contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account. The computer-readable program code executable by the processor circuit may further cause the processor circuit to receive, by the application from a server, a second verification of the user account based on the second set of encrypted data, authorize, by the application, access to the digital service in response to the first and second verification of the user account, and continuously provide, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

[0007a] An aspect of the present disclosure provides a method, comprising: receiving, by an application executing on a processor circuit of a client device, a request to access a digital service; receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; requesting, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device; receiving, by a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; performing, by the application, the second authentication based on the second set of encrypted data; authorizing, by the application, access to the digital service in response to the first authentication and the second authentication; transmitting, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receiving, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; providing, by the application based on the first response, access to the digital service without requiring re-authentication; determining, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminating, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

[0007b] Another aspect of the present disclosure provides a computer-readable storage medium including instructions that when executed by a processor of a client device, cause the processor to:receive, by an application, a request to access a digital service; receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device; receive, via a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; perform, by the application, the second authentication based on the second set of encrypted data; authorize, by the application, access to the digital service in response to the first authentication and the second authentication; transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; provide, by the application based on the first response, access to the digital service without requiring re-authentication; determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

[0007c] Another aspect of the present disclosure provides a computing apparatus comprising: a processor; a card reader; and a memory storing instructions that, when executed by the processor, cause the processor to: receive, by an application, a request to access a digital service; receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the apparatus; receive, by the card reader, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; perform, by the application, the second authentication based on the second set of encrypted data; authorize, by the application, access to the digital service

in response to the first authentication and the second authentication; transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; provide, by the application based on the first response, access to the digital service without requiring re-authentication; determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 illustrates an embodiment of a system for providing continuous authentication to a digital service.

[0009] FIGs. 2-3 illustrate embodiments for providing continuous authentication to the digital service based on proximity of a contactless card to a computing device.

[0010] FIGs. 4A-4B illustrate embodiments of a contactless card.

[0011] FIG. 5A illustrates a side view of an embodiment of a covering for a client device.

[0012] FIG. 5B illustrates an end view of an embodiment of the covering for the client device of FIG. 5A.

[0013] FIG. 6 illustrates an embodiment of a logic flow for providing continuous authentication to a digital service.

[0014] FIG. 7 illustrates an embodiment of a computing architecture.

[0015] The drawings are not necessarily to scale. The drawings are merely representations, not intended to portray specific parameters of the disclosure. The drawings are intended to depict example embodiments of the disclosure, and therefore are not be considered as limiting in scope. Certain elements in some of the FIG.s may be omitted, or illustrated not-to-scale, for illustrative clarity. Furthermore, some reference numbers may be omitted in certain drawings.

DETAILED DESCRIPTION

[0016] The present embodiments will now be described more fully hereinafter with reference to the accompanying drawings, where some embodiments are shown. The subject matter of the present disclosure may be embodied in many different forms and are not to be construed as

CLAIMS

What is claimed is:

1. A system, comprising:

a processor circuit; and

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

receive, by an application executing on the processor circuit, a request to access a digital service;

receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application, a second authentication from a contactless card;

receive, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account;

receive, by the application from a server, a second verification of the user account based on the second set of encrypted data;

authorize, by the application, access to the digital service in response to the first and second verification of the user account;

continuously provide, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

2. The system of claim 1, the memory storing instructions which when executed by the processor circuit, cause the application to determine the contactless card is inactive when a signal strength of the contactless card is below a predetermined threshold value.

3. The system of claim 1, the memory storing instructions which when executed by the processor circuit, cause the application to activate the contactless card in response to a magnetic field of the client device.

4. The system of claim 1, further comprising a second client device, wherein the application operates on the second client device.

5. The system of claim 1, wherein the client device is one of: a mobile device, a personal computer, and an external contactless card reader.

6. The system of claim 5, the memory storing instructions which when executed by the processor circuit, cause the application to:

request the second authentication directly from the mobile device;

receive the second set of encrypted data from the communications interface of the contactless card in response to the request for the second authentication; and

send the second set of encrypted data to the server to receive the second verification of the user account based on the second set of encrypted data.

7. The system of claim 1, further comprising a physical covering over the client device, the covering including a receptacle operable to receive the contactless card, wherein the receptacle is located proximate the card reader of the client device.

8. A method, comprising:

receiving, by an application executing on the processor circuit, a request to access a digital service;

receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

requesting, by the application, a second authentication from a contactless card;

receiving, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account;

receiving, by the application from a server, a second verification of the user account based on the second set of encrypted data;

authorizing, by the application, access to the digital service in response to the first and second verification of the user account; and

continuously providing, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

9. The method of claim 8, further comprising determining, by the application, the contactless card is inactive when a signal strength of the contactless card is below a predetermined threshold value.

10. The method of claim 8, further comprising activating, by the application, the contactless card in response to a magnetic field of the client device.

11. The method of claim 8, further comprising providing a second client device, wherein the application operates on the second client device.

12. The method of claim 8, the memory storing instructions which when executed by the processor circuit, cause the application to:

request the second authentication directly from the client device, wherein the client device is a mobile device;

receive the second set of encrypted data from the communications interface of the contactless card in response to the request for the second authentication; and

send the second set of encrypted data to the server to receive the second verification of the user account based on the second set of encrypted data.

