CLAIMS

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.