

CLAIMS

What is claimed is:

1. An apparatus, comprising:
a processor circuit; and
a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
receive at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;
receive, by an application executing on the processor circuit, authentication credentials for the primary account;
receive, by a card reader of the apparatus, encrypted data from a contactless card associated with the primary account, the encrypted data based on a cryptographic algorithm and a private key;
transmit, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;
receive, by the application, verification of the encrypted data from the authentication server based on the cryptographic algorithm and the private key;
provide, by the application to the server, the at least one parameter for authorizing the virtual account number; and
receive, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.
2. The apparatus of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
provide, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

3. The apparatus of claim 1, wherein the apparatus comprises a first apparatus associated with the subaccount, the at least one parameter received from at least one of:
(i) an applet executing in the memory of the contactless card, (ii) the first apparatus, and
(iii) a second apparatus associated with the primary account.

4. The apparatus of claim 3, the at least one parameter received from the second apparatus associated with the primary account.

5. The apparatus of claim 4, the at least one parameter received by the instance of the application executing on the processor circuit of the second apparatus responsive to a request generated by the instance of the application executing on the processor circuit of the first apparatus.

6. The apparatus of claim 1, wherein the at least one parameter further comprises a time parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.

7. The apparatus of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

output, by the application on a display, a plurality of virtual account numbers provided to a plurality of subaccounts associated with the primary account;

receive selection of one of the plurality of virtual account numbers, the selected one of the plurality of virtual account numbers comprising an inactive virtual account number; and

activate the selected one of the plurality of virtual account numbers, the activating to provide an additional amount of funds to the activated virtual account number.

8. A method, comprising:

receiving, at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;

receiving, by an application executing on a processor circuit of a first device, authentication credentials for the primary account;

receiving, by a card reader of the first device, encrypted data from a communications interface of a contactless card associated with the primary account, the encrypted data generated by an applet executing in a memory of the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card;

transmitting, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;

receiving, by the application, verification of the encrypted data from the authentication server, the authentication server to verify the encrypted data based on the cryptographic algorithm and an instance of the private key stored in a memory of the authentication server;

providing, by the application to the server, the at least one parameter for authorizing the virtual account number; and

receiving, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

9. The method of claim 8, further comprising:

providing, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

10. The method of claim 8, wherein the first device is associated with the subaccount, the at least one parameter received from at least one of: (i) the applet executing in the memory of the contactless card, (ii) the first device, and (iii) a second device associated with the primary account, wherein the at least one parameter further comprises a time

parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual account number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.

11. The method of claim 10, the at least one parameter received from the second device associated with the primary account, the authentication server further configured to:

receive, from an instance of the application executing on a processor circuit of the second device, encrypted data received by the second device from the communications interface of the contactless card associated with the primary account; and

verify the encrypted data received by the second device from the communications interface of the contactless card associated with the primary account.

12. The method of claim 11, the at least one parameter received by the instance of the application executing on the processor circuit of the second device responsive to a request generated by the instance of the application executing on the processor circuit of the first device.

13. The method of claim 8, the applet executing in the memory of the contactless card configured to:

receive an identifier of the first device, the identifier comprising one or more of: (i) a medium access control (MAC) address of the card reader, (ii) a unique identifier of the first device, and (iii) a software fingerprint of the first device generated based on a plurality of applications installed on the first device; and

determine that the identifier of the first device is specified as one of a plurality of devices associated with the primary account.

14. The method of claim 8, wherein the communication interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the method further comprising:

outputting, by the application on a display, a plurality of virtual account numbers provided to a plurality of subaccounts associated with the primary account;

receiving selection of one of the plurality of virtual account numbers, the selected one of the plurality of virtual account numbers comprising an inactive virtual account number; and

activating the selected one of the plurality of virtual account numbers, the activating to provide an additional amount of funds to the activated virtual account number.

15. A non-transitory computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code executable by a processor circuit of a first device to cause the processor circuit to:

receive at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;

receive, by an application executing on the processor circuit, authentication credentials for the primary account;

receive, by a card reader, encrypted data from a communications interface of a contactless card associated with the primary account, the encrypted data based on a cryptographic algorithm and a private key;

transmit, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;

receive, by the application, verification of the encrypted data from the authentication server based on the cryptographic algorithm and the private key;

provide, by the application to the server, the at least one parameter for authorizing the virtual account number; and

receive, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

16. The non-transitory computer-readable storage medium of claim 15, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to:

provide, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

17. The non-transitory computer-readable storage medium of claim 15, wherein the first device is associated with the subaccount, the at least one parameter received from at least one of: (i) an applet executing in the contactless card, (ii) the first device, and (iii) a second device associated with the primary account.

18. The non-transitory computer-readable storage medium of claim 17, the at least one parameter received from the second device associated with the primary account, storing instructions which when executed by the authentication server cause the authentication server to:

receive, from an instance of the application executing on a processor circuit of the second device, encrypted data received by the second device from the communications interface of the contactless card associated with the primary account; and

verify the encrypted data received by the second device from the communications interface of the contactless card associated with the primary account.

19. The non-transitory computer-readable storage medium of claim 18, the at least one parameter received by the instance of the application executing on the processor circuit of the second device responsive to a request generated by the instance of the application executing on the processor circuit of the first device.

20. The non-transitory computer-readable storage medium of claim 15, wherein the at least one parameter further comprises a time parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.