

CLAIMS

What is claimed is:

1. ~~—An apparatus comprising:~~
 - ~~a camera;~~
 - ~~a near-field communication (NFC) reader;~~
 - ~~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:~~
 - ~~detect a contactless card via the NFC reader, the contactless card being tapped to~~
 - ~~the apparatus by a user;~~
 - ~~receive one or more cryptograms from the contactless card via NFC, wherein~~
 - ~~information in the one or more cryptograms is encrypted by the contactless card using a~~
 - ~~diversified key and the information includes at least a first customer identifier;~~
 - ~~decrypt the information in the one or more cryptograms using the diversified key~~
 - ~~to obtain the first customer identifier;~~
 - ~~determine whether the first customer identifier and a second customer identifier stored~~
 - ~~in memory match, and~~
 - ~~determine, based on the determination that the first and second customer identifiers~~
 - ~~match, that user authentication is successful, the successful user authentication indicating that~~
 - ~~the contactless card is issued or authorized to the user; and~~
 - ~~display, via an augmented reality (AR) interface, sensitive card information~~
 - ~~associated with a card on or adjacent to the card in AR when the card is detected by the~~
 - ~~camera.~~
2. ~~—The apparatus of claim 1, wherein the card detected by the camera is the contactless~~
~~card or wherein the card detected by the camera is separate and distinct from the contactless~~
~~card and issued or authorized to the user.~~
3. ~~—The apparatus of claim 1, wherein the diversified key is generated by providing a~~
~~master key and a particular counter value to a cryptographic algorithm to obtain an output, the~~
~~output being the diversified key.~~
4. ~~—The apparatus of claim 1, wherein the first customer identifier is a first unique~~
~~alphanumeric identifier corresponding to contactless card being tapped to the apparatus and~~
~~the second customer identifier is a second alphanumeric identifier corresponding to or~~
~~associated with the user.~~
5. ~~—The apparatus of claim 1, wherein the sensitive card information includes at least a card~~
~~number, a primary account number, a card verification value, and an expiration date and~~
~~wherein~~

one or more portions of the sensitive card information is obfuscated by one or more characters or symbols.

6. ~~The apparatus of claim 5, wherein the one or more processors are further caused to:~~
~~receive a selection of the one or more obfuscated portions of the sensitive card~~
~~information;~~

~~receive verification information, the verification information being a password or a~~
~~personal identification number;~~

~~determine whether the verification information is correct; and~~

~~reveal, based on the determination that the verification information is correct, the~~
~~selected~~

~~one or more obfuscated portions of the sensitive card information; and~~

~~display, via the AR interface, the revealed portions in AR.~~

7. ~~The apparatus of claim 5, wherein the one or more processors are further caused to:~~
~~display one or more callouts adjacent to the sensitive card information, the one or more~~
~~callouts including information indicating that an AR element associated with the card~~
~~information is selectable or interactable by the user to perform an action,~~

~~wherein the AR element is the sensitive card information superimposed on the card, and~~

~~wherein the action includes copying the sensitive information to a digital clipboard for use~~
~~at a merchant website.~~

8. ~~An apparatus comprising:~~

~~a camera;~~

~~a near field communication (NFC) reader;~~

~~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:~~

~~detect a contactless card via the NFC reader, the contactless card being tapped to the~~
~~apparatus by a user;~~

~~receive one or more cryptograms from the contactless card via NFC, wherein information~~
~~in the one or more cryptograms is encrypted by the contactless card using a diversified key and~~
~~the information includes at least a first customer identifier;~~

~~send the one or more cryptograms including the first customer identifier to one or more~~
~~remote computing devices, wherein the one or more remote computing devices performs at least~~
~~the decryption of the information in the one or more cryptograms using the diversified key;~~

~~receive an indication or confirmation from the remote computing devices that the first~~
~~customer identifier and a second customer identifier stored at the one or more computing devices~~
~~or a database match;~~

determine, based on the indication or the confirmation from the remote computing devices, that user authentication is successful, the successful user authentication indicating that the contactless card is issued or authorized to the user; and

display, via an augmented reality (AR) interface, sensitive card information associated with a card on or adjacent to the card in AR when the card is detected by the camera.

9.—The apparatus of claim 8, wherein the card detected by the camera is the contactless card or wherein the card detected by the camera is separate and distinct from the contactless card and issued or authorized to the user.

10.—The apparatus of claim 8, wherein the diversified key is generated by providing a master key and a particular counter value to a cryptographic algorithm to obtain an output, the output being the diversified key.

