CLAIMS

What is claimed is:

1. A system for verified messaging, comprising:

a database storing user information for a plurality of users, the user information including, for each user, a user identifier and a client device address;

a server configured to communicate over a network with a client device, the client device associated with a user;

a contactless card associated with the user, the contactless card configured for data communication via a short-range communication field of the client device, the contactless card comprising a processor and a memory, the memory storing data and an applet, wherein the applet is configured to provide a uniform resource identifier (URI) after entry by the contactless card into the short-range communication field of the client device, and wherein the URI comprises a message destination address and a message payload, the message destination address associated with the server; and

a processor in data communication with the server and the database, the processor configured to:

receive a message session request from the client device, the request including the message payload;

determine, based on the message payload, a user identifier corresponding to the user;

identify a client device address associated with the user;

determine whether the client device address associated with the user corresponds to a source address accompanying the request; and

send a response message to the client device, the response message addressed to the client device address.

2. The system of claim 1, wherein the URI is configured for a short message service (SMS) message and the message destination address comprises a short message service (SMS) address.

3. The system of claim 2, wherein the request comprises a short message service (SMS) message.

4. The system of claim 3, wherein the client device address comprises a mobile telephone number assigned to the client device.

5. The system of claim 4, wherein the source address accompanying the request is obtained from caller identification data.

6. The system of claim 5, wherein the response message is a short message service (SMS) message.

7. The system of claim 6, wherein the server is configured for data communication with a short message service (SMS) gateway, and the response message is routed by the server to the SMS gateway.

8. The system of claim 1, wherein the message payload includes a token associated with the user.

9. The system of claim 8, wherein the processor is further configured to authenticate the user based on a user key obtained from the token.

10. The system of claim 1, wherein the short-range communication field comprises near field communication (NFC) and the contactless card is configured to communicate the URI according to the NFC Data Exchange Format (NDEF).

11. A method for establishing a verified message session, comprising:

receiving from a mobile device, via a network, a request to establish a verified message session, the request generated in response to entry by a contactless card into a short-range communication field of the mobile device, the request accompanied by a

~~message payload read from the contactless card, wherein the mobile device and the contactless card are associated with a user;~~

~~determining, based on the message payload, a user identifier corresponding to the user;~~

~~identifying a mobile device number associated with the user;~~

~~establishing a verified message session in response to the request; and~~

~~transmitting a first message to the mobile device via the mobile device number.~~

~~12. The method of claim 11, further comprising authenticating the user based on a user key obtained from a token associated with the user in the message payload.~~

~~13. The method of claim 12, wherein the verified message session corresponds to short message service (SMS) messaging.~~

~~14. The method of claim 13, further comprising receiving a second message from the mobile device, the second message responsive to the first message.~~

~~15. The method of claim 14, further comprising transmitting a third message to the mobile device via the mobile device number, the third message responsive to the second message.~~

~~16. The method of claim 11, further comprising transmitting a session warning message to the mobile device via the mobile device number if a message is not received from the mobile device within a first predetermined time period, the first predetermined time period restarting upon transmission of each message to the mobile device via the mobile device number, wherein the session warning message prompts the user to send a responsive message.~~

~~17. The method of claim 16, further comprising transmitting a session termination message if a message is not received from the mobile device within a second predetermined time period after transmitting the session warning message.~~

18. The method of claim 17, further comprising terminating the verified message session upon at least one of transmitting the session termination message or receiving a session termination request from the mobile device.

19. The method of claim 11, further comprising determining whether the mobile device number associated with the user corresponds to a caller identification number accompanying the request.

