

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
 - generating, with a point-of-sale (POS) terminal, a first ciphertext associated with a transaction, the first ciphertext comprising:
 - (i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and
 - (ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising a first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r);
 - communicating, with the POS terminal, the first ciphertext to at least one payment gateway;
 - re-encrypting, with the at least one payment gateway, the first ciphertext value with a first re-encryption key to transform the first ciphertext value encrypted under the first public key (pk_1) to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway;
 - communicating, with the at least one payment gateway, the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;
 - re-encrypting, with the at least one merchant bank, the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank;
 - communicating, with the at least one merchant bank, the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;
 - re-encrypting, with the payment network, the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network;

communicating, with the payment network, the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank;

determining, with the at least one consumer bank, the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and

decrypting, with the at least one consumer bank, the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

2. The computer-implemented method of claim 1, wherein an intermediary server translates between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

3. The computer-implemented method of claim 1, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

4. The computer-implemented method of claim 1, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.

5. A system comprising:

a point-of-sale (POS) terminal including one or more processors, wherein the POS terminal is programmed and/or configured to:

generate a first ciphertext associated with a transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and

(ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising a first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the

first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r); and

communicate the first ciphertext to at least one payment gateway;

the at least one payment gateway including one or more processors,

wherein the at least one payment gateway is programmed and/or configured to:

re-encrypt the first ciphertext value with a first re-encryption key to transform the first ciphertext value encrypted under the first public key (pk_1) to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway; and

communicate the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;

the at least one merchant bank including one or more processors,

wherein the at least one merchant bank is programmed and/or configured to:

re-encrypt the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank; and

communicate the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;

the payment network including one or more processors, wherein the payment network is programmed and/or configured to:

re-encrypt the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network; and

communicate the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank; and

the at least one consumer bank including one or more processors,

wherein the at least one consumer bank is programmed and/or configured to:

determine the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and
decrypt the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

6. The system of claim 5, further comprising:

an intermediary server programmed and/or configured to translate between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

7. The system of claim 5, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

8. The system of claim 5, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.

9. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

generate, with a point-of-sale (POS) terminal, a first ciphertext associated with a transaction, the first ciphertext comprising:

(i) a first ciphertext value associated with a randomly selected key (r), the first ciphertext value encrypted based on the randomly selected key (r) and a generator value (g); and

(ii) a second ciphertext value associated with a first public key (pk_1) of a first pair of keys comprising a first public key (pk_1) and a first secret key (sk_1), the first public key (pk_1) generated based on the first secret key (sk_1) and the generator value (g), the second ciphertext value encrypted based on transaction data associated with the transaction and a symmetric key (K) generated based on the first public key (pk_1) and the randomly selected key (r);

communicate, with the POS terminal, the first ciphertext to at least one payment gateway;

re-encrypt, with the at least one payment gateway, the first ciphertext value with a first re-encryption key to transform the first ciphertext value encrypted under the first public key (pk_1) to a re-encrypted first ciphertext value encrypted under a second public key (pk_2) associated with the at least one payment gateway;

communicate, with the at least one payment gateway, the re-encrypted first ciphertext value and the second ciphertext value to at least one merchant bank;

re-encrypt, with the at least one merchant bank, the re-encrypted first ciphertext value encrypted with a second re-encryption key to transform the re-encrypted first ciphertext value encrypted under the second public key (pk_2) of the at least one payment gateway to a second re-encrypted first ciphertext value under a third public key (pk_3) of the at least one merchant bank;

communicate, with the at least one merchant bank, the second re-encrypted first ciphertext value and the second ciphertext value to a payment network;

re-encrypt, with the payment network, the second re-encrypted first ciphertext value encrypted with a third re-encryption key to transform the second re-encrypted first ciphertext value encrypted under the third public key (pk_3) of the at least one merchant bank to a third re-encrypted first ciphertext value under a fourth public key (pk_4) of the payment network;

communicate, with the payment network, the third re-encrypted first ciphertext value and the second ciphertext value to at least one consumer bank;

determine, with the at least one consumer bank, the symmetric key (K) based on the third re-encrypted first ciphertext value and a secret key of the consumer bank; and

decrypt, with the at least one consumer bank, the second ciphertext value based on the symmetric key (K) to obtain the transaction data.

