CLAIMS

1. A computing device implemented method, comprising:

receiving, by a computing system, a message from a computing device having an associated identifier, wherein the message comprises an indication to initiate a ~~text~~ secure messaging session and a cryptogram generated by~~, and wherein the cryptogram comprises information to authenticate~~ a contactless card;

decrypting, by the computing system, the cryptogram to extract ~~the information~~ a onetime password and an account identifier;

~~authenticating~~determining, by the computing system, that the onetime password is valid ~~the information based on authenticated information stored on the computing system~~;

determining, by the computing system, the ~~contactless card is associated~~ account identifier matches ~~with the~~ a stored identifier;

initiating, by the computing system, the ~~text~~ secure messaging session between the computing system and the computing device based on the determination that the onetime password is valid and the determination that the account identifier matches the stored identifier ~~associated with the contactless card information authenticated and the contactless card associated with the identifier~~.

2. The method of claim 1, wherein the decrypting uses a symmetric decryption algorithm.

3. The method of claim 1, wherein the ~~text~~ secure messaging session is one of a Short Message Service (SMS) messaging session, an instant messaging session, a social media messaging session, a video messaging session, a chatbot messaging session, or a virtual assistant messaging session~~, and receiving the message comprises receiving an SMS message~~.

4. The method of claim 1, comprising utilizing a chatbot of the computing system to communicate with the computing device in the ~~text~~ secure messaging session.

~~5. The method of claim 1, comprising:~~

~~performing, by the computing system, a first factor authentication to authenticate a user of the computing device based on the identifier and an authenticated identifier associated with the computing device; and~~

~~performing, by the computing system, a second factor authentication to authenticate the user of the computing device based on the information and the authenticated information.~~

~~6~~5. The method of claim 1, wherein the account identifier comprises a phone number associated with the computing device.

~~7~~6. The method of claim 1, wherein the ~~authentication information comprises a~~onetime password is at least partially based on cryptographic algorithm applied to a counter value by the contactless card.

7. The method of claim 6, wherein the counter value of the contactless card is synchronized with a counter value maintained by the computing system.

8. The method of claim 1, comprising authenticating, by the computing system, a geolocation of the computing device based on the message prior to initiating the secure messaging session.

9. A computing system, comprising:

~~one or more servers, the one or more servers comprising:~~

memory configured to store instructions; and

one or more processors coupled with the memory, the one or more processors configured to process the instructions, that when executed, cause the one or more processors to:

~~process~~ receive a message ~~received~~ from a computing device, wherein ~~computing device is associated with a phone number,~~ the message comprises an indication to initiate a secure messaging session and a cryptogram~~, and the cryptogram comprises information to authenticate a user associated with~~ generated by a contactless card;

~~apply a cryptographic algorithm to~~ decrypt the cryptogram to yield a onetime password and an account identifier;

~~compare the information with authenticated information to authenticate the user;~~

determine the onetime password is valid;

determine that ~~whether~~ the ~~information~~ account identifier matches the ~~authenticated information~~ a stored identifier; and

~~compare the phone number with a stored phone number for the computing device;~~

~~determine whether the phone number matches the stored phone number;~~

~~if the information matches the authenticated information and the phone number matches the stored phone number,~~ initiate the messaging session with the computing device based on the determination that the onetime password is valid and the determination that the account identifier matches the stored identifier~~; and~~

~~if the information does not match the authenticated information or the phone number does not match the stored phone number, prevent the messaging session with the computing device~~.

10. The computing system of claim 9, wherein the decrypting uses a symmetric decryption algorithm, wherein the account identifier comprises a phone number.

11. The computing system of claim 9, wherein the secure messaging session is one of a Short Message Service (SMS) messaging session, an instant messaging session, a social media messaging session, a video messaging session, a chatbot messaging session, or a virtual

assistant messaging session~~wherein the messaging session is a Short Message Service (SMS) messaging session, and receiving the message comprises receiving an SMS message~~.

12. The computing system of claim 9, further comprising instructions to cause the one or more processors to execute a chatbot, and wherein the secure messaging session is established between the chatbot and the computing device.

13. The computing system of claim 9, wherein the ~~authentication information comprises a~~ onetime password is at least partially based on cryptographic algorithm applied to a counter value by the contactless card, wherein the counter value of the contactless card is synchronized with a counter value maintained by the computing system.

14. The computing system of claim 9, further comprising instructions to cause the one or more processors to authenticate a geolocation of the computing device ~~based on the message~~ prior to initiating the messaging session.

15. A computer-implemented method, comprising:

~~sending, by a computing device, a message to a computing system, the message comprising a identifier to identify the computing device and an indication to establish a messaging session between the computing device and the computing system;~~

~~initiating, by the computing device via a near-field communication (NFC) interface, an NFC exchange with a contactless card;~~

receiving, by ~~the~~ a computing device, a cryptogram from ~~the~~ a contactless card, wherein the cryptogram is generated by the contactless card based on a onetime password and an account identifier ~~in an NFC communication of the NFC exchange~~;

sending, by the computing device, a request to initiate a secure messaging system to ~~the cryptogram to the~~ a computing system, wherein the request comprises the cryptogram~~wherein the computing system is configured to authenticate a user associated with~~

~~the computing device based on the identifier and the cryptogram to establish the messaging session; and~~

receive, from the computing system, a response specifying that the onetime password is valid and that the account identifier matches a stored identifier;

establishing, by the computing device, the messaging session with the computing system based on the response specifying that the onetime password is valid and that the account identifier matches the stored identifier ~~a successful authentication of the identifier and the cryptogram~~.

16. The method of claim 15, wherein the secure messaging session is one of a Short Message Service (SMS) messaging session, an instant messaging session, a social media messaging session, a video messaging session, a chatbot messaging session, or a virtual assistant messaging session~~wherein the messaging session is a Short Message Service (SMS) messaging session, and sending the message comprises sending an SMS message~~.

17. The method of claim 15, wherein the secure messaging session is established with a chatbot of the computing system.

18. The method of claim 15, wherein the account identifier comprises a phone number ~~associated with the computing device~~.

19. The method of claim 15, wherein the ~~cryptogram comprises a~~ onetime password is at least partially based on cryptographic algorithm applied to a counter value by the contactless card, wherein the counter value of the contactless card is synchronized with a counter value maintained by the computing system.

20. The method of claim 15, further comprising sending geolocation information to the computing system to perform an additional authentication of the user.