user to engage in activity with the associated account. For example, a card that is mailed may be intercepted en route to a user and subject to misuse. Additionally, fraudulent actors may change the address such that the card is reissued to the address of their choice. Further, a card that has been mailed may be read contactlessly through the envelope and the card number may be skimmed.

**[0006]** These and other deficiencies exist. Accordingly, there is a need for systems and methods for authenticating secure card reprovisioning that overcome these deficiencies and results in a transition from a first account to a second account in a secure and reliable manner by protecting communications from interception and unauthorized access.

## SUMMARY OF THE DISCLOSURE

**[0006a]** According to one aspect, there is provided a method of secure reprovisioning of a contactless card storing first personalization data, the method comprising creating a cryptogram; transmitting, via a communication field, the cryptogram to a device; receiving, via the communication field, encrypted data from the device; decrypting the encrypted data to provide decrypted data corresponding to second personalization data; and reprovisioning the contactless card by storing the second personalization data on the contactless card.

**[0006b]** According to another aspect, there is provided a contactless card, comprising a memory storing first personalization data; and a processor, wherein the processor: creates a cryptogram; transmits, via a communication field, the cryptogram to a device; receives, via the communication field, encrypted data from the device; decrypts the encrypted data to provide decrypted data corresponding to second personalization data; and reprovisions the contactless card by storing the second personalization data on the contactless card.

**[0006c]** According to another aspect, there is provided a non-transitory computer-accessible medium storing instructions that, when executed by a computing arrangement, cause the computing arrangement to perform procedures comprising creating a cryptogram; transmitting, via a communication field, the cryptogram to a device; receiving, via the communication field, encrypted data from the device; decrypting the encrypted data to provide decrypted data corresponding to second personalization data; and reprovisioning the contactless card by storing the second personalization data on the contactless card.

**[0007]** Embodiments of the present disclosure provide a secure reprovisioning system. The secure reprovisioning system may include a first device. The first device having an association with a first account. The first device may include a memory containing one or more applets, a counter value, and transmission data. The first device may include a communication interface. The first device may include one or more processors in communication with the memory and communication interface. The first device may be configured to create a cryptogram based on the counter value, wherein the cryptogram includes the counter value and the transmission data. The first device may be configured to transmit, after entry of the communication interface into a communication field, the cryptogram. The first device may be configured to update, after transmission of the cryptogram, the counter value. The first device may be configured to receive, via the communication interface, one or more encrypted keys and one or more parameters. The first device may be configured to decrypt the one or more encrypted keys. The first device may be