Claims

1. A payment processing system comprising:
    a. a module (209) configured to:
        i. receive a payment request (303) for a payment transaction from one of a plurality of different merchant applications associated with a computing device (100) wherein the request comprises payment information comprising a merchant code or transaction identifier;
        ii. in response to receiving the payment request, receive (304) encrypted payment data from a reader (210) coupled to the computing device (100) wherein the payment data comprises an account number associated with a user wherein the account number is encrypted according to a first key; and
        iii. transmit (311) the payment information and the encrypted payment data to a payment server (211) to determine a payment service provider associated with the merchant code,

            wherein the module is configured to cause, based on the determined payment service provider, the encrypted payment data to be transmitted to a security module and wherein the security module is configured to decrypt the encrypted payment data using an encryption key associated with the determined payment service provider.

2. The payment processing system according to claim 1 wherein the module is further configured to determine a location identifier associated with an application (205) based on the location of the hardware on which the application is installed and preferably to determine a workstation identifier associated with the hardware and further preferably to determine a merchant code based on a received merchant code.

3. The payment processing system according to claim 1 wherein the module is further configured to receive (304) further encrypted payment data comprising a PIN number encrypted according to a second key for the PIN number wherein the first key is different from the second key.

4. The payment processing system according to any preceding claim wherein the module (209) is further configured to transmit data comprising any one or more of a merchant code, a workstation name, and a location identifier or code to the payment

server (211) and preferably wherein the module (209) is further configured to transmit further data comprising a serial device number, a transaction identifier for merchant tracking information to the payment server (211) and preferably wherein the data transmitted from the module (209) to the payment server (211) is transmitted in a source identifier message.

5. The payment processing system of any preceding claim wherein the payment request (303) comprises device information in particular any one or more of the or a device serial number, a terminal type, the or a transaction number, the or a merchant code as well as location information associated with the computing device (100) or the or a location identifier or code.

6. The payment processing system according to any preceding claim wherein the module (209) is further configured to transmit data which allows the payment request to be routed from one of a plurality of different merchants in different regions to one of a plurality of different payment service providers in each region.

7. The payment processing system according to any preceding claim wherein the module (209) is further configured to determine one of a plurality of different payment service providers to route the payment request to based on any one or more of a merchant code and the or a location information or code and preferably a workstation identifier and a particular payment service provider identifier and a comparison with a look-up table.

8. The payment processing system according to any preceding claim further comprising a second module (215) configured to receive an encrypted payment service provider key from a server.

9. The payment processing system according to any preceding claim wherein the or a second module (215) is configured to perform a key exchange function with a Payment Service provider associated with the merchant or transaction and preferably wherein the module (215) is configured to perform the key exchange ceremony based on a source ID or source identifier.

10. The payment processing system according to claim 7 wherein the second module (215) determines which of a plurality of payment service provider keys to transmit to a third module (216) preferably based on a look-up table of a plurality of payment

service provider identifiers and associated payment service provider keys and preferably wherein each payment service provider key is encrypted.

11. The payment processing system according to any preceding claim wherein the second module (215) is configured to transmit the encrypted payment data and the encrypted payment service provider key to a further security module (216).

12. The payment processing system according to any preceding claim wherein the or a further security module (216) is configured to decrypt the encrypted payment data using the first key and preferably using the second key.

13. The payment processing system according to any preceding claim wherein the or a further security module (216) is further configured to decrypt the encrypted payment service provider key using a further key and to re-encrypt the decrypted payment data using the decrypted payment service provider key.

14. The payment processing system according to any preceding claim wherein the or a security module (216) is further configured to encrypt the payment data according to a particular payment service provider format.

15. The payment processing system according to any preceding claim wherein the or a further security module (216) is further configured to transmit the payment data encrypted using the payment service provider key to the security module (215).

16. The payment processing system according to any preceding claim wherein the or a security module (215) is further configured to transmit the payment data encrypted using the payment service provider key to the payment server (211).

17. The payment processing system according to any one of claims 5 to 13 wherein the payment server (211) is further configured to transmit the payment data to a particular payment service provider preferably based on the determined payment service provider identifier.

18. The payment processing system according to any preceding claim wherein the reader (210) is further configured to receive a validation response to the payment request preferably via the module (209) and further preferably via the payment server (211).

19. The payment processing system according to any preceding wherein the payment data is encrypted at a message level and preferably wherein the payment data comprises payment card information in particular any one or more of a card number, expiry date, owner name, security code and payment transition validation data.

20. The payment processing system according to any preceding claim wherein the payment data is encrypted at all stages between the reader (210) and a payment service provider (217).

21. A method of processing a payment transaction, the method comprising:

i. receiving, by a gateway, a payment request for a payment transaction from one of a plurality of different merchant applications associated with a computing device, wherein the payment request comprises payment information comprising a merchant code;

ii. in response to receiving the payment request, receiving encrypted payment data from a reader coupled to the computing device, wherein the payment data comprises an account number associated with a user and wherein the account number is encrypted according to a first key; and

iii. transmitting the payment information and the encrypted payment data to a payment server to determine a payment service provider associated with the merchant code, and causing, based on the determined payment service provider, the encrypted payment data to be transmitted to a security module wherein the security module is configured to decrypt the encrypted payment data using the first key and to re-encrypt the decrypted payment data using an encryption key associated with the determined payment service provider.

22. A computer program product which when executed performs a method according to claim 21.