

CLAIMS

What is claimed is:

1. An apparatus comprising:
 - near field communication circuitry for receiving and transmitting data via near field communication (NFC);
 - memory to store instructions; and
 - one or more processors, coupled with the memory, operable to execute the instructions, that when executed, cause the one or more processors to:
 - receive login information from a user for accessing a software application and grant the user access to the software application based on the login information;
 - receive, via the software application, instruction or a selection from the user to generate a virtual card number from a user account;
 - determine whether one or more restrictions are associated with the generation of the virtual card number, wherein the one or more restrictions are input, set, or specified by the user;
 - authenticate the user by receiving one or more cryptograms from a first contactless card belonging to the user via NFC and decrypting the one or more cryptograms using a diversified key, the diversified key generated based on a master key and a counter value stored in the memory; and
 - apply, based on the authentication and the verification of the identity of the user being successful, the one or more restrictions to the virtual card number and generate the virtual card number.
2. The apparatus of claim 1, wherein the one or more restrictions include a merchant restriction, an amount restriction, a time period restriction, and/or a location restriction.
3. The apparatus of claim 1, wherein the one or more processors are further caused to:
 - detect a second contactless card via the NFC circuitry; and

write the virtual card number to the second contactless card as an NFC data exchange format (NDEF) tag between the apparatus and the second contactless card.

4. The apparatus of claim 3, wherein the second contactless card includes at least a first applet and a second applet different from the first applet, the first and second applets residing in a same secure domain.

5. The apparatus of claim 4, wherein the first applet consumes or processes the NDEF tag and forwards the virtual card number to the second applet such that the second contactless card becomes active for use at a point-of-sale system, the virtual card number being encrypted with a personal identification number (PIN) such that the PIN is required to use the virtual number.

6. The apparatus of claim 1, wherein the one or more processors are further caused to:

- detect an NFC compatible device via the NFC circuitry; and
- send the virtual card number to the NFC compatible device, and
- wherein the virtual card number is encrypted with a personal identification number (PIN) such that the PIN is required to use the virtual number.

7. The apparatus of claim 5, wherein the second contactless card is tapped to an NFC compatible device and the NFC compatible device reads at least the virtual card number so that the virtual card number is copied and pasted to or populated in one or more fields of a website or a web-based application in accordance with the one or more restrictions set by the user.

8. The apparatus of claim 6, wherein the one or more processors are further caused to send and provision the virtual card number to a third-party digital wallet.

9. The apparatus of claim 3, wherein the one or more processors are further caused to securely transmit, via NFC, expiration date and card verification value (CVV) information to the second contactless card.
10. The apparatus of claim 1, wherein the one or more processors are further caused to:
- prompt the user for confirmation or modification of the one or more restrictions input, set, or specified by the user prior to the authentication and receive a conformation or modification selection; and
 - allow, based on the modification selection, the user to modify the one or more restrictions.
11. The apparatus of claim 1, wherein the first contactless card comprises memory and processing circuitry for executing instructions stored in the memory to send the one or more cryptograms as one or more NFC data exchange format (NDEF) messages to the apparatus for performing the authentication and the verification of the identity of the user.
12. The apparatus of claim 4, wherein the second contactless card comprises memory and processing circuitry for executing instructions stored in the memory to process and execute the first and second applets residing in the same secure domain.
13. The apparatus of claim 3, wherein the second contactless card is a blank unlocked card and belongs to a recipient of the generated virtual card number.
14. A method for generating a virtual card number, the method comprising:
- receiving, via a computing device, login information from a user for accessing a software application;
 - receiving, via the software application, instruction or a selection from the user to generate the virtual card number from a user account;
 - authenticating, via the computing device, the user by receiving one or more cryptograms from a first contactless card belonging to the user via near field

communication (NFC) and decrypting the one or more cryptograms using a diversified key, the diversified key generated based on a master key and a counter value stored in memory;

determining, via the computing device, whether one or more restrictions are associated with the generating of the virtual card number, wherein the one or more restrictions are input, set, or specified by the user;

applying, based on the determination, the one or more restrictions to the virtual number and generating, via the computing device, the virtual card number; and

(i) detecting a second contactless card via NFC and writing the virtual card number to the second contactless card and/or (ii) sending the virtual card number to an NFC compatible device different from the computing device.

15. The method of claim 14, wherein the performing of the authentication further comprises:

detecting the contactless card via NFC and receiving the one or more cryptograms from the contactless card, the one or more cryptograms including at least card-user information; and

determining whether the card-user information from the received one or more cryptograms matches or corresponds to the user and, based on the determination that the card-user information matches or corresponds to the user, confirming the verification of the identity of the user.

16. The method of claim 14, wherein the one or more restrictions include a merchant restriction, an amount restriction, a time period restriction, and/or a location restriction.

17. The method of claim 14, wherein the second contactless card is a blank unlocked card and belongs to a recipient of the generated virtual card number.

18. A non-transitory computer-readable storage medium storing computer-readable program code executable by a processor to:

receive instruction or a selection from a user to generate a virtual card number from a user account;

receive one or more restrictions associated with the generation of the virtual card number;

authenticate the user by receiving one or more cryptograms from a first contactless card belonging to the user via near field communication (NFC) and decrypting the one or more cryptograms using a diversified key, the diversified key generated based on a master key and a counter value stored in memory;

verify an identity of the user based on the authentication and apply the one or more restrictions to the virtual card number; and

generate the virtual card number.

19. The non-transitory computer-readable storage medium of claim 17, wherein the one or more restrictions include a merchant restriction, an amount restriction, a time period restriction, and/or a location restriction.

20. The non-transitory computer-readable storage medium of claim 17, wherein the user account is a money account, a checking account, a credit card account, a debit card account, a digital wallet account, or a cryptocurrency account.