10. The computer program product of claim 9, wherein an intermediary server translates between multiple different parties by decrypting the second ciphertext value and using a portion of the transaction data to determine routing and a corresponding re-encryption key for a subsequent communication.

11. The computer program product of claim 9, wherein the transaction data includes at least one of a mobile personal identification number (PIN), a card verification number, or a card number associated therewith.

12. The computer program product of claim 9, wherein the second ciphertext value is used to encrypt a personal identification number (PIN) under the randomly selected key (r) protected by the first ciphertext value, and wherein a re-encryption generates a new ciphertext value while the second ciphertext value is unchanged.

13. A method for encrypting an authentication code, comprising:
receiving, at a payment gateway, a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;
communicating, from the payment gateway to a point-of-sale system, the merchant bank public key;
receiving, from the point-of-sale system, at least one re-encryption key, the at least one re-encryption key based on a private key associated with the point-of-sale system and the merchant bank public key;
receiving, from the point-of-sale system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system and corresponding to the private key associated with the point-of-sale system;
determining, with the payment gateway, a re-encryption key from the at least one re-encryption key based on the encrypted transaction data;
re-encrypting, with the payment gateway, the encrypted session key with the re-encryption key; and
communicating, with the payment gateway, the re-encrypted encrypted session key to a merchant bank system.

14. The method of claim 13, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer

associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

15. The method of claim 13, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

16. The method of claim 13, wherein the at least one re-encryption key is generated by the point-of-sale system.

17. The method of claim 13, wherein the private key associated with the point-of-sale system corresponds to a public key, and wherein the private key and public key associated with the point-of-sale system are generated by the point-of-sale system.

18. The method of claim 13, further comprising:
receiving or generating, at a transaction processing system, an issuer public key corresponding to an issuer private key, the issuer public key and the issuer private key associated with an issuer system;
generating, with the transaction processing system, at least one second re-encryption key based on the issuer private key and the merchant bank private key or a second merchant bank private key;
re-encrypting the encrypted session key with the at least one second re-encryption key; and
communicating the re-encrypted encrypted session key to the issuer system.

19. The method of claim 13, further comprising:
generating, by the merchant bank system or the payment gateway, an authorization request message in response to verifying the authentication code; and
communicating, by the merchant bank system or the payment gateway, the authorization request message to a transaction processing system.

20. A method for encrypting an authentication code, comprising:

- generating, with a point-of-sale system, a public key and a private key associated with the point-of-sale system;
- receiving, at the point-of-sale system, a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;
- generating, with a point-of-sale system, at least one re-encryption key based on the private key associated with the point-of-sale system;
- communicating, from the point-of-sale system to a payment gateway, the at least one re-encryption key;
- generating, with the point-of-sale system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with the public key associated with the point-of-sale system; and
- communicating, from the point-of-sale system to the payment gateway, the encrypted transaction data.

21. The method of claim 20, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

22. The method of claim 20, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

23. A method for encrypting an authentication code, comprising:

- generating, with a merchant bank system, a public key and a private key associated with the merchant bank system;

communicating, with the merchant bank system to a payment gateway, the public key associated with the merchant bank system;

receiving, with the merchant bank system from the payment gateway, encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) a re-encrypted encrypted session key comprising an encrypted session key encrypted with a re-encryption key, the encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system; and

decrypting, with the merchant bank system, the re-encrypted encrypted session key based on the private key associated with the merchant bank system.

24. The method of claim 23, further comprising:

generating, with the merchant bank system, an authorization request message in response to verifying the authentication code; and

communicating, with the merchant bank system, the authorization request message to a transaction processing system.

25. A method for encrypting an authentication code, comprising:

receiving or generating, with a transaction processing system, an issuer key pair comprising an issuer public key and a corresponding issuer private key, the issuer key pair associated with an issuer system;

receiving or generating, with the transaction processing system, a merchant bank key pair comprising a merchant bank public key and a corresponding merchant bank private key, the merchant bank key pair associated with a merchant bank system;

generating, with the transaction processing system, at least one re-encryption key based at least partially on the issuer key pair and the merchant bank key pair;

receiving, from the merchant bank system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising a session key encrypted with the merchant bank public key;

re-encrypting the encrypted session key with the at least one re-encryption key; and

communicating the re-encrypted encrypted session key and the encrypted code to the issuer system.