11.—The apparatus of claim 8, wherein the first customer identifier is a first unique alphanumeric identifier corresponding to contactless card being tapped to the apparatus and the second customer identifier is a second alphanumeric identifier corresponding to or associated with the user.

12.—The apparatus of claim 8, wherein the sensitive card information includes at least a card number, a primary account number, a card verification value, and an expiration date and wherein one or more portions of the sensitive card information is obfuscated by one or more characters or symbols.

13.—The apparatus of claim 12, wherein the one or more processors are further caused to:
receive a selection of the one or more obfuscated portions of the sensitive card information;

receive verification information, the verification information being a password or a personal identification number;

determine whether the verification information is correct; and

reveal, based on the determination that the verification information is correct, the selected

one or more obfuscated portions of the sensitive card information; and

display, via the AR interface, the revealed portions in AR.

14.—The apparatus of claim 12, wherein the one or more processors are further caused to:
display one or more callouts adjacent to the sensitive card information, the one or more callouts including information indicating that an AR element associated with the card information is selectable or interactable by the user to perform an action,

wherein the AR element is the sensitive card information superimposed on the card, and
wherein the action includes copying the sensitive information to a digital clipboard for use at a merchant website.

15. — The apparatus of claim 8, wherein the one or more remote computing devices are backend authentication servers with access to the database and a plurality of authentication-based services.

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

detect a contactless card via the NFC reader, the contactless card being tapped to the apparatus by a user;

receive one or more cryptograms from the contactless card via NFC, wherein information in the one or more cryptograms is encrypted by the contactless card using a diversified key and the information includes at least a first customer identifier;

perform user authentication by:

(i) decrypting the information in the one or more cryptograms using the diversified key to obtain the first customer identifier and (ii) determining whether the first customer identifier and a second customer identifier stored in memory match; or

(i) sending the one or more cryptograms including the first customer identifier to one or more remote computing devices, wherein the one or more remote computing devices performs at least the decryption of the information in the one or more cryptograms using the diversified key and (ii) receiving an indication or confirmation from the remote computing devices that the first customer identifier and a second customer identifier stored at the one or more computing devices or a database match; and

determine, based on the determination that the first and second customer identifiers match, that user authentication is successful, the successful user authentication indicating that the contactless card is issued or authorized to the user; and

display, via an augmented reality (AR) interface, sensitive card information associated with a card on or adjacent to the card in AR when the card is detected by the camera.

17. — The non-transitory computer-readable storage medium of claim 16, wherein the card detected by the camera is the contactless card or wherein the card detected by the camera is separate and distinct from the contactless card and issued or authorized to the user.

18. — The non-transitory computer-readable storage medium of claim 16, wherein the diversified key is generated by providing a master key and a particular counter value to a cryptographic algorithm to obtain an output, the output being the diversified key.

19. — The non-transitory computer-readable storage medium of claim 16, wherein the first customer identifier is a first unique alphanumeric identifier corresponding to contactless card being tapped to the apparatus and the second customer identifier is a second alphanumeric identifier corresponding to or associated with the user.

~~20. The non-transitory computer-readable storage medium of claim 16, wherein the sensitive card information includes at least a card number, a primary account number, a card verification value, and an expiration date and wherein one or more portions of the sensitive card information is obfuscated by one or more characters or symbols.~~

1. An apparatus comprising:

a camera;

a near-field communication (NFC) reader;

a memory to store instructions; and

a processor operable to execute the instructions that, when executed, cause the processor

to:

receive a cryptogram from a contactless card via the NFC reader;

decrypt the cryptogram;

authenticate, based on the decryption, a request to display card information of the contactless card; and

display, via an augmented reality (AR) interface based on the authentication, the card information of the contactless card on the contactless card in AR when the contactless card is detected by the camera.

2. The apparatus of claim 1, wherein the card information includes at least a card number, a primary account number, a card verification value, and an expiration date, wherein one or more portions of the card information is obfuscated by one or more characters or symbols.

3. The apparatus of claim 2, the processor operable to execute the instructions that, when executed, cause the processor to:

receive a selection of the one or more obfuscated portions of the card information;

receive verification information, the verification information comprising a password or a personal identification number;

determine that the verification information is valid;

reveal, based on the determination that the verification information is valid, the selected one or more obfuscated portions of the card information; and

display, via the AR interface, the revealed portions in AR.

