CLAIMS

1. A mobile device, comprising:

a display device;

a processor; and

memory comprising instructions that when executed by the processor, cause the processor to:

receive an input to perform an electronic exchange of money with a second mobile device of a first user;

receive, from a contactless card, first data, the first data encrypted with a private key of a second user;

generate a message comprising a uniform resource locator (URL) comprising the first data to communicate to the second mobile device, the URL configured to cause the second mobile device to perform authentication of the second user with the first data;

communicate the message to the second mobile device; and

cause the electronic exchange of money based on the authentication of the second user.

2. The mobile device of claim 1, comprising an input device coupled with the memory and the processor, the input device configured to receive the input comprising a selection of a contact, an indicated amount of money to electronically exchange, or a combination thereof.

3. The mobile device of claim 2, wherein the URL further comprises a first identifier to identify the amount of money, and a second identifier to identify the first user.

4. The mobile device of claim 1, the processor to:

detect, via a near-field communication (NFC) signal, the contactless card;

initiate an NFC exchange with the contactless card based on the contactless card coming within a communication range of the mobile device; and

receive the first data from the contactless card via the NFC exchange.

5. The mobile device of claim 1, wherein the URL comprises a link, that when activated, is configured to launch a webpage on the second mobile device to perform the authentication of the second user with the first data.

6. The mobile device of claim 1, wherein the first data comprises a string encrypted with the private key stored on the contactless card.

7. The mobile device of claim 1, wherein the private key is part of a key pair, and the key pair further comprising a public key associated with the contactless card, the first user, or a combination thereof.

8. The mobile device of claim 1, the processor to receive a result indicating that the second user is successfully authenticated from the second mobile device, and to cause the electronic exchange based on the result.

9. The mobile device of claim 1, the processor to communicate the message to the second mobile device as a Short Message Service (SMS) message, a Multimedia Message Service (MMS) message, or a Rich Communication Service (RCS) message.

10. A mobile device, comprising:

an input device;

a processor; and

memory comprising instructions that when executed by the processor, cause the processor to:

receive a message comprising a uniform resource locator (URL) comprising first data from a second mobile device, the URL configured to cause the mobile device to perform authentication of a first user with the first data;

detect, via the input device, an input to activate the URL;

launch an application in response to the input, wherein the application is configured to communicate with a server to perform the authentication of the first user with the first data;

receive an indication that the first user is authenticated by the server; and

cause performance of an exchange of money based on the first data and the indication that the first user is authenticated.

11. The mobile device of claim 10, wherein the input device comprises a touchscreen interface, the touchscreen interface to detect a selection of the URL on a display device.

12. The mobile device of claim 11, wherein the URL comprises a link, that when selected, launches the application.

13. The mobile device of claim 10, comprising a display device configured to present the message in a graphical user interface (GUI) display.

14. The mobile device of claim 10, the processor to communicate the first data to the server to perform the authentication of the first user.

15. The mobile device of claim 14, wherein the URL further comprises a first identifier of an amount of money to exchange, and a second identifier to identify the first user, and the processor to communicate at least one of the first identifier and the second identifier to the server.

16. The mobile device of claim 15, wherein the processor to cause the performance of the exchange based the amount of money and the first user being authenticated.

17. The mobile device of claim 10, wherein first data comprises an encrypted string associated with the first user, and the indication comprising information to indicate that the encrypted string was successful decrypted with a private key associated with the first user.

18. The mobile device of claim 17, wherein encrypted string is encrypted with a private key stored on a contactless card associated with the first user.

19. The mobile device of claim 10, the processor to receive the message as a Short Message Service (SMS) message, a Multimedia Message Service (MMS) message, or a Rich Communication Service (RCS) message.

20. A computer-implemented method, comprising:

detecting, by a processor of a first mobile device associated with a first user, a request to exchange money with a second user of a second mobile device;

receiving, from a contactless card, first data, the first data encrypted with a private key associated with the first user;

generating a text message comprising a uniform resource locator (URL) further comprising the first data to communicate to second user device, the URL configured to cause the second mobile device to perform authentication of the first user with the first data;

communicating the message to the second mobile device;

receiving an indication from the second mobile device indicating the first user is authenticated; and

exchanging information with the second mobile device to exchange the money.