

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.