13. The method of claim 8, further comprising receiving the contactless card within a receptacle of a physical covering, the receptacle located proximate to the card reader of the client device when the client device is coupled with the physical covering.

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

receive, by an application executing on the processor circuit, a request to access a digital service;

receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application, a second authentication from a contactless card;

receive, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account;

receive, by the application from a server, a second verification of the user account based on the second set of encrypted data;

~~authorize, by the application, access to the digital service in response to the first and second verification of the user account; and~~

~~continuously provide, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.~~

~~15. The non-transitory computer-readable storage medium of claim 14, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to determine, by the application, the contactless card is inactive when a signal strength of the contactless card is below a predetermined threshold value.~~

~~16. The non-transitory computer-readable storage medium of claim 14, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to activate, by the application, the contactless card in response to a magnetic field of the client device.~~

~~17. The non-transitory computer-readable storage medium of claim 14, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to operate the application on a second client device.~~

~~18. The non-transitory computer-readable storage medium of claim 14, wherein the client device is one of: a mobile device, a personal computer, and an external contactless card reader.~~

~~19. The non-transitory computer-readable storage medium of claim 18, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to:~~

~~request, by the application, the second authentication directly from the client device;~~

~~receive, by the application, the second set of encrypted data from the communications interface of the contactless card in response to the request for the second authentication; and~~

~~send, by the application, the second set of encrypted data to the server to receive the second verification of the user account based on the second set of encrypted data.~~

~~20. The non-transitory computer-readable storage medium of claim 14, wherein the communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, and wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the account.~~

1. A method, comprising:

receiving, by an application executing on a processor circuit of a client device, a request to access a digital service;

receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

requesting, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device;

receiving, by a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

performing, by the application, the second authentication based on the second set of encrypted data;

authorizing, by the application, access to the digital service in response to the first authentication and the second authentication;

transmitting, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receiving, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

providing, by the application based on the first response, access to the digital service without requiring re-authentication;

determining, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminating, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

2. The method of claim 1, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card coming into a communication range of the client device, wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

3. The method of claim 2, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

4. The method of claim 1, wherein performing the second authentication comprises:

sending, by the application, the second set of encrypted data to a server; and

receiving, by the application from the server, the second authentication based on the second set of encrypted data.

5. The method of claim 1, wherein determining the response to the second status message is not received comprises:

determining, by the application, that a signal strength of the contactless card is below a threshold value.

6. The method of claim 1, further comprising receiving the contactless card within a slot through an end wall of a physical covering, the slot defining a set of walls operable to house the contactless card, and the slot disposed along a backside of the client device when the client device is coupled with the physical covering.

7. The method of claim 1, wherein authorization to access the digital service continues while the contactless card is active, wherein authorization to access the digital service terminates when the contactless card is inactive, wherein a third response of the plurality of responses is received subsequent to the first response and prior to determining the response to the second status message is not received, wherein the application provides access to the digital service without requiring re-authentication based on the third response.

8. A computer-readable storage medium including instructions that when executed by a processor of a client device, cause the processor to:

receive, by an application, a request to access a digital service;

receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device;

receive, via a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

perform, by the application, the second authentication based on the second set of encrypted data;

authorize, by the application, access to the digital service in response to the first authentication and the second authentication;

transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

provide, by the application based on the first response, access to the digital service without requiring re-authentication;

determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

9. The computer-readable storage medium of claim 8, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card come into a communication range of the client device, wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

10. The computer-readable storage medium of claim 9, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card.

11. The computer-readable storage medium of claim 10, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

12. The computer-readable storage medium of claim 8, wherein determining the response to the second status message is not received comprises:

determine, by the application, that a signal strength of the contactless card is below a threshold value.

13. The computer-readable storage medium of claim 12, wherein the instructions further configure the processor to:

display, by the application, the signal strength of the contactless card in a graphical user interface.

14. The computer-readable storage medium of claim 8, wherein authorization to access the digital service continues while the contactless card is active, wherein authorization to access the digital service terminates when the contactless card is inactive, wherein a third response of the plurality of responses is received subsequent to the first response and prior to determining the response to the second status message is not received, wherein the application provides access to the digital service without requiring re-authentication based on the third response.

15. A computing apparatus comprising:

a processor;

a card reader; and

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

receive, by an application, a request to access a digital service;

receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the apparatus;

receive, by the card reader, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

perform, by the application, the second authentication based on the second set of encrypted data;

authorize, by the application, access to the digital service in response to the first authentication and the second authentication;

transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

provide, by the application based on the first response, access to the digital service without requiring re-authentication;

determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

16. The computing apparatus of claim 15, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card come into a communication range of the apparatus, wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

17. The computing apparatus of claim 16, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card.

18. The computing apparatus of claim 17, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

19. The computing apparatus of claim 15, wherein determining the response to the second status message is not received comprises:

determining, by the application, that a signal strength of the contactless card is below a threshold value.

20. The computing apparatus of claim 15, further comprising a slot configured to receive the contactless card through an end wall of a physical covering, the slot defining a set of walls

operable to house the contactless card, and the slot disposed along a backside of the apparatus.