TAP TO COPY DATA TO CLIPBOARD VIA NFC

TECHNICAL FIELD

[0001] Embodiments herein generally relate to mobile computing platforms, and more specifically, to tap to copy data to a clipboard via near-field communication (NFC).

RELATED APPLICATIONS

[0002] This application claims priority to U.S. Patent Application Serial No. 16/359,966, titled "TAP TO COPY DATA TO CLIPBOARD VIA NFC" filed on March 20, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

BACKGROUND

[0003] Account identifiers for payment cards are often long numeric and/or character strings. As such, it is difficult for a user to manually enter the account identifier correctly. Indeed, users often make mistakes and enter incorrect account numbers into computing interfaces (e.g., payment interfaces). Furthermore, even if the user enters the correct account identifier, processes have been developed that allow cameras to capture the account identifier.

SUMMARY

[0003a] According to a first aspect, there is provided an apparatus, including: a processor; and a memory storing instructions which when executed by the processor, cause the processor to: receive, by an application executing on the processor, encrypted data from a contactless card associated with an account; receive, by the application from a server, verification of the encrypted data; receive, by the application, an account number associated with the account; and copy, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

[0003b] According to a second aspect, there is provided a computer-readable storage medium storing instructions which when executed by a processor cause the processor to: receive, by an application executing on the processor, encrypted data from a contactless card associated with an account; receive, by the application from a server, verification of the encrypted data; receive, by the application, an account number associated with the account; and copy, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

[0003c] According to a third aspect, there is provided a method, including: receiving, by an application executing on a processor, encrypted data from a contactless card associated with an account; receiving, by the application from a server, verification of the encrypted data; receiving, by the application, an account number associated with the account; and copying, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for tapping to copy data to a clipboard via NFC. According to one example, an application may receive encrypted data from a communications interface of a contactless card associated with an account, the encrypted data generated based on one or more cryptographic algorithms and a diversified key, the diversified key stored in a memory of the contactless card and generated based on a master key and a counter value stored in the memory of the

CLAIMS

1. An apparatus, comprising:

a processor; and

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

receive, by an application executing on the processor, encrypted data from a contactless card associated with an account;

receive, by the application from a server, verification of the encrypted data;

receive, by the application, an account number associated with the account; and

copy, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

2. The apparatus of claim 1, wherein the account number is received from one of the contactless card or the server, the memory storing instructions which when executed by the processor, cause the processor to:

transmit the encrypted data to the server prior to receiving the verification.

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

determine the received account number is encrypted; and

decrypt the encrypted account number prior to copying the account number to the clipboard.

4. The apparatus of claim 1, wherein the encrypted data received from the contactless card is based on one or more cryptographic algorithms and a diversified key, wherein the diversified key is based on a master key and a counter value.

5. The apparatus of claim 4, wherein the server is to verify the encrypted data based on an instance of the diversified key, wherein the instance of the diversified key is based an instance of the master key and an instance of the counter value.

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

paste, by the OS from the clipboard, the account number to a first form field of a form.

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

modify the clipboard based on at least one of: (i) completion of a purchase, or (ii) expiration of a time threshold, wherein modifying the clipboard comprises one or more of: (i) erasing all data stored in the clipboard, or (ii) copying random data to the clipboard.

8. A computer-readable storage medium storing instructions which when executed by a processor cause the processor to:

receive, by an application executing on the processor, encrypted data from a contactless card associated with an account;

receive, by the application from a server, verification of the encrypted data;

receive, by the application, an account number associated with the account; and

copy, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

9. The medium of claim 8, wherein the account number is received from one of the contactless card or the server, the medium storing instructions which when executed by the processor, cause the processor to:

transmit the encrypted data to the server prior to receiving the verification.

10. The medium of claim 8, storing instructions which when executed by the processor, cause the processor to:

determine the received account number is encrypted; and

decrypt the encrypted account number prior to copying the account number to the clipboard.

11. The medium of claim 8, wherein the encrypted data received from the contactless card is based on one or more cryptographic algorithms and a diversified key, wherein the diversified key is based on a master key and a counter value.

12. The medium of claim 11, wherein the server is to verify the encrypted data based on an instance of the diversified key, wherein the instance of the diversified key is based an instance of the master key and an instance of the counter value.

13. The medium of claim 8, storing instructions which when executed by the processor, cause the processor to:

paste, by the OS from the clipboard, the account number to a first form field of a form.

14. The medium of claim 13, storing instructions which when executed by the processor, cause the processor to:

modify the clipboard based on at least one of: (i) completion of a purchase, or (ii) expiration of a time threshold, wherein modifying the clipboard comprises one or more of: (i) erasing all data stored in the clipboard, or (ii) copying random data to the clipboard.

15. A method, comprising:

receiving, by an application executing on a processor, encrypted data from a contactless card associated with an account;

receiving, by the application from a server, verification of the encrypted data;

receiving, by the application, an account number associated with the account; and

copying, by the application, the account number to a clipboard of an operating system (OS) executing on the processor.

16. The method of claim 15, wherein the account number is received from one of the contactless card or the server, the method further comprising:

transmitting the encrypted data to the server prior to receiving the verification.

17. The method of claim 15, further comprising:

determining the account number is encrypted; and

decrypting the encrypted account number prior to copying the account number to the clipboard.

18. The method of claim 15, wherein the encrypted data received from the contactless card is based on one or more cryptographic algorithms and a diversified key, wherein the diversified key is based on a master key and a counter value.

19. The method of claim 18, wherein the server is to verify the encrypted data based on an instance of the diversified key, wherein the instance of the diversified key is based an instance of the master key and an instance of the counter value.

20. The method of claim 15, further comprising:

pasting, by the OS from the clipboard, the account number to a first form field of a form.