26. The method of claim 25, further comprising:

receiving, with the issuer system, the re-encrypted encrypted session key from the transaction processing system;

decrypting, with the issuer system, the re-encrypted encrypted session key based at least partially on the issuer private key; and

decrypting, with the issuer system, the encrypted code based at least partially on the session key.

27. A system for encrypting an authentication code, comprising a payment gateway including at least one processor programmed or configured to:

receive a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;

communicate, to a point-of-sale system, the merchant bank public key;

receive, from the point-of-sale system, at least one re-encryption key, the at least one re-encryption key based on a private key associated with the point-of-sale system and the merchant bank public key;

receive, from the point-of-sale system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system and corresponding to the private key associated with the point-of-sale system;

determine a re-encryption key from the at least one re-encryption key based on the encrypted transaction data;

re-encrypt the encrypted session key with the re-encryption key; and

communicate the re-encrypted encrypted session key to a merchant bank system.

28. The system of claim 27, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer

associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

29. The system of claim 27, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

30. The system of claim 27, wherein the at least one re-encryption key is generated by the point-of-sale system.

31. The system of claim 27, wherein the private key associated with the point-of-sale system corresponds to a public key, and wherein the private key and public key associated with the point-of-sale system are generated by the point-of-sale system.

32. The system of claim 27, further comprising a transaction processing system including at least one processor programmed or configured to:

receive or generate an issuer public key corresponding to an issuer private key, the issuer public key and the issuer private key associated with an issuer system;

generate at least one second re-encryption key based on the issuer private key and the merchant bank private key or a second merchant bank private key;

re-encrypt the encrypted session key with the at least one second re-encryption key; and

communicate the re-encrypted encrypted session key to the issuer system.

33. The system of claim 27, wherein the at least one processor of the payment gateway or at least one processor of the merchant bank system is programmed or configured to:

generate an authorization request message in response to verifying the authentication code; and

communicate the authorization request message to a transaction processing system.

34. A system for encrypting an authentication code, comprising a point-of-sale system including at least one processor programmed or configured to:

generate a public key and a private key associated with the point-of-sale system;

receive a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;

generate at least one re-encryption key based on the private key associated with the point-of-sale system;

communicate, to a payment gateway, the at least one re-encryption key;

generate encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with the public key associated with the point-of-sale system; and

communicate, to the payment gateway, the encrypted transaction data.

35. The system of claim 34, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

36. The system of claim 34, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

37. A system for encrypting an authentication code, comprising a merchant bank system including at least one processor, the at least one processor programmed or configured to:

generate a public key and a private key associated with the merchant bank system;

communicate, to a payment gateway, the public key associated with the merchant bank system;

receive, from the payment gateway, encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) a re-encrypted encrypted session key comprising an encrypted session key encrypted with a re-encryption key, the encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system; and

decrypt the re-encrypted encrypted session key based on the private key associated with the merchant bank system.

38. The system of claim 37, wherein the at least one processor is further programmed or configured to:

generate an authorization request message in response to verifying the authentication code; and

communicate the authorization request message to a transaction processing system.

39. A system for encrypting an authentication code, comprising a transaction processing system including at least one processor programmed or configured to:

receive or generate an issuer key pair comprising an issuer public key and a corresponding issuer private key, the issuer key pair associated with an issuer system;

receive or generate a merchant bank key pair comprising a merchant bank public key and a corresponding merchant bank private key, the merchant bank key pair associated with a merchant bank system;

generate at least one re-encryption key based at least partially on the issuer key pair and the merchant bank key pair;

receive, from the merchant bank system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code

comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising a session key encrypted with the merchant bank public key;
re-encrypt the encrypted session key with the at least one re-encryption key; and
communicate the re-encrypted encrypted session key and the encrypted code to the issuer system.

40. The system of claim 39, further comprising the issuer system, the issuer system including at least one processor programmed or configured to:
receive the re-encrypted encrypted session key from the transaction processing system;
decrypt the re-encrypted encrypted session key based at least partially on the issuer private key; and
decrypt the encrypted code based at least partially on the session key.

41. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:
receive, at a payment gateway, a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;
communicate, from the payment gateway to a point-of-sale system, the merchant bank public key;
receive, from the point-of-sale system, at least one re-encryption key, the at least one re-encryption key based on a private key associated with the point-of-sale system and the merchant bank public key;
receive, from the point-of-sale system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system and corresponding to the private key associated with the point-of-sale system;
determine, with the payment gateway, a re-encryption key from the at least one re-encryption key based on the encrypted transaction data;

re-encrypt the encrypted session key with the re-encryption key; and
communicate the re-encrypted encrypted session key to a merchant
bank system.

