

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

_____generating, with an electronic wallet transaction processing system, an electronic wallet key pair including an electronic wallet public key and a corresponding electronic wallet secret key, the electronic wallet key pair associated with the electronic wallet transaction processing system;

_receiving, with the electronic wallet transaction processing system, a payment gateway public key corresponding to a payment gateway secret key, the payment gateway public key and the payment gateway secret key associated with a payment gateway system;

_generating, with the electronic wallet transaction processing system, a public re-encryption key based on the payment gateway public key;

communicating, from the electronic wallet transaction processing system to the payment gateway system, the public re-encryption key;

_wherein the public re-encryption key is a proxy re-encryption key;
receiving or determining, with the electronic wallet transaction processing system, encrypted transaction data associated with a transaction, the encrypted transaction data including an account identifier encrypted with the electronic wallet public key;

_re-encrypting, with the electronic wallet transaction processing system, the encrypted transaction data with the public re-encryption key; and

_communicating, from the electronic wallet transaction processing system to the payment gateway system, the re-encrypted transaction data.

2. The computer-implemented method of claim 1, further comprising:

_____receiving, with the electronic wallet transaction processing system, user credentials associated with a user for the transaction; and

_____authenticating, with the electronic wallet transaction processing system, the user for the transaction based on the user credentials, wherein authenticating the user for the transaction includes re-encrypting the encrypted transaction data with the public re-encryption key and communicating the re-encrypted transaction data to the payment gateway system.

3. The computer-implemented method of claim 2, wherein the electronic wallet transaction processing system authenticates the user for the transaction based on the user credentials without decrypting the encrypted transaction data including the account identifier encrypted with the electronic wallet public key.

4. The computer-implemented method of claim 2, further comprising:

_____storing, with the electronic wallet transaction processing system in an in-memory database, the account identifier encrypted with the electronic wallet public key in association with the user credentials.

5. The computer-implemented method of claim 2, wherein the electronic wallet transaction processing system communicates the re-encrypted transaction data to the payment gateway system via a merchant system.

6. The computer-implemented method of claim 5, wherein the electronic wallet transaction processing system receives the user credentials associated with the user for the transaction from the merchant system.

7. The computer-implemented method of claim 1, further comprising:

 _receiving, with the payment gateway system, the re-encrypted transaction data;

 decrypting, with the payment gateway system, the re-encrypted transaction data based at least partially on the payment gateway secret key; and

 _identifying, with the payment gateway, the account identifier.

8. A system comprising:

_an electronic wallet transaction processing system including one or more processors programmed and/or configured to:

_generate an electronic wallet key pair including an electronic wallet public key and a corresponding electronic wallet secret key, the electronic wallet key pair associated with the electronic wallet transaction processing system;

_receive a payment gateway public key corresponding to a payment gateway secret key, the payment gateway public key and the payment gateway secret key associated with a payment gateway system;

_generate a public re-encryption key based on the payment gateway public key;

_communicate, to the payment gateway system, the public re-encryption key;

, wherein the public re-encryption key is a proxy re-encryption key; receive or determine encrypted transaction data associated with a transaction, the encrypted transaction data including an account identifier encrypted with the electronic wallet public key;

_re-encrypt the encrypted transaction data with the public re-encryption key; and

_communicate, to the payment gateway system, the re-encrypted transaction data.

9. The system of claim 8, wherein the electronic wallet transaction processing system including the one or more processors is further programmed and/or configured to:

_____receive user credentials associated with a user for the transaction;
and

_____authenticate the user for the transaction based on the user credentials, wherein authenticating the user for the transaction includes re-encrypting the encrypted transaction data with the public re-encryption key and communicating the re-encrypted transaction data to the payment gateway system.

10. The system of claim 9, wherein the electronic wallet transaction processing system including the one or more processors authenticates the user for the transaction based on the user credentials without decrypting the encrypted transaction data including the account identifier encrypted with the electronic wallet public key.

11. The system of claim 9, wherein the electronic wallet transaction processing system including the one or more processors is further programmed and/or configured to:

_____store, in an in-memory database, the account identifier encrypted with the electronic wallet public key in association with the user credentials.

12. The system of claim 9, wherein the electronic wallet transaction processing system including the one or more processors communicates the re-encrypted transaction data to the payment gateway system via a merchant system.

13. The system of claim 12, wherein the electronic wallet transaction processing system including the one or more processors receives the user credentials associated with the user for the transaction from the merchant system.

14. The system of claim 8, further comprising:

 the payment gateway system including one or more processors programmed and/or configured to:

 receive the re-encrypted transaction data;

 decrypt the re-encrypted transaction data based at least partially on the payment gateway secret key; and

 identify the account identifier.

15. 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 an electronic wallet key pair including an electronic wallet public key and a corresponding electronic wallet secret key, the electronic wallet key pair associated with the electronic wallet transaction processing system;

 _receive a payment gateway public key corresponding to a payment gateway secret key, the payment gateway public key and the payment gateway secret key associated with a payment gateway system;

 _generate a public re-encryption key based on the payment gateway public key;

 communicate, to the payment gateway system, the public re-encryption key;

, wherein the public re-encryption key is a proxy re-encryption key;
 receive or determine encrypted transaction data associated with a transaction, the encrypted transaction data including an account identifier encrypted with the electronic wallet public key;

 _re-encrypt the encrypted transaction data with the public re-encryption key; and

 _communicate, to the payment gateway system, the re-encrypted transaction data.

16. The computer program product of claim 15, wherein the instructions further cause the at least one processor to:

_____receive user credentials associated with a user for the transaction;
and

_____authenticate the user for the transaction based on the user credentials, wherein authenticating the user for the transaction includes re-encrypting the encrypted transaction data with the public re-encryption key and communicating the re-encrypted transaction data to the payment gateway system.

17. The computer program product of claim 16, wherein the instructions cause the at least one processor to authenticate the user for the transaction based on the user credentials without decrypting the encrypted transaction data including the account identifier encrypted with the electronic wallet public key.

18. The computer program product of claim 16, wherein the instructions further cause the at least one processor to:

_____store, in an in-memory database, the account identifier encrypted with the electronic wallet public key in association with the user credentials.

19. The computer program product of claim 16, wherein the instructions cause the at least one processor to:

 _communicate the re-encrypted transaction data to the payment gateway system via a merchant system; and

 receive the user credentials associated with the user for the transaction from the merchant system.

20. The computer program product of claim 15, wherein the instructions further cause the at least one processor to:

 _receive the re-encrypted transaction data;

 decrypt the re-encrypted transaction data based at least partially on the payment gateway secret key; and

 _identify the account identifier.