

CLAIMS

Therefore, the following is claimed:

1. A system, comprising:

a computing device comprising a processor and a memory; and

machine-readable instructions stored in the memory that, when executed by the processor, cause the computing device to at least:

receive a merchant identifier and a transaction amount for a transaction from a merchant terminal;

receive the merchant identifier and encrypted payment account data for the transaction from a digital wallet;

decrypt the encrypted payment account data to generate payment account data;

identify the payment network to be used for the transaction from a plurality of supported payment networks;

generate an authorization request cryptogram based at least in part on an identification of the payment network;

generate an authorization request for the transaction based at least in part on the authorization request cryptogram, the merchant identifier, the transaction amount, and the payment account data;

send the authorization request to a payment processor, the payment processor being configured to route the authorization request to an authorizing entity via a payment network;

receive an authorization response from the authorizing entity via the payment processor; and

forward the contents of the authorization response to the merchant terminal.

2. The system of claim 1, wherein:

the encrypted payment account data include a cryptogram generating key and an application transaction counter (ATC) value; and

the authorization request cryptogram is generated based at least in part on the ATC value and the cryptogram generating key.

3. The system of any of claims 1-2, wherein the machine-readable instructions further cause the computing device to at least:

receive a transaction identifier for the transaction from the merchant terminal in conjunction with the merchant identifier and the transaction amount;

receive the transaction identifier for the transaction from a client device in conjunction with the merchant identifier and the encrypted payment account data;

link the transaction amount, merchant identifier, and the encrypted payment account data to the transaction based at least in part on the transaction identifier; and

wherein the authorization request for the transaction is generated in response to the transaction amount, merchant identifier, and the encrypted payment account data being linked and/or, wherein the machine-readable instructions that cause the

computing device to forward the contents of the authorization response on to the merchant terminal, when executed by the computing device, further cause the computing device to at least:

- evaluate the authorization response received from the authorizing entity via the payment processor for a subset of data contained in the authorization response;
- and

- forward the subset of the data contained in the authorization response to the merchant terminal.

4. The system of any of claims 1-2, wherein the machine-readable instructions that cause the computing device to generate the authorization request cryptogram, when executed by the processor, further cause the computing device to at least:

- create a derived cryptogram generating key from a master cryptogram generating key; and

- generate the authorization request cryptogram using the derived cryptogram generating key.

5. A computer-implemented method, comprising:

- receiving a merchant identifier and a transaction amount for a transaction from a merchant terminal;

- receiving the merchant identifier and encrypted payment account data for the transaction from a digital wallet;

decrypting the encrypted payment account data to generate payment account data;

identifying the payment network to be used for the transaction from a plurality of supported payment networks;

generating an authorization request cryptogram based at least in part on an identification of the payment network;

generating an authorization request for the transaction based at least in part on the authorization request cryptogram; the merchant identifier, the transaction amount, and the payment account data;

sending the authorization request to a payment processor, the payment processor being configured to route the authorization request to an authorizing entity via a payment network;

receiving an authorization response from the authorizing entity via the payment processor; and

forwarding the contents of the authorization response to the merchant terminal.

6. The computer-implemented method of claim 5, wherein:

the encrypted payment account data include a cryptogram generating key and an application transaction counter (ATC) value; and

the authorization request cryptogram is generated based at least in part on the ATC value and the cryptogram generating key.

7. The computer-implemented method of any of claims 5-6, further comprising:

- receiving a transaction identifier for the transaction from the merchant terminal in conjunction with the merchant identifier and the transaction amount;
- receiving the transaction identifier for the transaction from a client device in conjunction with the merchant identifier and the encrypted payment account data;
- linking the transaction amount, merchant identifier, and the encrypted payment account data to the transaction based at least in part on the transaction identifier; and
- wherein the authorization request for the transaction is generated in response to the transaction amount, merchant identifier, and the encrypted payment account data being linked.

8. The computer-implemented method of any of claims 5-7, further comprising:

- verifying an authorization response cryptogram included in the authorization response; and
- wherein forwarding the contents of the authorization response to the merchant terminal occurs in response to verifying the authorization response cryptogram and/or wherein forwarding the contents of the authorization response on to the merchant terminal further comprises:
 - evaluating the authorization response received from the authorizing entity via the payment processor for a subset of data contained in the authorization response; and
 - forwarding the subset of the data contained in the authorization response to the merchant terminal.

9. A computer program or computer program product comprising instructions, or a computer-readable medium storing instructions, that when executed by a processor of a computer system cause the computer system to at least:

receive a merchant identifier and a transaction amount for a transaction from a merchant terminal;

receive the merchant identifier and encrypted payment account data for the transaction from a digital wallet;

decrypt the encrypted payment account data to generate payment account data;

identify the payment network to be used for the transaction from a plurality of supported payment networks;

generate an authorization request cryptogram based at least in part on an identification of the payment network;

generate an authorization request for the transaction based at least in part on the authorization request cryptogram, the merchant identifier, the transaction amount, and the payment account data;

send the authorization request to a payment processor, the payment processor being configured to route the authorization request to an authorizing entity via a payment network;

receive an authorization response from the authorizing entity via the payment processor; and

forward the contents of the authorization response to the merchant terminal.

10. The computer program, computer program product or computer readable medium of claim 9, wherein:

the encrypted payment account data include a cryptogram generating key and an application transaction counter, ATC, value; and

the authorization request cryptogram is generated based at least in part on the ATC value and the cryptogram generating key.

11. The computer program, computer program product or computer readable medium of any of claims 9-10 wherein the instructions further cause the computing device to at least:

receive a transaction identifier for the transaction from the merchant terminal in conjunction with the merchant identifier and the transaction amount;

receive the transaction identifier for the transaction from a client device in conjunction with the merchant identifier and the encrypted payment account data;

link the transaction amount, merchant identifier, and the encrypted payment account data to the transaction based at least in part on the transaction identifier; and

wherein the authorization request for the transaction is generated in response to the transaction amount, merchant identifier, and the encrypted payment account data being linked and/or, wherein the instructions that cause the computing device to forward the contents of the authorization response on to the merchant terminal, when executed by the computing device, further cause the computing device to at least:

evaluate the authorization response received from the authorizing entity via the payment processor for a subset of data contained in the authorization response; and

forward the subset of the data contained in the authorization response to the merchant terminal.

12. The computer program, computer program product or computer-readable medium of any of claims 9-11, wherein:

the instructions, when executed by the processor, further cause the computing device to at least create a derived cryptogram generating key from a master cryptogram generating key; and

the instructions that cause the computing device to generate the authorization request cryptogram, when executed by the processor, further cause the computing device to at least generate the authorization request cryptogram using the derived cryptogram generating key.

13. The computer-implemented method of any of claims 5-8, further comprising:

creating a derived cryptogram generating key from a master cryptogram generating key; and

wherein the derived cryptogram generating key is used in generating the authorization request cryptogram.

14. The system of any of claims 1-4, or the computer program, computer program product or computer-readable medium of any of claims 9-12, wherein:

the instructions, when executed by the processor, further cause the computing device to at least verify an authorization response cryptogram included in the authorization response; and

the instructions that forward the contents of the authorization response to the merchant terminal, when executed by the processor, further causes the computer to forward the contents of the authorization response to the merchant terminal in response to verifying the authorization response cryptogram.

15. The system of any of claims 1-4 and/or 14, or the computer-implemented method of any of claims 5-8 and/or 13, or the computer program, computer program product or computer-readable medium of any of claims 9-12 and/or 14, wherein the authorization request cryptogram is formatted to comply with the ISO 8583 1100 standard.