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 secure messaging session and a cryptogram generated by a contactless card;

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

determining, by the computing system, that the onetime password is valid;

determining, by the computing system, the account identifier matches a stored identifier;

initiating, by the computing system, the 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 d.

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

3. The method of claim 1, 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.

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

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

6. The method of claim 1, wherein the 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:

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:

receive a message from a computing device, wherein the message comprises an indication to initiate a secure messaging session and a cryptogram generated by a contactless card;

decrypt the cryptogram to yield a onetime password and an account identifier;

determine the onetime password is valid;

determine that the account identifier matches the a stored identifier; and

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.

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.

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 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 prior to initiating the messaging session.

15. A computer-implemented method, comprising:

receiving, by a computing device, a cryptogram from a contactless card, wherein the cryptogram is generated by the contactless card based on a onetime password and an account identifier;

sending, by the computing device, a request to initiate a secure messaging system to a computing system, wherein the request comprises the cryptogram;

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.

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.

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.

19. The method of claim 15, wherein the 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.