CLAIMS

What is claimed is:

1. A contactless card, comprising:

a processor circuit; and

a storage device comprising a controller;

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

receive a request to access the storage device, wherein the storage device is in a locked state;

generate encrypted data based on the request;

transmit the encrypted data to a computing device via a wireless communications interface;

receive, from the computing device, an indication specifying that a server decrypted the encrypted data; and

transmit, to the controller based on the indication specifying that the server decrypted the encrypted data, an indication specifying to unlock the storage device, wherein the controller transitions the storage device from the locked state to an unlocked state based on the indication.

2. The contactless card of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive another request specifying to lock the storage device;

generate another encrypted data;

transmit the another encrypted data to the computing device;

receive, from the computing device, an indication specifying that the server decrypted the another encrypted data; and

transmit, to the controller based on the indication specifying that the server decrypted the another encrypted data, an indication specifying to lock the storage device, wherein the controller transitions the storage device from the unlocked state to the locked state based on the indication to lock the storage device.

3. The contactless card of claim 1, wherein the controller is configured to:

determine that an amount of time elapsed subsequent to unlocking the storage device exceeds a threshold; and

lock the storage device based on the amount of time exceeding the threshold.

4. The contactless card of any one of claims 1 to 3, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive another request to access the storage device;

generate another encrypted data;

transmit the another encrypted data to the computing device;

receive, from the computing device, an indication specifying that the server did not decrypt the another encrypted data; and

reject the another request to access the storage device based on the indication that the server did not decrypt the another encrypted data, wherein the controller maintains the storage device in the locked state.

5. The contactless card of claim 1, further comprising the wireless communications interface, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

transmit, to the computing device via the wireless communications interface, an indication specifying that the storage device is in the unlocked state.

6. The contactless card of claim 5, wherein the storage device comprises a universal serial bus (USB) storage device, wherein the controller is configured to:

determine that a connector of the storage device has been inserted into a USB port; and

expose the unlocked storage device to the USB port.

7. The contactless card of any one of claims 1-3 or 5-6, wherein the requested access comprises one or more of: (i) reading data stored in the storage device, or (ii) writing data to the storage device, wherein the requested access is processed via one or more of: (i) inserting the storage device in a port, or (ii) the wireless communications interface, wherein the wireless communications interface comprises a near field communication (NFC) interface.

8. A method, comprising:

receiving, by an applet executing on a processor of a contactless card via a wireless communications interface of the contactless card, a request to access a storage device of the contactless card, wherein the storage device is in a locked state;

generating, by the applet, encrypted data based on the request;

transmitting, by the applet, the encrypted data to a computing device via the wireless communications interface;

receiving, by the applet from the computing device, an indication specifying that a server decrypted the encrypted data;

transmitting, by the applet to a controller of the storage device and based on the indication specifying that the server decrypted the encrypted data, an indication specifying to unlock the storage device; and

transitioning, by the controller based on the indication received from the applet, the storage device from the locked state to an unlocked state.

9. The method of claim 8, further comprising:

receiving, by the applet, another request specifying to lock the storage device;

generating, by the applet, another encrypted data;

transmitting, by the applet, the another encrypted data to the computing device;

receiving, by the applet from the computing device, an indication specifying that the server decrypted the another encrypted data;

transmitting, by the applet to the controller based on the indication specifying that the server decrypted the another encrypted data, an indication specifying to lock the storage device; and

transitioning, by the controller based on the indication to lock the storage device, the storage device from the unlocked state to the locked state.

10. The method of claim 8, further comprising:

determining, by the controller, an amount of time elapsed subsequent to unlocking the storage device exceeds a threshold; and

transitioning, by the controller based on the determination that the amount of time exceeds the threshold, the storage device from the locked state to the unlocked state.

11. The method of any one of claims 8 to 10, further comprising:

receiving, by the applet, another request to access the storage device;

generating, by the applet, another encrypted data;

transmitting, by the applet, the another encrypted data to the computing device;

receiving, by the applet from the computing device, an indication specifying that the server did not decrypt the another encrypted data; and

rejecting, by the applet, the another request to access the storage device based on the indication that the server did not decrypt the another encrypted data, wherein the controller maintains the storage device in the locked state.

12. The method of claim 8, further comprising:

transmitting, by the applet to the computing device via the wireless communications interface, an indication specifying that the storage device is in the unlocked state.

13. The method of claim 8, wherein the storage device comprises a universal serial bus (USB) storage device, the method further comprising:

determining, by the controller, that a connector of the storage device has been inserted into a USB port; and

exposing, by the controller, the unlocked storage device to the USB port.

14. The method of any one of claims 8-10 or 12-13, wherein the requested access comprises one or more of: (i) reading data stored in the storage device, or (ii) writing data to the storage device, wherein the requested access is processed via one or more of: (i) inserting the storage device in a port, or (ii) the wireless communications interface, wherein the wireless communications interface comprises a near field communication (NFC) interface.

15. A non-transitory computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code when executed by a processor circuit of a contactless card causes the processor circuit to:

receive a request to access a storage device of the contactless card, wherein the storage device is in a locked state;

generate encrypted data based on the request;

transmit the encrypted data to a computing device via a wireless communications interface;

receive, from the computing device, an indication specifying that a server decrypted the encrypted data; and

transmit, to a controller of the storage device based on the indication specifying that the server decrypted the encrypted data, an indication specifying to unlock the storage device, wherein the controller transitions the storage device from the locked state to an unlocked state based on the indication.

16. The non-transitory computer-readable storage medium of claim 15, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to:

receive another request specifying to lock the storage device;

generate another encrypted data;

transmit the another encrypted data to the computing device;

receive, from the computing device, an indication specifying that the server decrypted the another encrypted data; and

transmit, to the controller based on the indication specifying that the server decrypted the another encrypted data, an indication specifying to lock the storage device, wherein the controller transitions the storage device from the unlocked state to the locked state based on the indication to lock the storage device.

17. The non-transitory computer-readable storage medium of claim 15, further comprising computer-readable program code executable by the processor circuit to:

determine an amount of time elapsed subsequent to unlocking the storage device exceeds a threshold; and

transmit, to the controller based on the amount of time exceeding the threshold, an indication to lock the storage device, wherein the controller transitions the storage device from the locked state to the unlocked state based on the indication to lock the storage device.

18. The non-transitory computer-readable storage medium of any one of claims 15 to 17, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to:

receive another request to access the storage device;

generate another encrypted data;

transmit the another encrypted data to the computing device;

receive, from the computing device, an indication specifying that the server did not decrypt the another encrypted data; and

reject the another request to access the storage device based on the indication that the server did not decrypt the another encrypted data, wherein the controller maintains the storage device in the locked state.

19. The non-transitory computer-readable storage medium of claim 15, wherein the storage device comprises a universal serial bus (USB) storage device, further comprising computer-readable program code executable by the controller to cause the controller to:

determine that a connector of the storage device has been inserted into a USB port; and

expose the unlocked storage device to the USB port.

20. The non-transitory computer-readable storage medium of any one of claims 15-17 or 19, wherein the requested access comprises one or more of: (i) reading data stored in the storage device, or (ii) writing data to the storage device, wherein the requested access is processed via one or more of: (i) inserting the storage device in a port, or (ii) the wireless communications interface, wherein the wireless communications interface comprises a near field communication (NFC) interface.