CLAIMS

1. A contactless card, comprising:

a memory to store instructions, verification values, and applets, wherein at least a portion of the verification values correspond to other applets not stored in the memory and the verification values are encrypted and stored in a secure portion of the memory; and

processing circuitry, coupled with the memory, operable to execute the instructions, that when executed, cause the processing circuitry to:

perform a verification process to verify a new or updated applet, the verification process to;

retrieve a verification value from the secure portion of the memory, decrypt the verification value, and

compare a verification value received with the new or updated applet with the verification value retrieved from the memory and decrypted;

enable the new or updated applet to execute on the processing circuitry in response to the verification value matching ~~one of~~ the verification value~~s~~ stored in the memory; and

prevent enablement of the new or updated applet in response to the verification value not matching the verification value stored in memory.

2. The contactless card of claim 1, wherein the new or updated applet is signed with the verification value received with the new or updated applet.

3. The contactless card of claim 1, wherein the verification values are stored in the memory during an original equipment manufacturer (OEM) programming process.

4. The contactless card of claim 1, the processing circuitry configured to receive at least one additional verification value from a computing device, and store the at least one additional verification value in the memory, and the at least one additional verification value is received subsequent to the original equipment manufacturer programming process, encrypted and stored in the secure portion of the memory.

5. The contactless card of claim 1, comprising:

one or more contact pads coupled with the memory and the processing circuitry, the one or more contact pads configured to couple with one or more corresponding contact pads of a computing device; and

the processing circuitry configured to receive the new or updated applet from the computing device via the one or more contact pads when coupled with the one or more corresponding contact pads.

6. The contactless card of claim 5, wherein the one or more contact pads are configured to electrically couple with the one or more corresponding contact pads of an EMV writer of the computing device, and the processing circuitry to receive the new or updated applet from the computing device via the EMV writer as one or more signals from the computing device in accordance with an EMV protocol and cause storage of the new or updated applet in at least a portion of memory.

7. The contactless card of the claim 1, the processing circuitry configured to:

determine the new or updated applet is encrypted; and

perform a decryption operation to decrypt the new or updated applet utilizing a key.

8. The contactless card of claim 1, comprising:

an antenna configured to communicate near-field communications;

a near-field communication (NFC) interface coupled with the antenna and the processing circuitry; and

the processing circuitry configured to receive the new or updated applet from another device via the antenna and the NFC interface and in accordance with an NFC protocol.

9. The contactless card of claim 1, wherein the new or updated applet is an updated applet for one of the one of the applets stored on the memory, and the processing circuitry configured to delete a corresponding older version of the new or updated applet from the memory in response to verifying the new or updated applet.

10. The contactless card of claim 1, wherein the new or updated applet is a new applet to store on the memory, and the processing circuitry configured cause storage of the new applet in the memory in response to verifying the new or updated applet.

11. A computer-implemented method, comprising:

storing, in a memory of a contactless card, verification values, and applets, wherein at least a portion of the verification values correspond to other applets not stored in the memory, and the verification values are encrypted and stored in a secure portion of the memory;

performing, by processing circuitry of the contactless card, a verification process to verify a new or updated applet, the verification process comprising:

retrieving a verification value from the secure portion of the memory,

decrypting the verification value,

comparing a verification value received with the new or updated applet with the verification value stored in the secure portion of the memory of a contactless card, and

repeating, retrieving, decrypting, and comparing until the verification value received matches one of the verification values stored in the secure portion of the memory or all of the verification values stored are processed;

enabling, by the processing circuitry of the contactless card, the new or updated applet to execute on the processing circuitry of the contactless card in response to the verification value matching one of the verification values stored in the memory; and

preventing, by the processing circuitry of the contactless card, enablement of the new or updated applet in response to the verification value not matching any of the verification values.

12. The computer-implemented method of claim 11, wherein the new or updated applet is signed with the verification value received.

13. The computer-implemented method of claim 11, wherein the verification values are stored in the memory during an original equipment manufacturer (OEM) programming process.

14. The computer-implemented method of claim 11, comprising receiving at least one additional verification value from a computing device, and storing the at least one additional verification value in the memory subsequent to the OEM programming process.

15. The computer-implemented method of claim 11, comprising receiving the new or updated applet from a computing device via one or more contact pads of the contactless card coupled with one or more corresponding contact pads of the computing device.

16. The computer-implemented method of claim 15, wherein the one or more contact pads are configured to electrically couple with the one or more corresponding contact pads of an EMV writer of the computing device, and the method comprising receiving the new or updated applet from the computing device via the EMV writer as one or more signals from the computing device in accordance with an EMV protocol and cause storage of the new or updated applet in at least a portion of memory.

17. The computer-implemented method of claim 11, comprising: determining the new or updated applet is encrypted; and

performing a decryption operation to decrypt the new or updated applet utilizing a key.

18. The computer-implemented method of claim 11, comprising receiving the new or updated from another via an antenna and an near-field communication (NFC) interface of the contactless card.

19. The computer-implemented method of claim 11, wherein the new or updated applet is an updated applet for one of the one of the applets stored on the memory, and the method comprising deleting a corresponding older version of the new or updated applet from the memory in response to verifying the new or updated applet.

20. The computer-implemented method of claim 11, wherein the new or updated applet is a new applet, and the method comprising storing of the new applet in the memory in response to verifying the new or updated applet.