CLAIMS

1. A method, comprising:

receiving, by a first server system, a request to perform an authentication operation to authenticate a user from a second server system, the second server system configured to perform check in operations to access a space secured by a lock;

receiving, by the first server system, from a computing device, encrypted data comprising a unique identifier and a counter value originating from a contactless card via a wireless communication protocol, wherein the encrypted data is generated by the contactless card based on the counter value maintained by the contactless card and encrypted with at least one diversified key and an encryption algorithm;

determining, by the first server system, corresponding information for the contactless card stored by the first server system, the information comprising an authentic unique identifier for the user, a stored counter value for the contactless card, and one more additional diversified keys;

decrypting, by the first server system, the encrypted data with the one or more additional diversified keys to extract the unique identifier and the counter value;

verifying, by the first server system, the unique identifier and the counter value from the contactless card are valid based on the authentic unique identifier and the stored counter value; and

sending, by the first server system, a response to the second server system, the response comprising an indication that the user is authenticated, the second server system is configured to generate a code to provide to the lock to access the space and send the code to the contactless card via the computing device, the contactless card configured to store the code and communicate the code to the lock to access the space.

2. The method of claim 1, wherein the contactless card is one of a smart card or a credit card with capabilities for the wireless communication protocol.

3. The method of claim 1, wherein the computing device and the contactless care configured to communicate via Near Field Communication (NFC).

4. The method of claim 1, wherein the first server system and the second server system are different systems maintained by different entities.

5. The method of claim 4, further comprising storing a room number for the code and storing an identity of a party onto the contactless card.

6. The method of claim 1, wherein the one or more diversified keys and the one or more additional diversified keys are generated from a master key.

7. A method, comprising:

providing a first application associated with a first server system, the first application and the first server system to provide check-in services to gain access to a space via a lock;

performing, by the first application, a check-in process comprising authenticating a user comprising:

communicating, by the first application, an exchange with a contactless card;

receiving, by the first application, encrypted data comprising a unique identifier and a counter value from the contactless card via wireless communications, wherein the encrypted data is encrypted by the contactless card with one or more diversified keys and an encryption algorithm; and

sending, by the first application, the encrypted data to a second server system, wherein the second server system is associated with the contactless card and configured to authenticate the encrypted data;

receiving, by the first application, a code from the first server system based on the encrypted data being authenticated by the second server system, the code serving as a digital key to unlock the lock to access the space; and

communicating, by the first application, a second exchange with the contactless card to send or write the code to the contactless card.

8. The method of claim 7, wherein the first application is executing on a portable computing device comprising one of a smartphone, tablet computing device, a smartwatch, a kiosk computing system, or a wearable device.

9. The method of claim 7, wherein the wireless communication is a Near Field Communication (NFC) communication.

10. The method of claim 7, wherein the first server system and the second server system are different systems maintained by different entities.

11. The method of claim 7, wherein the first application and the first server system are part of a hotel system, and the second server system is part of a banking system.

12. The method of claim 11, wherein the first server system is configured to with the second server system to perform at least a portion of the authenticating the user.

13. A contactless card, comprising:

communication hardware;

a memory configured to store:

a counter value configured to count based on each read operation performed by the contactless card;

identity information regarding a user;

computer program instructions configured to perform wireless payments and authentication operations;

computer program instructions configured to perform locking and unlocking functions;

a processor configured to execute the computer program instructions configured to perform the wireless payments and the authentication operations that cause the processor to:

detect a communication exchange with a computing device, the communication exchange comprising a request to perform an authentication operation;

generate encrypted data comprising the identity information to perform the authentication operation;

send the encrypted data to the computing device to perform the authentication operation;

the processor further configured to execute the computing program instructions configured to perform locking and unlocking functions that cause the processor to:

receive a key code for unlocking a lock in response to the authentication operation being successful;

store the key code in the memory; and

communicate, via the communication hardware, with a lock the key code to perform the locking and unlocking functions.

14. The contactless card of claim 13, wherein the communication hardware enables Near Field Communication (NFC) wireless communications, Bluetooth communications, or both.

15. The contactless card of claim 13, communicating the key code to the lock comprises sending the key code via a Near Field Communication (NFC) protocol or Bluetooth protocol.

16. The contactless card of claim 15, wherein the computer program instructions configured to perform wireless payments and authentication operations is comprised in a first JavaCard applet; and the computer program instructions configured to perform locking and unlocking functions is comprised in a second JavaCard applet.

17. The contactless card of claim 13, wherein the key code is receive from a a mobile phone or a kiosk device.