CLAIMS

WHAT IS CLAIMED IS:

1. A computing device comprising:

a short-range wireless signaling component configured for wireless communication within a proximity range via a wireless signaling protocol;

a non-transitory memory; and

one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the computing device to perform operations comprising:

receiving, from a computing system that is managed by a service provider responsible for issuing a physical payment card, a multifactor authentication challenge that is generated in response to an attempt to use the physical payment card, wherein the physical payment card comprises a microchip having cryptographic signing data;

activating the short-range wireless signaling component to enable wireless communication within the proximity range;

receiving, from a second computing device via the short-range wireless signaling component, a request corresponding to an authentication protocol that authenticates a user on the computing device;

prompting, based on the request, the user to enter an authentication credential associated with the physical payment card on the computing device;

unlocking, based on the authentication credential and the authentication protocol, signing operations for the microchip of the physical payment card;

requesting, via the short-range wireless signaling component, that the microchip digitally sign the multifactor authentication challenge using the cryptographic signing data;

receiving, from the microchip, a digitally signed multifactor authentication challenge based on the multifactor authentication challenge and the cryptographic signing data; and

processing the digitally signed multifactor authentication challenge from the computing system that is managed by the service provider during the authentication attempt.

2. The computing device of claim 1, wherein prior to receiving the multifactor authentication challenge, the operations further comprise:

linking the physical payment card to at least one of, a device identifier for the computing device, an identifier for the user associated with the computing device, or an account of the user.

3. The computing device of claim 1, wherein the microchip comprises a Java Card chip that utilizes a Java-based application with the cryptographic signing data.

4. The computing device of claim 1, wherein the authentication attempt is associated with a card-not-present transaction over a network with an online merchant or an online service provider, and wherein the digitally signed multifactor authentication challenge converts the card-not-present transaction to a card-present transaction.

5. The computing device of claim 1, wherein the authentication attempt is associated with a use of the physical payment card at a physical merchant location for a card-present transaction, and wherein the multifactor authentication challenge comprises a step-up authentication for the use of the physical payment card for the card-present transaction.

6. The computing device of claim 1, wherein the one of the computing device or the microchip further stores an amount of a cryptocurrency, and wherein the authentication attempt is for a use of the amount of the cryptocurrency for a transaction that requires the multifactor authentication challenge for the use.

7. The computing device of claim 1, wherein the multifactor authentication challenge is received via an electronic communication channel comprising one of a push notification for an application on the computing device, a text message, an email, or an operating system level message.

8. The computing device of claim 1, wherein the cryptographic signing data is specific to the microchip based on a time of creating the microchip with encoded data for the cryptographic signing data.

9. The computing device of claim 1, wherein processing the digitally signed multifactor authentication challenge further comprises providing at least one additional confidence factor for the multifactor authentication challenge that comprises one of a location, a current time of the computing device, a network identifier, a connected device, an image, or a biometric.

10. A method comprising:

receiving, by a first computing device, a multifactor authentication challenge from a service provider server during an authentication attempt associated with a physical payment card, wherein the physical payment card comprises a microchip having cryptographic signing data;

activating, on the first computing device, a short-range wireless signaling component that utilizes a wireless signaling protocol for wireless communication with devices within a proximity range of the mobile device;

receiving, by the first computing device from a second computing device via the short-range wireless signaling component within the proximity range, a request corresponding to an authentication protocol that authenticates a user on the first computing device;

prompting, by the first computing device based on the request, the user to enter an authentication credential associated with the physical payment card;

unlocking, by the first computing device based on the authentication credential and the authentication protocol, signing operations for the microchip of the physical payment card;

requesting, by the first computing device via the short-range wireless signaling component in response to said unlocking, that the microchip digitally sign the multifactor authentication challenge using the cryptographic signing data;

receiving, by the first computing device from the microchip, a digitally signed multifactor authentication challenge based on the multifactor authentication challenge and the cryptographic signing data; and

processing, by the first computing device, the digitally signed multifactor authentication challenge from the service provider server during the authentication attempt.

11. The method of claim 10, wherein prior to receiving the multifactor authentication challenge, the method further comprises:

linking the physical payment card to at least one of, a device identifier for the first computing device, an identifier for the user associated with the first computing device, or an account of the user.

12. The method of claim 10, wherein the microchip comprises a Java Card chip that utilizes a Java-based application with the cryptographic signing data.

13. The method of claim 10, wherein the authentication attempt is associated with a card-not-present transaction over a network with an online merchant or an online service provider, and wherein the digitally signed multifactor authentication challenge converts the card-not-present transaction to a card-present transaction.

14. The method of claim 10, wherein the authentication attempt is associated with a use of the physical payment card at a physical merchant location for a card-present transaction, and wherein the multifactor authentication challenge comprises a step-up authentication for the use of the physical payment card for the card-present transaction.

15. The method of claim 10, wherein the one of the first computing device or the microchip further stores an amount of a cryptocurrency, and wherein the authentication attempt is for a use of the amount of the cryptocurrency for a transaction that requires the multifactor authentication challenge for the use.

16. The method of claim 10, wherein the multifactor authentication challenge is received via an electronic communication channel comprising one of a push notification for an application on the first computing device, a text message, an email, or an operating system level message.

17. The method of claim 10, wherein the cryptographic signing data is specific to the microchip based on a time of creating the microchip with encoded data for the cryptographic signing data.

18. The method of claim 10, wherein processing the digitally signed multifactor authentication challenge further comprises providing at least one additional confidence factor

for the multifactor authentication challenge that comprises one of a location, a current time of the first computing device, a network identifier, a connected device, an image, or a biometric.

19. A service provider system comprising:

a non-transitory memory; and

one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the service provider system to perform operations comprising:

receiving an authentication request associated with a transaction involving a physical payment card;

issuing an authentication challenge to a computing device associated with the physical payment card, wherein the authentication challenge comprises executable code that causes the computing device and/or the physical payment card to generate a cryptographic signature using a cryptographic function stored on a microchip of the physical payment card;

receiving, from the computing device, a response to the authentication challenge;

determining whether the response comprises the cryptographic signature to the authentication request that is associated with the cryptographic function;

in response to a determination that the response comprises the cryptographic signature, authenticate an account with which the physical payment card is associated; and

in response to a determination that the response does not comprise the cryptographic signature, refuse authentication of the account by preventing the transaction and/or providing increased security to the transaction, the physical payment card, or the account.

20. The service provider system of claim 19, wherein the executable code further causes the computing device to request that the physical payment card be brought within a proximity range associated with short-range wireless signaling of the computing device, and wherein the cryptographic function performs the cryptographic signature responsive to detecting the short-range wireless signaling of the computing device within the proximity range.