200**). UI **300** does indicate that the message has been validated by TRUSTED_INTERMEDIARY.

[0034] FIG. 4A illustrates a UI **400A** of an enhanced messaging service application. UI **400** illustrates a message to USER_NAME from TRUSTED_INTERMEDIARY with an alert. In UI **400A**, the TRUSTED_INTERMEDIARY indicates that Red (a user identifier associated with phone number 202-555-1994) wants to send USER_NAME a message. UI **400A** also indicates that despite a history of communications with Red, Red is sending USER_NAME a message with an enhanced feature set. UI **400A** then communicates a warning relating to the enhanced feature set. UI **400A** indicates, "Note that while the enhanced feature set can be used to pay a bill, the enhanced feature set also may be used for undesired purposes. As a result, we recommend validating all messages

using the enhanced feature set." The recipient second user (USER_NAME) then is equipped to accept the message, deny the message, or validate the message. In FIG. 4B, UI **400B** indicates that the message from Red has been validated. The second user is then prompted to accept or deny the message. In FIG. 4C, the message has been delivered and appears in UI **400C**. In particular, Red appears to be asking his father to pay for a bill related to school books. The second user is then prompted to execute the payment of \$142 or deny the charges.

[0035] In contrast, and to illustrate a report where the message cannot be validated, FIG. 5 illustrates a GUI **500** indicating that the message from Red cannot be validated. The report in GUI **500** includes a recommendation to deny the message.

[0036] FIG. 6 is a block diagram of an exemplary communications system **600** where wireless phones **601** and **602** are configured to interface with a wireless infrastructure. Generally, wireless phones **601** and **602** display one or more UIs (e.g., the UIs described previously in FIGS. 1-5) to exchange messages using the wireless intermediary **620**.

[0037] Each of the wireless phones **601** and **602** may include one or more devices capable of accessing a wireless network infrastructure **610** to exchange communications. The wireless phones may include one or more messaging applications.

[0038] In one implementation, the messaging application includes a messaging application that has been included by a manufacturer of a wireless phone. For example, a wireless manufacturer may develop a messaging application that works with other applications on the wireless phone (e.g., an address book application) in assisting users that are exchanging messages. The messaging application may include separately accessed modules for SMS and MMS applications. Alternatively, the messaging application may selectively invoke the appropriate messaging format (e.g., SMS vs. MMS) when format constraints call for a particular format to be used. For example, if the message is longer than 160 characters or includes an image, the messaging application may automatically format the message as a MMS message.

[0039] The messaging application also may include advanced modules that offer additional functionality beyond functionality required to exchange a SMS or MMS message. In one instance, the messaging application includes a certificate cache enabling a handset to perform its own certificate validation operations. For example, the message application may be configured to download automatically (or via user instruction) certificates for sending users with whom the receiving user has received communications. In particular, after a user has received a report indicating that a particular message has been validated, the user may be prompted to download the certificate for a particular user. The messaging application may be configured to then selectively download certificates in response to user instructions.

[0040] In another implementation, the messaging application may include modules that reduce the burden of responding to messages, alerts and reports. For example, the messaging application may be configured to determine that special terms appearing in a messaging application are "significant" in order to invoke advanced functionality. The messaging application may be configured to determine that the sending user's phone number represents a contact in an address book. As a result, the phone number may be replaced with the user's contact information from the address book. The receiving