4. The apparatus of claim 3, the processor operable to execute the instructions that, when executed, cause the processor to:

display one or more callouts adjacent to the card information, the one or more callouts comprising information indicating that an AR element associated with the card information is selectable to perform an action, wherein the AR element is the card information superimposed on the contactless card, and wherein the action comprises copying the selected information to a clipboard.

5. The apparatus of claim 1, the processor operable to execute the instructions that, when executed, cause the processor to, prior to authenticating the request:

determine that a first customer identifier yielded by decrypting the cryptogram matches a second customer identifier stored in the memory, wherein the request is further authenticated based on the determination that the first and second customer identifiers match.

6. The apparatus of claim 5, wherein the cryptogram is based on a diversified key, wherein the diversified key is based on a master key and a counter value.

7. The apparatus of claim 1, the processor operable to execute the instructions that, when executed, cause the processor to, prior to receiving the cryptogram:

download and install an application comprising the AR interface based on a tap of the contactless card to the apparatus.

8. A method, comprising:

decrypting, by a processor of a device, a cryptogram received from a contactless card via an NFC reader of the device;

authenticating, by the processor based on the decryption, a request to display card information of the contactless card; and

displaying, by the processor via an augmented reality (AR) interface based on the authentication, the card information of the contactless card on the contactless card in AR when the contactless card is detected by a camera of the device.

9. The method of claim 8, wherein the card information includes at least a card number, a primary account number, a card verification value, and an expiration date, wherein one or more portions of the card information is obfuscated by one or more characters or symbols.

10. The method of claim 9, further comprising:

receiving, by the processor, a selection of the one or more obfuscated portions of the card information;

receiving, by the processor, verification information, the verification information comprising a password or a personal identification number;

determining, by the processor, that the verification information is valid; and
revealing, by the processor based on the determination that the verification
information is valid, the selected one or more obfuscated portions of the card information;
and

displaying, by the processor via the AR interface, the revealed portions in AR.

11. The method of claim 10, further comprising:

displaying, by the processor, one or more callouts adjacent to the card information,
the one or more callouts comprising information indicating that an AR element associated
with the card information is selectable to perform an action.

wherein the AR element is the card information superimposed on the card, and

wherein the action comprises copying the selected information to a digital clipboard.

12. The method of claim 8, further comprising prior to authenticating the request:

determining, by the processor, that a first customer identifier yielded by decrypting
the cryptogram matches a second customer identifier stored in the device, wherein the
request is further authenticated based on the determination that the first and second customer
identifiers match.

13. The method of claim 8, further comprising, prior to receiving the cryptogram:

downloading and installing, by the processor, an application comprising the AR
interface based on a tap of the contactless card to the device.

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

receive a cryptogram from a contactless card via a near-field communication (NFC)
reader;

decrypt the cryptogram;

authenticate, based on the decryption, a request to display card information of the
contactless card; and

display, via an augmented reality (AR) interface executing on the processor based on the
authentication, the card information of the contactless card on the contactless card in AR when
the contactless card is detected by a camera.

15. The medium of claim 14, wherein the card information includes at least a card
number, a primary account number, a card verification value, and an expiration date, wherein one
or more portions of the card information is obfuscated by one or more characters or symbols.

16. The medium of claim 15, storing computer-readable program code executable by the processor to cause the processor to:

receive a selection of the one or more obfuscated portions of the card information;

receive verification information, the verification information comprising a password or a personal identification number;

determine that the verification information is valid;

reveal, based on the determination that the verification information is valid, the selected one or more obfuscated portions of the card information; and

display, via the AR interface, the revealed portions in AR.

17. The medium of claim 16, storing computer-readable program code executable by the processor to cause the processor to:

display one or more callouts adjacent to the card information, the one or more callouts comprising information indicating that an AR element associated with the card information is selectable to perform an action, wherein the AR element is the card information superimposed on the contactless card, and wherein the action comprises copying the selected information to a clipboard.

18. The medium of claim 14, storing computer-readable program code executable by the processor to cause the processor to, prior to authenticating the request:

determine that a first customer identifier yielded by decrypting the cryptogram matches a second customer identifier, wherein the request is further authenticated based on the determination that the first and second customer identifiers match.

19. The medium of claim 18, wherein the cryptogram is based on a diversified key, wherein the diversified key is based on a master key and a counter value.

20. The medium of claim 14, storing computer-readable program code executable by the processor to cause the processor to, prior to receiving the cryptogram:

download and install an application comprising the AR interface based on a tap of the contactless card to a device comprising the processor.