CLAIMS

1. A contactless card, comprising:

a memory;

at least one communication interface; and

one or more processors operable to execute stored instructions that, when executed, cause the one or more processors to:

determine whether the at least one communication interface is in a near-field communication (NFC) communication with an NFC reader of a computing device;

generate a random number via a secure random number generator;

convert the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user;

generate a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and

transmit the password via the at least one communication interface to the computing device, the transmitted password being a master password for triggering execution of at least one application on the computing device for managing one or more passwords used for accessing at least another application.

2. The contactless card of claim 1, wherein the random number generated by the secure random number generator has a predetermined length.

3. The contactless card of claim 1, wherein the conversion of the random number into the sequence of the one or more human-readable characters comprises the one or more processors further caused to apply a code-based or key-based cryptography system to the random number.

4. The contactless card of claim 1, wherein the password is transmitted from the contactless card to the computing device via one or more NFC data exchange format (NDEF) messages, wherein the password is included in a payload portion of the one or more NDEF messages and the payload portion is encrypted via a key.

5. The contactless card of claim 4, wherein the one or more processors are further caused to receive an acknowledgement (ACK) message from the computing device, the ACK message containing an indication that a first checksum value generated at the computing device matches a second checksum value provided in the one or more NDEF messages.

6. The contactless card of claim 1, wherein the one or more processors are further caused to receive a request or instruction to generate the password or wherein the password is automatically generated when an NFC communication is established and authenticated between the contactless card and the computing device.

7. The contactless card of claim 1, wherein the random number generator is stored in the contactless card and the generated password is stored in the memory of the contactless card.

8. A method, comprising:

determining, via one or more processors of a contactless card, whether at least one communication interface of the contactless card is in a near-field communication (NFC) communication with an NFC reader of a computing device;

generating, via a secure random number generator of the contactless card, a random number;

converting, via the one or more processors of the contactless card, the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user;

generating, via the one or more processors of the contactless card, a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or

capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and

transmitting, via the at least one communication interface of the contactless card, the password to the computing device, the transmitted password being a master password for triggering execution of at least one application on the computing device for managing one or more passwords used for accessing at least another application.

9. The method of claim 8, wherein the random number generated by the secure random number generator has a predetermined length.

10. The method of claim 8, wherein the converting of the random number into the sequence of the one or more human-readable characters comprises applying, via the one or more processors, a code-based or key-based cryptography system to the random number.

11. The method of claim 8, wherein the password is transmitted from the contactless card to the computing device via one or more NFC data exchange format (NDEF) messages, wherein the password is included in a payload portion of the one or more NDEF messages and the payload portion is encrypted via a key.

12. The method of claim 11, further comprising receiving an acknowledgement (ACK) message from the computing device, the ACK message containing an indication that a first checksum value generated at the computing device matches a second checksum value provided in the one or more NDEF messages.

13. The method of claim 8, further comprising receiving a request or instruction to generate the password or wherein the password is automatically generated when an NFC communication is established and authenticated between the contactless card and the computing device.

14. A non-transitory computer-readable storage medium storing computer-readable program code executable by at least one processor to:

determine, at a countless card, whether at least one communication interface of the contactless card is in a near-field communication (NFC) communication with an NFC reader of a computing device;

generate, at the contactless card, a random number via a secure random number generator;

convert, at the contactless card, the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user;

generate, at the contactless card, a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and

transmit the password via the at least one communication interface of the contactless card to the computing device, the transmitted password being a master password for triggering execution of at least one application on the computing device for managing one or more passwords used for accessing at least another application.

15. The non-transitory computer-readable storage medium of claim 14, wherein the password is transmitted from the contactless card to the computing device via one or more NFC data exchange format (NDEF) messages, wherein the password is included in a payload portion of the one or more NDEF messages and the payload portion is encrypted via a key.

16. The non-transitory computer-readable storage medium of claim 15, wherein the computer-readable program code further causes the at least one processor to receive an acknowledgement (ACK) message from the computing device, the ACK message containing an indication that a first checksum value generated at the computing device matches a second checksum value provided in the one or more NDEF messages.

17. The non-transitory computer-readable storage medium of claim 14, wherein the computer-readable program code further causes the at least one processor to receive a request or instruction to generate the password or wherein the password is automatically generated when an NFC communication is established and authenticated between the contactless card and the computing device.