

TECHNIQUES TO PERFORM APPLLET PROGRAMMING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/503,003, entitled “TECHNIQUES TO PERFORM APPLLET PROGRAMMING” filed on July 3, 2019. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Today credit card users can use their cards at merchants across the country and around the world. Card issuers continue to work tirelessly to increase security and protect cardholders’ personal information, while also providing enhancements and new features. One new technology, is the Europay, Mastercard, Visa (EMV) chip card technology that increasingly being adopted by card issuers and merchants in the United States and around the world. Chip cards feature both the chip and traditional magnetic stripe, so they’re usable even when the merchant doesn’t yet support chip technology. When the card issuer and merchant both support chip technology, the chip card can be inserted into the terminal to complete the transaction. However, one drawback of the current card technology is that they are not easily upgradable in a secure manner. Thus, when there is a problem with the card, Card issuers typically issue a new card and the old card is discarded. This approach is costly and leaves card users without a card while they are waiting for a new card.

SUMMARY

[0002a] According to a first aspect of the present invention, there is provided 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

- 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 compare a verification value associated with the new or updated applet with the verification values;

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

- prevent enablement of the new or updated applet in response to the verification value not matching any of the verification values.

[0002b] According to a second aspect of the present invention, there is provided 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;

performing, by processing circuitry of the contactless card, a verification process to verify a new or updated applet, the verification process to compare a verification value associated with the new or updated applet with the verification values stored in the memory of a contactless card;

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.

[0003] Various embodiments described herein may include a transaction card including a memory to store instructions and one or more verification values, and processing circuitry, coupled with the memory. The processing circuitry operable to execute the instructions, that when executed, cause the processing circuitry to receive, from an automatic teller machine (ATM), an applet signed with a verification signature, the applet comprising instructions capable for execution by the processing circuitry, determine whether the verification signature matches one of the verification values stored on the memory, enable the applet including the instructions for execution by the processing circuitry in response to the determination the verification signature matches one of the verification values, and prevent enablement of the applet including the instructions for execution in response to the determination the verification signature does not match any of the verification values.

[0004] Various embodiments described herein may also include a system, a device, a computing device, etc. including an EMV device, a memory coupled with the EMV device, the memory to store instructions, and processing circuitry coupled with the memory and the EMV device. The processing circuitry operable to execute the instructions, that when executed, cause

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
 - 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 compare a verification value associated with the new or updated applet with the verification values;
 - enable the new or updated applet to execute on the processing circuitry in response to the verification value matching one of the verification values stored in the memory; and
 - prevent enablement of the new or updated applet in response to the verification value not matching any of the verification values.
2. The contactless card of claim 1, wherein the new or updated applet is signed with the verification value.
3. The contactless card of claim 1, wherein the verification values are stored in the memory during original equipment manufacturer 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.
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;
performing, by processing circuitry of the contactless card, a verification process to verify a new or updated applet, the verification process to compare a verification value associated with the new or updated applet with the verification values stored in the memory of a contactless card;

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.

13. The computer-implemented method of claim 11, wherein the verification values are stored in the memory during original equipment manufacturer 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.

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.