20. A method for verified SMS messaging, comprising:

establishing a database storing user information for a plurality of users, the user information including, for each user, a user identifier and a mobile device number;

providing a contactless card configured for data communication via a near field communication (NFC) field of a mobile device, the contactless card comprising a processor and a memory, the memory storing data and an applet, wherein the applet is configured to provide a short message service (SMS) uniform resource identifier (URI) after entry by the contactless card into the NFC field of the mobile device, and wherein the URI comprises a short message service (SMS) destination address and a message payload, the SMS destination address associated with the server;

receiving from the mobile device, via a network, a request to establish a verified SMS message session, the request generated in response to entry by the contactless card into the NFC field of the mobile device, the request accompanied by a message payload read from the contactless card;

determining, based on the message payload, a user identifier corresponding to the user;

obtaining from the database a mobile device number associated with the user;

determining whether the mobile device number associated with the user corresponds to a caller identification number accompanying the request;

~~establishing a verified SMS message session in response to the request; and~~

~~transmitting a short message service (SMS) message to the mobile device via the mobile device number.~~

1. A method for verified messaging, comprising:

receiving, by a server, a message session request from a client device associated with a user, the message session request including a message payload;

determining, by the server based on the message payload, a user identifier corresponding to a user;

identifying, by the server, a client device address for the user;

determining, by the server, whether the client device address for the user corresponds to a source address accompanying the message session request; and

sending, by the server, a response message to the client device, the response message addressed to the client device address.

2. The method of claim 1, wherein the response message is a short message service (SMS) message.

3. The method of claim 2, wherein:

the server is configured for data communication with an SMS gateway, and

the response message is routed by the server to the SMS gateway.

4. The method of claim 1, wherein:

the message payload includes a token associated with the user, and

the method further comprises authenticating, by the server, the user based on a user key obtained from the token.

5. The method of claim 1, wherein the server is in data communication with a database storing user information for a plurality of users, the user information including, for each of the plurality of users, a user identifier and a client device address.

6. The method of claim 1, further comprising:

providing, by a card applet of a contactless card associated with the user after entry of the contactless card into a communication field of the client device, a uniform resource identifier (URI) into the short-range communication field of the client device,

wherein the URI comprises a message destination address of the server and the message payload.

7. The method of claim 6, wherein the message payload includes a data item from the contactless card.

8. The method of claim 7, wherein the data item includes at least one selected from the group of a counter and a cryptogram generated using the counter.

9. The method of claim 6, wherein the message payload includes a token associated with the user.

10. The method of claim 6, wherein the message payload includes a request to engage in a verified message session.

11. A system for verified messaging, comprising:

a server in data communication with a client device associated with a user, wherein the server:

receives a message session request from the client device, the message session request including a message payload,

determines, based on the message payload, a user identifier,

identifying a client device address for the user,

determining whether the client device address for the user corresponds to a source address accompanying the message session request, and

sending a response message to the client device, the response message addressed to the client device address.

12. The system of claim 11, wherein the client device address comprises a mobile phone number.

13. The system of claim 11, wherein the server is in data communication with a database storing user information for a plurality of users, the user information including, for each of the plurality of users, a user identifier and a client device address.

14. The system of claim 11, further comprising

a contactless card associated with the user, wherein:

the contactless card is configured for data communication via a short-range communication field of the client device,

the contactless card comprises at least one card processor and at least one card memory,

the at least one card memory stores data and a card applet, and

after entry by the contactless card into the short-range communication field of the client device, the card applet provides a uniform resource identifier (URI).

15. The system of claim 14, wherein the URI comprises a message destination address of the server and a message payload.

16. The system of claim 15, wherein the message payload includes a user key and a cryptogram.

17. The system of claim 16, wherein:

the card memory further includes a card number and a counter, and

the cryptogram is generated using the user key, the card number, and the counter.

18. A method for verified messaging, comprising:

providing, by an applet of a contactless card for a user after entry of the contactless card into a communication field of a client device belonging to a user, the contactless card comprising at least one card processor and a card memory storing data and the card applet, a uniform resource identifier (URI) into the short-range communication field of the client device, the URI comprising a message destination address of a server and a message payload;

receiving, by the server, a message session request from the client device, the message session request including the message payload;

determining, by the server based on the message payload, a user identifier corresponding to the user;

identifying, by the server, a client device address for the user;

determining, by the server, whether the client device address for the user corresponds to a source address accompanying the message session request; and

sending, by the server, a response message to the client device, the response message addressed to the client device address.

19. The method of claim 18, wherein the message payload includes a user key and a cryptogram.

20. The method of claim 19, wherein:

the card memory further stores a card number, and

the cryptogram is generated using the user key and the card number.