CLAIMS

What is claimed is:

1. A method, comprising:

receiving, by a device, a request for authorizing a virtual account number for a first account associated with a second account;

receiving, by a card reader of the device from a contactless card, a uniform resource locator (URL) comprising at least one parameter for the virtual account number and encrypted data, the contactless card associated with the second account;

opening, by the device, an application responsive to receiving the URL;

transmitting, by the application, the encrypted data to an authentication server at the URL;

receiving, by the application, an indication specifying the authentication server decrypted the encrypted data;

providing, by the application to the authentication server and responsive to receiving the indication specifying the authentication server decrypted the encrypted data, the at least one parameter for the virtual account number; and

receiving, by the application based on the decryption of the encrypted data, a virtual account number for the first account from a virtual card number server, the virtual account number restricted based on the at least one parameter.

2. The method of claim 1, the at least one parameter comprising one or more of: an amount parameter for the virtual account number, a location parameter for the virtual account number, a time parameter, and a merchant parameter.

3. The method of claim 2, wherein the virtual account number is restricted to a spending limit based on the amount parameter, wherein the virtual account number is restricted to one or more locations based on the location parameter, wherein the virtual account number is restricted to a time limit specified by the time parameter, wherein the virtual account number is restricted to one or more merchants specified by the merchant parameter.

4. The method of claim 2, further comprising:

receiving, via the application, an additional parameter for the virtual account number, wherein the application provides the additional parameter to the authentication server, wherein the virtual account number is restricted based on the additional parameter.

5. The method of claim 1, wherein the URL is directed to a page of the application, wherein the device opens the page of the application.

6. The method of claim 1, wherein the encrypted data is based on a diversified key, wherein the diversified key is based on an identifier of the second account, a counter value, and a key stored in the contactless card.

7. The method of claim 6, wherein the indication specifies that the authentication server decrypted the encrypted data based on instances of the diversified key and the counter value stored by the authentication server.

8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor of a device, cause the processor to:

receive a request for authorizing a virtual account number for a first account associated with a second account;

receive, by a card reader of the device from a contactless card, a uniform resource locator (URL) comprising at least one parameter for the virtual account number and encrypted data, the contactless card associated with the second account;

open an application responsive to receiving the URL;

transmit, by the application, the encrypted data to an authentication server at the URL;

receive, by the application, an indication specifying the authentication server decrypted the encrypted data;

provide, by the application to the authentication server and responsive to receiving the indication specifying the authentication server decrypted the encrypted data, the at least one parameter for the virtual account number; and

receive, by the application based on the decryption of the encrypted data, a virtual account number for the first account from a virtual card number server, the virtual account number restricted based on the at least one parameter.

9. The computer-readable storage medium of claim 8, the at least one parameter comprising one or more of: an amount parameter for the virtual account number, a location parameter for the virtual account number, a time parameter, and a merchant parameter.

10. The computer-readable storage medium of claim 9, wherein the virtual account number is restricted to a spending limit based on the amount parameter, wherein the virtual account

number is restricted to one or more locations based on the location parameter, wherein the virtual account number is restricted to a time limit specified by the time parameter, wherein the virtual account number is restricted to one or more merchants specified by the merchant parameter.

11. The computer-readable storage medium of claim 9, wherein the instructions further cause the processor to:

receive, via the application, an additional parameter for the virtual account number, wherein the application provides the additional parameter to the authentication server, wherein the virtual account number is restricted based on the additional parameter.

12. The computer-readable storage medium of claim 8, wherein the URL is directed to a page of the application, wherein the device opens the page of the application.

13. The computer-readable storage medium of claim 8, wherein the encrypted data is based on a diversified key, wherein the diversified key is based on an identifier of the second account, a counter value, and a key stored in the contactless card.

14. The computer-readable storage medium of claim 13, wherein the indication specifies that the authentication server decrypted the encrypted data based on instances of the diversified key and the counter value stored by the authentication server.

15. A computing apparatus comprising:

a card reader;

a processor; and

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

receive a request for authorizing a virtual account number for a first account associated with a second account;

receive, by the card reader from a contactless card, a uniform resource locator (URL) comprising at least one parameter for the virtual account number and encrypted data, the contactless card associated with the second account;

open an application responsive to receiving the URL;

transmit, by the application, the encrypted data to an authentication server at the URL;

receive, by the application, an indication specifying the authentication server decrypted the encrypted data;

provide, by the application to the authentication server and responsive to receiving the indication specifying the authentication server decrypted the encrypted data, the at least one parameter for the virtual account number; and

receive, by the application based on the decryption of the encrypted data, a virtual account number for the first account from a virtual card number server, the virtual account number restricted based on the at least one parameter.

16. The computing apparatus of claim 15, the at least one parameter comprising one or more of: an amount parameter for the virtual account number, a location parameter for the virtual account number, a time parameter, and a merchant parameter.

17. The computing apparatus of claim 16, wherein the virtual account number is restricted to a spending limit based on the amount parameter, wherein the virtual account number is restricted to one or more locations based on the location parameter, wherein the virtual account number is restricted to a time limit specified by the time parameter, wherein the virtual account number is restricted to one or more merchants specified by the merchant parameter.

18. The computing apparatus of claim 16, wherein the instructions further cause the processor to:

receive, via the application, an additional parameter for the virtual account number, wherein the application provides the additional parameter to the authentication server, wherein the virtual account number is restricted based on the additional parameter.

19. The computing apparatus of claim 15, wherein the URL is directed to a page of the application, wherein the page of the application is opened.

20. The computing apparatus of claim 15, wherein the encrypted data is based on a diversified key, wherein the diversified key is based on an identifier of the second account, a counter value, and a key stored in the contactless card.