42. The computer program product of claim 41, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

43. The computer program product of claim 41, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

44. The computer program product of claim 41, wherein the at least one re-encryption key is generated by the point-of-sale system.

45. The computer program product of claim 41, wherein the private key associated with the point-of-sale system corresponds to a public key, and wherein the private key and public key associated with the point-of-sale system are generated by the point-of-sale system.

46. The computer program product of claim 41, wherein the one or more processors are further programmed and/or configured to:

receive or generate, at a transaction processing system, an issuer public key corresponding to an issuer private key, the issuer public key and the issuer private key associated with an issuer system;

generate, with the transaction processing system, at least one second re-encryption key based on the issuer private key and the merchant bank private key or a second merchant bank private key;

re-encrypt the encrypted session key with the at least one second re-encryption key; and

communicate the re-encrypted encrypted session key to the issuer system.

47. The computer program product of claim 41, wherein the one or more processors are further programmed and/or configured to:

generate, by the merchant bank system or the payment gateway, an authorization request message in response to verifying the authentication code; and
communicate, by the merchant bank system or the payment gateway, the authorization request message to a transaction processing system.

48. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

generate, with a point-of-sale system, a public key and a private key associated with the point-of-sale system;

receive, at the point-of-sale system, a merchant bank public key corresponding to a merchant bank private key, the merchant bank public key and the merchant bank private key associated with a merchant bank system;

generate, with a point-of-sale system, at least one re-encryption key based on the private key associated with the point-of-sale system;

communicate, from the point-of-sale system to a payment gateway, the at least one re-encryption key;

generate, with the point-of-sale system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising the session key encrypted with the public key associated with the point-of-sale system; and

communicate, from the point-of-sale system to the payment gateway, the encrypted transaction data.

49. The computer program product of claim 48, wherein the point-of-sale system comprises at least one of the following: a point-of-sale terminal, a server computer associated with a merchant or merchant bank system, a server computer associated with a point-of-sale service provider, or any combination thereof.

50. The computer program product of claim 48, wherein the at least one re-encryption key comprises a plurality of re-encryption keys, and wherein each re-encryption key of the plurality of re-encryption keys corresponds with a public key of a plurality of merchant bank public keys, the plurality of merchant bank public keys including the merchant bank public key.

51. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

generate, with a merchant bank system, a public key and a private key associated with the merchant bank system;

communicate, with the merchant bank system to a payment gateway, the public key associated with the merchant bank system;

receive, with the merchant bank system from the payment gateway, encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) a re-encrypted encrypted session key comprising an encrypted session key encrypted with a re-encryption key, the encrypted session key comprising the session key encrypted with a public key associated with the point-of-sale system; and

decrypt, with the merchant bank system, the re-encrypted encrypted session key based on the private key associated with the merchant bank system.

52. The computer program product of claim 51, wherein the one or more processors are further programmed and/or configured to:

generate, with the merchant bank system, an authorization request message in response to verifying the authentication code; and

communicate, with the merchant bank system, the authorization request message to a transaction processing system.

53. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

receive or generate, with a transaction processing system, an issuer key pair comprising an issuer public key and a corresponding issuer private key, the issuer key pair associated with an issuer system;

receive or generate, with the transaction processing system, a merchant bank key pair comprising a merchant bank public key and a corresponding merchant bank private key, the merchant bank key pair associated with a merchant bank system;

generate, with the transaction processing system, at least one re-encryption key based at least partially on the issuer key pair and the merchant bank key pair;

receive, from the merchant bank system, encrypted transaction data for a transaction, the encrypted transaction data comprising: (i) an encrypted code comprising an authentication code encrypted with a session key, and (ii) an encrypted session key comprising a session key encrypted with the merchant bank public key;

re-encrypt the encrypted session key with the at least one re-encryption key; and

communicate the re-encrypted encrypted session key and the encrypted code to the issuer system.

54. The computer program product of claim 53, wherein the instructions further cause the at least one processor to:

receive, with the issuer system, the re-encrypted encrypted session key from the transaction processing system;

decrypt, with the issuer system, the re-encrypted encrypted session key based at least partially on the issuer private key; and

decrypt, with the issuer system, the encrypted code based at least partially on the session key.