WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by an access device, a personal identification number (PIN) and sensitive data;

encrypting, by the access device, the PIN, wherein PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, the sensitive data, wherein sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

2. The method of claim 1, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

3. The method of claim 1, wherein at least one of the PIN and the sensitive data are encrypted using Triple DES Encryption Algorithm (TDEA).

4. The method of claim 1, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

5. The method of claim 1, wherein a subset of discretionary data remains unencrypted when discretionary data is included in encrypted sensitive data.

6. The method of claim 1, wherein an encrypted PAN is written to the PAN field of the authorization request message, wherein the encrypted PAN has the same format as the unencrypted PAN.

7. The method of claim 6, wherein a subset of digits of the unencrypted PAN remain unencrypted in the encrypted PAN.

8. The method of claim 6, wherein an expiration date field of the authorization request message is overwritten with an altered expiration date to indicate that the PAN field of the authorization request message contains an encrypted PAN.

9. A method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes encrypted sensitive data;

decrypting, by a secure module communicatively connected to the merchant server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the host server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes the re-encrypted sensitive data.

10. The method of claim 9, wherein the authorization request message further includes an encrypted PIN, the method further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

11. The method of claim 10, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

12. The method of claim 9, wherein the encrypted PIN is encrypted using a first encryption key variant based on an initial key and the encrypted sensitive data is encrypted using a second encryption key variant based on the initial key.

13. The method of claim 12, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

14. The method of claim 9, wherein the secure device is a hardware security module.

15. The method of claim 9, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

16. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method of routing transactions, the method comprising:

encrypting, by an access device, a personal identification number (PIN), wherein the PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, sensitive data, wherein the sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

17. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes encrypted sensitive data;

decrypting, by a secure module communicatively connected to the merchant server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the merchant server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes re-encrypted sensitive data.

18. The method of claim 17, wherein the authorization request message further includes an encrypted PIN, the method further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

19. The system of claim 17, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption of a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

20. The system of claim 17, wherein the system includes a hardware security module.

21. A method, comprising:

receiving data associated with a personal account identifier (PAI)

encrypting, by the access device, the PAI, wherein the encrypted PAI has the same format as the PAI;

writing the encrypted PAI to a field of an authorization request message, wherein the field is designated to receive a PAI;

using an authorization request message data element as a signal to identify the presence of the encrypted PAI in the authorization request message; and

transmitting the authorization request message.

22. The method of claim 21, wherein the PAI is a primary account number (PAN), wherein a subset of digits of the encrypted PAN in the authorization request message are unencrypted digits of the PAN.

23. The method of claim 21, wherein the first six digits of the encrypted PAN are the same as the first six digits of the unencrypted PAN and wherein the last four digits of the encrypted PAN are the same as the last six digits of the unencrypted PAN.

24. The method of claim 22, further comprising calculating a value for a designated digit of the encrypted PAN such that the last digit of the unencrypted PAN is the same as the last digit of the encrypted PAN and wherein the last digit of the encrypted PAN is a valid check digit for the encrypted PAN.

25. The method of claim 21, wherein the authorization request message includes an expiration date, and wherein the expiration date field of the authorization request message is overwritten with an altered expiration date when the PAI field of the authorization request message contains an encrypted PAI.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by an access device, a personal identification number (PIN) and sensitive data;

encrypting, by the access device, the PIN, wherein PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, the sensitive data, wherein sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

2. The method of claim 1, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

3. The method of claim 1, wherein at least one of the PIN and the sensitive data are encrypted using Triple DES Encryption Algorithm (TDEA).

4. The method of claim 1, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

5. The method of claim 1, wherein a subset of discretionary data remains unencrypted when discretionary data is included in encrypted sensitive data.

6. The method of claim 1, wherein an encrypted PAN is written to the PAN field of the authorization request message, wherein the encrypted PAN has the same format as the unencrypted PAN.

7. The method of claim 6, wherein a subset of digits of the unencrypted PAN remain unencrypted in the encrypted PAN.

8 . The method of claim 6, wherein an expiration date field of the authorization request message is overwritten with an altered expiration date to indicate that the PAN field of the authorization request message contains an encrypted PAN.

9. A method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes an encrypted PIN that was encrypted using a first encryption key variant based on an initial key, and encrypted sensitive data that was encrypted using a second encryption key variant based on the initial key;

decrypting, by a secure module communicatively connected to the merchant server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the host server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes the re-encrypted sensitive data.

10. The method of claim 9, further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

11. The method of claim 10, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

12. The method of claim 9, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

13. The method of claim 9, wherein the decrypting of the encrypted sensitive data, and the re-encrypting of the decrypted sensitive data are performed by a hardware security module acting as the secure module.

14. The method of claim 9, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

15. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method of routing transactions, the method comprising:

encrypting, by an access device, a personal identification number (PIN), wherein the PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, sensitive data, wherein the sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

16. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes an encrypted PIN that was encrypted using a first encryption key variant based on an initial key, and encrypted sensitive data that was encrypted using a second encryption key variant based on the initial key;

decrypting, by a secure module communicatively connected to the merchant server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the merchant server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes re-encrypted sensitive data.

17. The method of claim 16, further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

18. The system of claim 16, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption of a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

19. The system of claim 16, wherein the system includes a hardware security module.

20. A method, comprising:

receiving data associated with a personal account identifier (PAI)

encrypting, by the access device, the PAI, wherein the encrypted PAI has the same format as the PAI;

writing the encrypted PAI to a field of an authorization request message, wherein the field is designated to receive a PAI;

using an authorization request message data element as a signal to identify the presence of the encrypted PAI in the authorization request message; and

transmitting the authorization request message.

21. The method of claim 20, wherein the PAI is a primary account number (PAN), wherein a subset of digits of the encrypted PAN in the authorization request message are unencrypted digits of the PAN.

22. The method of claim 20, wherein the first six digits of the encrypted PAN are the same as the first six digits of the unencrypted PAN and wherein the last four digits of the encrypted PAN are the same as the last six digits of the unencrypted PAN.

23. The method of claim 21, further comprising calculating a value for a designated digit of the encrypted PAN such that the last digit of the unencrypted PAN is the

same as the last digit of the encrypted PAN and wherein the last digit of the encrypted PAN is a valid check digit for the encrypted PAN.

24. The method of claim 20, wherein the authorization request message includes an expiration date, and wherein the expiration date field of the authorization request message is overwritten with an altered expiration date when the PAI field of the authorization request message contains an encrypted PAI.