CLAIMS

1. A computer-implemented method, comprising:

receiving, at an entrance control device of an access-controlled area, a near-field communication signal from a mobile computing device comprising a key storage unit that stores an APP public key and an APP private key;

generating and sending, by the entrance control device, a credit payment request to a user account of a credit payment application (APP) installed on the mobile computing device, the credit payment request including an information field indicating a card information reading message for reading an APP public key certificate;

receiving, by the entrance control device, a payment response message from the mobile computing device, the payment response message including at least one of: a payment card number, an available balance, a station entrance/exit flag, or information about a last transaction;

parsing, by the entrance control device, the payment response message to identify the APP public key certificate;

verifying, by the entrance control device, using a pre-stored credit authorization public key, the APP public key certificate;

determining, by the entrance control device, that the APP public key certificate is successfully verified;

in response to determining that the APP public key certificate is successfully verified, retrieving, by the entrance control device, the APP public key from the APP public key certificate;

calculating a payment amount based on the payment response message;

generating and sending, by the entrance control device, a payment deduction request to the user account of the credit payment APP;

receiving, by the entrance control device, a payment authorization encrypted using asymmetric key encryption from the mobile computing device, wherein the payment authorization includes payment information encrypted by using the APP private key and a transaction authentication code (TAC);

using the APP public key to decrypt the payment authorization;

determining that the payment authorization is successfully decrypted;

in response to determining that the payment authorization is successfully decrypted:

recording, on a storage device, a transaction log, and

granting, by the entrance control device, entry to the access controlled area;

sending the transaction log to a credit payment authorization server to decrypt the transaction authentication code (TAC) of the transaction log; and

receiving a payment from the credit payment authorization server according to the payment amount.

2. The computer-implemented method of claim 1, wherein the station entrance/exit flag indicates an entrance or exit status of a station and the information about the last transaction includes transaction date, transaction time, and station information.

3. The computer-implemented method of claim 2, further comprising rejecting the credit payment request if the payment card number is blacklisted, and the available balance is less than a transaction amount, or the station entrance/exit flag does not match the mobile computing device's entrance or exit status.

4. The computer-implemented method of claim 1, wherein the payment deduction request includes an information field indicating at least one of the payment amount, transaction date and time, the station entrance/exit flag, or station information of a current transaction.

5. The computer-implemented method of claim 1, wherein the TAC is generated based on at least part of the payment information by using a TAC sub-key that is pre-generated.

6. The computer-implemented method of claim 1, wherein the payment information includes the payment amount and at least one of a transaction date and time, the station entrance/exit flag, station information of a current transaction, the payment card number, or a credit limit.

7. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, at an entrance control device of an access-controlled area, a near-field communication signal from a mobile computing device comprising a key storage unit that stores an APP public key and an APP private key;

generating and sending, by the entrance control device, a credit payment request to a

user account of a credit payment application (APP) installed on the mobile computing device, the credit payment request including an information field indicating a card information reading message for reading an APP public key certificate;

receiving, by the entrance control device, a payment response message from the mobile computing device, the payment response message including at least one of: a payment card number, an available balance, a station entrance/exit flag, or information about a last transaction;

parsing, by the entrance control device, the payment response message to identify the APP public key certificate;

verifying, by the entrance control device, using a pre-stored credit authorization public key, the APP public key certificate;

determining, by the entrance control device, that the APP public key certificate is successfully verified;

in response to determining that the APP public key certificate is successfully verified, retrieving, by the entrance control device, the APP public key from the APP public key certificate;

calculating a payment amount based on the payment response message;

generating and sending, by the entrance control device, a payment deduction request to the user account of the credit payment APP;

receiving, by the entrance control device, a payment authorization encrypted using asymmetric key encryption from the mobile computing device, wherein the payment authorization includes payment information encrypted by using the APP private key and a transaction authentication code (TAC);

using the APP public key to decrypt the payment authorization;

determining that the payment authorization is successfully decrypted;

in response to determining that the payment authorization is successfully decrypted:

recording, on a storage device, a transaction log, and

granting, by the entrance control device, entry to the access controlled area;

sending the transaction log to a credit payment authorization server to decrypt the transaction authentication code (TAC) of the transaction log; and

receiving a payment from the credit payment authorization server according to the payment amount.

