What is claimed is:

1. A method, comprising:

accessing, by a web browser executing on a processor, a web page at a network address based on a link received from a contactless card;

receiving, by the web page, a cryptogram from the contactless card;

transmitting, by the web page, the cryptogram to a server;

determining, by the web page based on a response received from the server, that the server transitioned the contactless card from an inactivated payment state to an activated payment state based on the cryptogram;

generating, by the web page based on the determination that the server transitioned the contactless card from the inactivated payment state to the activated payment state, an instruction to activate a payment applet of the contactless card; and

transmitting, by the web page, the instruction to the contactless card to activate the payment applet of the contactless card.

2. The method of claim 1, further comprising:

determining, by the web page based on the response, that the server decrypted the cryptogram.

3. The method of claim 1, wherein the link comprises a uniform resource locator (URL).

4. The method of claim 1, wherein the instruction to activate the payment applet is configured to transition the payment applet from an inactivated state to an activated state.

5. The method of claim 1, further comprising:

launching, by an operating system executing on the processor, the web browser based on the network address specified by the link.

6. The method of claim 1, further comprising:

transmitting, by the web page, an instruction to the contactless card specifying to generate one or more of the link and the cryptogram.

7. The method of claim 1, further comprising:

receiving, by the web page, an unencrypted customer identifier from the contactless card; and

transmitting, via the web page, the unencrypted customer identifier to the server.

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

access, by a web browser executing on a processor, a web page at a network address based on a link received from a contactless card;

receive, by the web page, a cryptogram from the contactless card;

transmit, by the web page, the cryptogram to a server;

determine, by the web page based on a response received from the server, that the server transitioned the contactless card from an inactivated payment state to an activated payment state based on the cryptogram;

generate, by the web page based on the determination that the server transitioned the contactless card from the inactivated payment state to the activated payment state, an instruction to activate a payment applet of the contactless card; and

transmit, by the web page, the instruction to the contactless card to activate the payment applet of the contactless card.

9. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

determine, by the web page based on the response, that the server decrypted the cryptogram.

10. The computer-readable storage medium of claim 8, wherein the link comprises a uniform resource locator (URL).

11. The computer-readable storage medium of claim 8, wherein the instruction to activate the payment applet is configured to transition the payment applet from an inactivated state to an activated state.

12. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

launch, by an operating system executing on the processor, the web browser based on the network address specified by the link.

13. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

transmit, by the web page, an instruction to the contactless card specifying to generate one or more of the link and the cryptogram.

14. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the web page, an unencrypted customer identifier from the contactless card; and

transmit, via the web page, the unencrypted customer identifier to the server.

15. A computing apparatus comprising:

a processor;

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

access, by a web browser, a web page at a network address based on a link received from a contactless card;

receive, by the web page via the wireless card reader, a cryptogram from the contactless card;

transmit, by the web page, the cryptogram to a server;

receive, by the web page from the server, a response;

determine, by the web page based on the response, that the server transitioned the contactless card from an inactivated payment state to an activated payment state based on the cryptogram;

generate, by the web page based on the determination that the server transitioned the contactless card from the inactivated payment state to the activated payment state, an instruction to activate a payment applet of the contactless card; and

transmit, by the web page, the instruction to the contactless card to activate the payment applet of the contactless card.

16. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

determine, by the web page based on the response, that the server decrypted the cryptogram.

17. The computing apparatus of claim 15, wherein the link comprises a uniform resource locator (URL).

18. The computing apparatus of claim 15, wherein the instruction to activate the payment applet is configured to transition the payment applet from an inactivated state to an activated state.

19. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

launch, by an operating system executing on the processor, the web browser based on the network address specified by the link.

20. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

transmit, by the web page via the wireless card reader, an instruction to the contactless card specifying to generate the network address and the cryptogram.