

CLAIMS

What is claimed is:

1. An apparatus, comprising:
 - a processor circuit; and
 - a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
 - initiate, by an application executing on the processor circuit, a request for generation of a barcode;
 - receive, by the application, encrypted data from a communications interface of a contactless card associated with an account, the encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card and generated based on a master key and a counter value stored in the memory of the contactless card;
 - receive, by the application and from a server, verification of the encrypted data;
 - receive, by the application and from the server, an encrypted authorization token associated with the account; and
 - generate the barcode on either i) a computing device associated with the processor circuit or ii) the contactless card utilizing the encrypted authorization token.
2. The apparatus of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
 - scan the barcode; and
 - decrypt the authorization token to authorize a transaction.
3. The apparatus of claim 2, wherein the generated barcode is displayed on the contactless card.
4. The apparatus of claim 3, wherein the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
 - invalidate the authorization token and the barcode for a subsequent transaction after the scanning of the barcode.
5. The apparatus of claim 4, wherein the transaction is a payment transaction and the authorization token is a payment token, and wherein the payment token is associated with a pre-stipulated user limitation in relation to the transaction.
6. The apparatus of claim 3, wherein the encrypted data received from the contactless card is based on a first tap of the contactless card to a computing device.
7. The apparatus of claim 2, wherein the processor circuit is associated with a mobile device, and wherein the barcode is displayed on the mobile device.

8. The apparatus of claim 7, wherein the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:
- invalidate the authorization token and the barcode for a subsequent transaction after the scanning of the barcode.
9. The apparatus of claim 7, wherein the encrypted data received from the contactless card is based on a first tap of the contactless card to a computing device.
10. A method comprising:
- receiving, by an application associated with a computing device and from a user, a first application user credential associated with a user profile;
 - comparing, for a first match and by a processor associated with the application, the first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity;
 - responsive to finding a first match, performing at least one verification operation by the application and in communication with a contactless card to verify the user;
 - responsive to performing the at least one verification operation, generating an encrypted authorization token associated with the account; and
 - generating a barcode on either i) a computing device associated with the processor or ii) the contactless card utilizing the encrypted authorization token.
11. The method of claim 10, wherein performing the at least one verification operation comprises:
- communicating, by the application and using near field communication (NFC), with the contactless card, the contactless card having a radio frequency identification (RFID) chip, the contactless card being within an NFC range of a digital reader associated with the computing device;
 - receiving, by the application and from the contactless card, a public key of a key pair of the contactless card and cardholder identification information of an account holder of the contactless card;
 - instructing, by the application, generation of a digital signature by the contactless card using a private key of the key pair of the contactless card;
 - receiving the digital signature from the contactless card;
 - verifying the digital signature using the public key; and
 - comparing, for a second match and by the processor, at least a portion of the user identity with at least a portion of the cardholder identification information.
12. The method of claim 11, the method further comprising:
- scanning the barcode; and

decrypting the authorization to authorize a transaction.

13. The method of claim 12, wherein the generated barcode is displayed on the contactless card.
14. The method of claim 13, the method further comprising:
invalidating the authorization token and the barcode for a subsequent transaction after the scanning of the barcode.
15. The method of claim 14, wherein the transaction is a payment transaction and the authorization token is a payment token, and wherein the payment token is associated with a pre-stipulated user limitation in relation to the transaction.
16. The method of claim 12, wherein the computer device associated with the processor is a mobile device, and wherein the barcode is displayed on the mobile device.
17. The method of claim 16, the method further comprising:
invalidating the authorization token and the barcode for a subsequent transaction after the scanning of the barcode.
18. The method of claim 17, wherein the transaction is a payment transaction and the authorization token is a payment token.
19. The method of claim 18, wherein the payment token is associated with a pre-stipulated user limitation in relation to the transaction.
20. A contactless card comprising:
a communication interface for communicating with a computing device; and
a processing circuitry for storing information, the information including an authorization token received from a transaction associated with the computing device, wherein the authorization token is embedded in a dynamic barcode projected from a surface of the contactless card, wherein the dynamic barcode is pre-configured by the authorization token to authorize a single transaction, and wherein the barcode and the authorization token are configured to expire after the authorization of the single transaction.