WE CLAIM:

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.