What is claimed is:

1. An apparatus, comprising:

a processor; and

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

receive a network address for a resource from a contactless card via a wireless card reader, wherein the contactless card is in an inactivated payment state;

access, with a web browser, the resource at the network address received from the contactless card via the card reader;

operate, by the resource in the web browser, the card reader to receive a cryptogram from the contactless card;

transmit, by the resource in the web browser, the cryptogram to a server; and

receive, by the resource in the web browser from the server, a response specifying that the contactless card has been transitioned from the inactivated payment state to an activated payment state.

2. The apparatus of claim 1, the memory comprising instructions that when executed by the processor cause the processor to:

receive, by the resource in the web browser, a decryption result from the server; and

determine, by the resource in the web browser, that the server decrypted the cryptogram.

3. The apparatus of claim 1, the memory comprising instructions that when executed by the processor cause the processor to:

launch, by an operating system executing on the processor, the web browser to access the resource responsive to receiving the network address; and

display, by the resource in the web browser, the response specifying that the contactless card has been transitioned from the inactivated payment state to the activated payment state.

4. The apparatus of claim 1, wherein the network address comprises a uniform resource locator (URL) generated by the contactless card.

5. The apparatus of claim 1, wherein the card reader utilizes near field communication (NFC) to receive the network address for the resource from the contactless card.

6. The apparatus of claim 1, wherein the operation of the card reader includes instructing an applet executing on the contactless card to generate the network address and the cryptogram.

7. The apparatus of claim 1, the memory comprising instructions that when executed by the processor cause the processor to:

receive, by the resource in the web browser, an unencrypted customer identifier with the cryptogram; and

transmit, by the resource in the web browser, the unencrypted customer identifier to the server with the cryptogram.

8. A non-transitory computer-readable medium comprising a set of instructions that, in response to being executed by a processor circuit, cause the processor circuit to:

receive a network address for a resource from a contactless card via a wireless card reader, wherein the contactless card is in an inactivated payment state;

access, with a web browser, the resource at the network address received from the contactless card via the card reader;

operate, by the resource in the web browser, the card reader to receive a cryptogram from the contactless card;

transmit, by the resource in the web browser, the cryptogram to a server; and

receive, by the resource in the web browser from the server, a response specifying that the contactless card has been transitioned from the inactivated payment state to an activated payment state.

9. The non-transitory computer-readable medium of claim 8, comprising instructions that, in response to being executed by the processor circuit, cause the processor circuit to:

receive, by the resource in the web browser, a decryption result from the server; and

determine, by the resource in the web browser, that the server decrypted the cryptogram.

10. The non-transitory computer-readable medium of claim 8, comprising instructions that, in response to being executed by the processor circuit, cause the processor circuit to:

launch, by an operating system executing on the processor circuit, the web browser to access the resource responsive to receiving the network address; and

display, by the resource in the web browser, the response specifying that the contactless card has been transitioned from the inactivated payment state to the activated payment state.

11. The non-transitory computer-readable medium of claim 8, wherein the network address comprises a uniform resource locator (URL) generated by the contactless card.

12. The non-transitory computer-readable medium of claim 8, wherein the card reader utilizes near field communication (NFC) to receive the network address for the resource from the contactless card, wherein the operation of the card reader includes instructing an applet executing on the contactless card to generate the network address and the cryptogram.

13. The non-transitory computer-readable medium of claim 8, comprising instructions that, in response to being executed by the processor circuit, cause the processor circuit to:

receive, by the resource in the web browser, an unencrypted customer identifier with the cryptogram; and

transmit, by the resource in the web browser, the unencrypted customer identifier to the server with the cryptogram.

14. A method, comprising:

receiving, by a computing device, a network address for a resource from a contactless card via a wireless card reader of the computing device, wherein the contactless card is in an inactivated payment state;

accessing, with a web browser executing on the computing device, the resource at the network address received from the contactless card via the card reader;

operating, by the resource in the web browser, the card reader to receive a cryptogram from the contactless card;

transmitting, by the resource in the web browser, the cryptogram to a server; and

receiving, by the resource in the web browser from the server, a response specifying that the contactless card has been transitioned from the inactivated payment state to an activated payment state.

15. The method of claim 14, further comprising:

receiving, by the resource in the web browser, a decryption result from the server; and

determining, by the resource in the web browser, that the server decrypted the cryptogram.

16. The method of claim 14, further comprising:

launching, by an operating system of the device, the web browser to access the resource responsive to receiving the network address; and

displaying, by the resource in the web browser, the response specifying that the contactless card has been transitioned from the inactivated payment state to the activated payment state.

17. The method of claim 14, wherein the network address comprises a uniform resource locator (URL) generated by the contactless card.

18. The method of claim 14, wherein the card reader utilizes near field communication (NFC) to receive the network address for the resource from the contactless card, wherein the operation of the card reader includes instructing an applet executing on the contactless card to generate the network address and the cryptogram.

19. The method of claim 14, further comprising:

receiving, by the resource in the web browser, an unencrypted customer identifier with the cryptogram; and

transmitting, by the resource in the web browser, the unencrypted customer identifier to the server with the cryptogram.

20. The method of claim 19, further comprising:

~~identifying, by the server based on the unencrypted customer identifier, an encryption key and a counter value associated with the contactless card;~~

~~incrementing, by the server, the identified counter value associated with the contactless card;~~

~~encrypting, by the server, the incremented counter value and the encryption key to generate a diversified key associated with the contactless card;~~

~~decrypting the cryptogram by the server using the diversified key;~~

~~storing, by the server based on the decryption of the cryptogram, an indication that the contactless card has been activated;~~

~~receiving, by the server, a request to process a payment using the contactless card; and~~

~~authorizing, by the server, the request based at least in part on the activation of the contactless card.~~

1. A method, comprising:

accessing, by a web browser executing on a processor, a web page at a network address received from a contactless card via a wireless card reader;

receiving, by the web page via the wireless card reader, 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 network address 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:

receiving, by the web page, the network address from the contactless card; and

launching, by an operating system executing on the processor, the web browser responsive to receiving the network address.

6. The method of claim 1, further comprising:

transmitting, by the web page via the wireless card reader, an instruction to the contactless card specifying to generate the network address 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 received from a contactless card via a wireless card reader;

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;

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 network address 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:

receive, by the web page, the network address from the contactless card; and

launch, by an operating system executing on the processor, the web browser responsive to receiving the network address.

13. The computer-readable storage medium of claim 8, 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.

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 wireless card reader; and

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 received from a contactless card via the wireless card reader;

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 network address 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:

receive, by the web page, the network address from the contactless card; and

launch, by an operating system executing on the processor, the web browser responsive to receiving the network address.

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.