8. The non-transitory, computer-readable medium of claim 7, wherein the station entrance/exit flag indicates an entrance or exit status of a station and the information about the last transaction includes transaction date, transaction time, and station information.

9. The non-transitory, computer-readable medium of claim 8, further comprising one or more instructions to reject the credit payment request if the payment card number is blacklisted, and the available balance is less than a transaction amount, or the station entrance/exit flag does not match the mobile computing device's entrance or exit status.

10. The non-transitory, computer-readable medium of claim 7, wherein the payment deduction request includes an information field indicating at least one of the payment amount, transaction date and time, the station entrance/exit flag, or station information of a current transaction.

11. The non-transitory, computer-readable medium of claim 7, wherein the TAC is generated based on at least part of the payment information by using a TAC sub-key that is pre-generated.

12. The non-transitory, computer-readable medium of claim 7, wherein the payment information includes the payment amount and at least one of a transaction date and time, the station entrance/exit flag, station information of a current transaction, the payment card number, or a credit limit.

13. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving, at an entrance control device of an access-controlled area, a near-field communication signal from a mobile computing device comprising a key storage unit that stores an APP public key and an APP private key;

generating and sending, by the entrance control device, a credit payment request to a user account of a credit payment application (APP) installed on the mobile computing device,

the credit payment request including an information field indicating a card information reading message for reading an APP public key certificate;

receiving, by the entrance control device, a payment response message from the mobile computing device, the payment response message including at least one of: a payment card number, an available balance, a station entrance/exit flag, or information about a last transaction;

parsing, by the entrance control device, the payment response message to identify the APP public key certificate;

verifying, by the entrance control device, using a pre-stored credit authorization public key, the APP public key certificate;

determining, by the entrance control device, that the APP public key certificate is successfully verified;

in response to determining that the APP public key certificate is successfully verified, retrieving, by the entrance control device, the APP public key from the APP public key certificate;

calculating a payment amount based on the payment response message;

generating and sending, by the entrance control device, a payment deduction request to the user account of the credit payment APP;

receiving, by the entrance control device, a payment authorization encrypted using asymmetric key encryption from the mobile computing device, wherein the payment authorization includes payment information encrypted by using the APP private key and a transaction authentication code (TAC);

using the APP public key to decrypt the payment authorization;

determining that the payment authorization is successfully decrypted;

in response to determining that the payment authorization is successfully decrypted:

recording, on a storage device, a transaction log, and

granting, by the entrance control device, entry to the access controlled area;

sending the transaction log to a credit payment authorization server to decrypt the transaction authentication code (TAC) of the transaction log; and

receiving a payment from the credit payment authorization server according to the payment amount.

14. The computer-implemented system of claim 13, wherein the station entrance/exit flag

indicates an entrance or exit status of a station and the information about the last transaction includes transaction date, transaction time, and station information.

15. The computer-implemented system of claim 14, further comprising one or more operations to reject the credit payment request if the payment card number is blacklisted, and the available balance is less than a transaction amount, or the station entrance/exit flag does not match the mobile computing device's entrance or exit status.

16. The computer-implemented system of claim 13, wherein the payment deduction request includes an information field indicating at least one of the payment amount, transaction date and time, the station entrance/exit flag, or station information of a current transaction.

17. The computer-implemented system of claim 13, wherein the TAC is generated based on at least part of the payment information by using a TAC sub-key that is pre-generated.

18. The computer-implemented system of claim 13, wherein the payment information includes the payment amount and at least one of a transaction date and time, the station entrance/exit flag, station information of a current transaction, the payment card number, or a credit limit.