CLAIMS:

1. A method for mapping a payment account to a mobile cloud account number, comprising:

generating, by a generating device, an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key;

generating, by the generating device, an ICC master key based on at least a master key identifier;

transmitting, by a transmitting device, the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element;

receiving, by a receiving device, a real card account number (RCA) corresponding to a payment account;

identifying, by a processing device, attributes of the RCA;

identifying, by the processing device, a mobile cloud account number (MCA) based on the attributes of the RCA;

receiving, by the receiving device, an issuer private key and an issuer private key certificate;

generating, by the generating device, an ICC public key certificate based on certification of the ICC public key by the issuer private key;

creating, by the processing device, a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, wherein the mobile cloud account data includes at least an issuer public key certificate, the MCA, and the ICC public key certificate;

transmitting, by the transmitting device, the created post issuance script to the mobile device; and

storing, in a mapping database, a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

2. The method of claim 1, wherein identifying a MCA based on the attributes of the RCA includes receiving, by the receiving device, the MCA from an issuer associated with the RCA.

3. The method of claim 1, wherein the identified MCA includes at least a portion of the RCA.

4. The method of claim 3, wherein the portion of the RCA includes at least the last four digits of the RCA.

5. The method of claim 1, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

6. The method of claim 1, wherein the master key identifier is a sixteen or nineteen digit number.

7. A method for processing a financial transaction, comprising:

storing, in a mapping database, a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), wherein (i) the mobile cloud service provider is configured to bi-directionally communicate with point-of-sale (POS) devices of merchants, via associated acquirers and/or issuers; (ii) the master key identifier is a value unique to a mobile device and is provisioned to a secure element of the mobile device, and (iii) the MCA is based on attributes of the RCA;

receiving, by a receiving device of the mobile cloud service provider, from a contactless POS terminal of a merchant, transaction data related to a financial transaction,

receiving, by the receiving device of the mobile cloud service provider, from a mobile device via the contactless POS terminal of the merchant, at least an MCA and a payment cryptogram, wherein the transaction data, the MCA, and the payment cryptogram are received as a first authorization request;

performing, by the mobile cloud service provider, cryptography to validate the MCA and the payment cryptogram received from the mobile device via the contactless POS terminal of the merchant;

when the MCA and payment cryptogram are successfully validated, (i) identifying, in the mapping database of the mobile cloud service provider, a specific mapping record, wherein the specific mapping record includes the MCA included in the first authorization request, and (ii) electronically transmitting, by a transmitting device of the mobile cloud service provider, a second authorization request comprising at least the RCA included in the specific mapping record and the transaction data to a computer system of an issuer associated with the RCA, via a payment network; and

when the MCA and payment cryptogram are not successfully validated, transmitting by the transmitting device of the mobile cloud service provider, an indication of failure of the validation to the contactless POS terminal of the merchant via the payment network without communicating with an issuer computer system.

8. The method of claim 7, further comprising:

provisioning, to a secure element of the mobile device, the MCA.

9. The method of claim 8, further comprising:

receiving, by the receiving device of the mobile cloud service provider, an authorization response from an issuer associated with the RCA, wherein the authorization response includes at least the RCA included in the specific mapping record and an indication of approval or denial of the financial transaction; and

transmitting, by the transmitting device of the mobile cloud service provider, an authorization response including the MCA included in the specific mapping record in response to the authorization request.

10. The method of claim 7, wherein the MCA includes at least a portion of the RCA.

11. The method of claim 10, wherein the portion of the RCA includes at least the last four digits of the RCA.

12. The method of claim 7, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

13. The method of claim 7, wherein the master key identifier is a sixteen or nineteen digit number.

14. The method of claim 7, wherein the payment cryptogram is one of: a dynamic card validation code and an authorization request cryptogram.

15. A method for providing payment credentials for a financial transaction, comprising:

receiving, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier;

storing, in a first location of a secure element of a mobile device, the received personalization data;

receiving, by the receiving device, at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA);

storing, in a database not included in the secure element, the received at least one post issuance script;

receiving, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script; and

executing, by a processing device, the specific post issuance script,

wherein the MCA is based on attributes of a real card account number (RCA).

16. The method of claim 15, further comprising:

generating, by a generating device, a payment cryptogram based on at least a portion of the mobile cloud account data; and

transmitting, via near field communication, at least the generated payment cryptogram and the indicated MCA.

the receiving device is further configured to receive an issuer private key and an issuer private key certificate,

the generating device is further configured to generate an ICC public key certificate based on certification of the ICC public key by the issuer private key,

the processing device is further configured to create a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, the mobile cloud account data including at least an issuer public key certificate, the MCA, and the ICC public key certificate,

the transmitting device is further configured to transmit the created post issuance script to the mobile device, and

the mapping database is configured to store a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

23. The system of claim 22, wherein the processing device is configured to identify the MCA by causing the receiving device to receive the MCA from an issuer associated with the RCA.

24. The system of claim 22, wherein the identified MCA includes at least a portion of the RCA.

25. The system of claim 24, wherein the portion of the RCA includes at least the last four digits of the RCA.

26. The system of claim 22, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

27. The system of claim 22, wherein the master key identifier is a sixteen or nineteen digit number.

28. A system for processing a financial transaction initiated by a secure element of a mobile device, comprising:

a mapping database of a mobile cloud service provider configured to store a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), wherein (i) the mobile cloud service provider is configured to bi-directionally communicated with point-of-sale (POS) devices of merchants, via associated acquirers and/or issuers, (ii) the master key identifier is a value unique to a mobile device and is provisioned to a secure element of the mobile device, and (iii) the MCA is based on attributes of the RCA;

a receiving device of the mobile cloud service provider, configured to receive:

from a contactless POS terminal of a merchant, transaction data related to a financial transaction, and

from a mobile device via the contactless POS terminal of the merchant, at least an MCA and a payment cryptogram,

wherein the transaction data, the MCA and the payment cryptogram are received as a first authorization request;

a validation device of the mobile cloud service provider configured to perform cryptography to validate the MCA and payment cryptogram received from the mobile device via the contactless POS terminal of the merchant;

a processing device of the mobile cloud service provider; and

a transmitting device of the mobile cloud service provider,

wherein when the MCA and payment cryptogram are successfully validated, (i) the processing device is configured to identify, in the mapping database of the mobile cloud service provider, a specific mapping record, said specific mapping record including the MCA included in the first authorization request, and (ii) the transmitting device is configured to transmit a second authorization request comprising at least the RCA included in the identified

specific mapping record and transaction data to a computer system of an issuer associated with the RCA, via a payment network, and

when the MCA and payment cryptogram are not successfully validated, (i) the transmitting device, of the mobile cloud service provider, is configured to transmit an indication of failure of the validation to the contactless POS terminal of the merchant via the payment network without communicating with an issuer computer system.

29. The system of claim 28, wherein the MCA is stored in a secure element of the mobile device.

30. The system of claim 29, wherein

the receiving device of the mobile cloud service provider is further configured to receive an authorization response from an issuer associated with the RCA, the authorization response including at least the RCA included in the specific mapping record and an indication of approval or denial of the financial transaction, and

the transmitting device of the mobile cloud service provider is further configured to transmit an authorization response including the MCA included in the specific mapping record in response to the authorization request.

31. The system of claim 28, wherein the MCA includes at least a portion of the RCA.