WE CLAIM:

1. A secure reprovisioning system, comprising:

a first device having an association with a first account, comprising:

a memory containing one or more applets, a counter value, and transmission data;

a communication interface; and

one or more processors in communication with the memory and the communication interface;

wherein the first device is configured to:

create a cryptogram based on the counter value, wherein the cryptogram includes the counter value and the transmission data,

transmit, after entry of the communication interface into a communication field, the cryptogram,

update, after transmission of the cryptogram, the counter value,

receive, via the communication interface, one or more encrypted keys and one or more parameters,

decrypt the one or more encrypted keys, and

after decryption of the one or more encrypted keys, switch an association from the first account to a second account.

2. The secure reprovisioning system of claim 1, wherein the first device is configured to receive the one or more encrypted keys and the one or more parameters after a determination of a security concern.

~~3. The secure reprovisioning system of claim 1, wherein the first device is subject to one or more eligibility criteria prior to receiving the one or more encrypted keys and the one or more parameters.~~

~~4. The secure reprovisioning system of claim 1, wherein the one or more parameters comprises a primary account number.~~

~~5. The secure reprovisioning system of claim 1, wherein the one or more applets are configured to store the one or more decrypted keys in a secure element.~~

~~6. The secure reprovisioning system of claim 1, wherein the first device is configured to receive the one or more encrypted keys and the one or more parameters on a predetermined time basis.~~

~~7. The secure reprovisioning system of claim 1, wherein the one or more encrypted keys and the one or more parameters are received from a first automated teller machine (ATM) at a first location.~~

~~8. The secure reprovisioning system of claim 1, wherein the first device is restricted to a predetermined use.~~

~~9. The secure reprovisioning system of claim 1, wherein a first applet is configured to transmit, via a communication channel, the one or more decrypted keys and one or more parameters to a second applet.~~

~~10. The secure reprovisioning system of claim 1, wherein the first device is configured to receive a command application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class.~~

~~11. The secure reprovisioning system of claim 10, wherein the first device is configured to transmit, responsive to the command-application protocol data unit, a response-application protocol data unit indicating an execution status associated with the one or more instructions.~~

~~12. A method of secure reprovisioning, comprising:~~

~~creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data;~~

~~transmitting, via a communication interface, the cryptogram;~~

~~updating the counter value;~~

~~receiving, via the communication interface, a first set of one or more encrypted keys and a first set of one or more parameters;~~

~~decrypting the first set of one or more encrypted keys; and~~

~~changing an association from a first account to a second account.~~

~~13. The method of claim 12, further comprising receiving the first set of one or more encrypted keys and the first set of one or more parameters after a determination of a security concern.~~

~~14. The method of claim 12, wherein the association is changed from the first account to the second account in response to a detection of a type of transaction.~~

~~15. The method of claim 12, wherein the first set of one or more encrypted keys and the first set of one or more parameters are received from a first automated teller machine (ATM) at a first location.~~

~~16. The method of claim 15, further comprising:~~

~~receiving, via the communication interface from a second ATM at a second location, a second set of one or more encrypted keys and a second set of one or more parameters;~~

~~decrypting the second set of one or more encrypted keys; and~~

~~changing the association from the second account to the first account.~~

~~17. The method of claim 12, further comprising transmitting a response application protocol data unit indicating an execution status responsive to one or more instructions of a command application protocol data unit.~~

~~18. The method of claim 12, further comprising transmitting, via a communication channel, a first set of one or more decrypted keys and first set of one or more parameters from a first applet to a second applet.~~

~~19. The method of claim 12, further comprising receiving, after input authentication, the first set of one or more encrypted keys and the first set of one or more parameters.~~

~~20. A non-transitory computer-readable medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:~~

~~creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data;~~

~~transmitting, via a communication interface, the cryptogram;~~

~~updating the counter value;~~

~~receiving, via the communication interface, a command application protocol data unit including one or more encrypted keys, one or more parameters, one or more applet identifiers, and one or more instructions associated with a class;~~

~~decrypting the one or more encrypted keys in accordance with the one or more instructions;~~

~~switching an association from a first account to a second account; and~~

~~transmitting a response-application protocol data unit indicating an execution status associated with the one or more instructions.~~

1. 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.

2. The method of secure reprovisioning of claim 1, wherein the cryptogram is created after an entry of the contactless card into the communication field.

3. The method of secure reprovisioning of claim 1, wherein:

the first personalization data comprises one or more first keys, and

the second personalization data comprises one or more second keys.

4. The method of secure reprovisioning of claim 1, wherein storing the second personalization data changes an association of the contactless card from a first account to a second account.

5. The method of secure reprovisioning of claim 1, wherein the contactless card is restricted to a predetermined usage after decrypting the second data.

6. The method of secure reprovisioning of claim 5, wherein the predetermined usage comprises a predetermined spending threshold.

7. The method of secure reprovisioning of claim 1, wherein:

the cryptogram includes transmission data, and

the encrypted data are received following a decryption of the cryptogram and a validation of the transmission data.

8. The method of secure reprovisioning of claim 7, wherein the encrypted data comprises at least one selected from the group of a primary account number information, an expiration date, a card verification code, a spending limit, a public key, and a private key.

9. The method of secure reprovisioning of claim 7, wherein:

the validation of the transmission data is performed by an authentication server communicatively coupled to the device, and

the authentication server receives the transmission data from the device.

10. The method of secure reprovisioning of claim 1, wherein the contactless card receives the encrypted data on a predetermined time basis.

11. The method of secure reprovisioning of claim 1, wherein:

the contactless card is subject to one or more eligibility criteria prior to receiving the encrypted data, and

the one or more eligibility criteria comprise at least one selected from the group of a time elapsed since issuance of the contactless card, usage of the contactless card for transactions, a transaction type, a contactless card type.

12. The method of secure reprovisioning of claim 1, wherein the device comprises a mobile device, a personal computer, a tablet, an automated teller machine (ATM), a wearable device, or a terminal.

13. 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.

14. The contactless card of claim 13, wherein:

the encrypted data is received from an teller machine (ATM) at a first location, and

the encrypted data is generated by an authentication server associated with the contactless card, and

the encrypted data is transmitted by the authentication server to the ATM.

15. The contactless card of claim 14, wherein the device stores an application comprising instructions for execution on an ATM at a second location.

16. The contactless card of claim 13, wherein:

the cryptogram includes transmission data, and

the encrypted data are received following a decryption of the cryptogram and a validation of the and transmission data.

17. The contactless card of claim 13, wherein the processor receives the encrypted data after a determination of a security concern associated with the contactless card.

18. 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.

19. The non-transitory computer-accessible medium of claim 18, wherein the computing arrangement comprises a contactless card.

20. The non-transitory computer-accessible medium of claim 18, wherein storing the second personalization data changes an association of the contactless card from a first account to a second account.