

WHAT IS CLAIMED IS:

1. A method comprising:
 - providing, by a remote computer, a first transaction cryptogram generation key to a communication device;
 - receiving, by the remote computer, transaction information for each transaction conducted by the communication device using the first transaction cryptogram generation key;
 - receiving, by the remote computer, a replenishment request for a second transaction cryptogram generation key, the replenishment request including transaction log information derived from transaction data stored in a transaction log on the communication device, the transaction data being unique for each transaction conducted by the communication device using the first transaction cryptogram generation key;
 - verifying, by the remote computer, that the transaction log information in the replenishment request is consistent with the previously received transaction information; and
 - providing, by the remote computer, the second transaction cryptogram generation key to the communication device in response to verifying the transaction log information in the replenishment request.
2. The method of claim 1, wherein providing the second transaction cryptogram generation key to the communication device includes providing, to the communication device, a key index that includes information pertaining to generation of the second transaction cryptogram generation key.
3. The method of claim 2, wherein the key index includes at least one of:
 - time information indicating when the second transaction cryptogram generation key is generated; and
 - a replenishment counter value indicating a number of times that the communication device has been replenished with a transaction cryptogram generation key.
4. The method of claim 2, wherein the key index includes:
 - a pseudo-random number that is used as a seed to generate the second transaction cryptogram generation key; or

a transaction counter value indicating a number of transactions that has been previously conducted by a mobile application of the communication device at the time the second transaction cryptogram generation key is generated.

5. The method of claim 1, wherein the first transaction cryptogram generation key is associated with a set of one or more limited-use thresholds that includes at least one of:

a time-to-live indicating a time duration that the first transaction cryptogram generation key is valid for;

a predetermined number of transactions that the first transaction cryptogram generation key is valid for; and

a cumulative transaction amount indicating a total transaction amount that the first transaction cryptogram generation key is valid for.

6. The method of claim 5, wherein the set of one or more limited-use thresholds includes an international usage threshold and a domestic usage threshold.

7. The method of claim 1, wherein the transaction log stored on the communication device includes:

for each transaction conducted using the first transaction cryptogram generation key:

a transaction timestamp indicating the time of the corresponding transaction; and

an application transaction counter value associated with the corresponding transaction.

8. The method of claim 1, wherein the transaction log information in the replenishment request includes an authentication code computed over at least the transaction log using the first transaction cryptogram generation key.

9. The method of claim 1, wherein the replenishment request is received by the remote computer in response to:

the communication device determining that a next transaction conducted with the first transaction cryptogram generation key will exhaust one or more limited-use thresholds of the first transaction cryptogram generation key;

the communication device determining that the one or more limited-use thresholds associated with the first transaction cryptogram generation key has been exhausted; or

the communication device receiving a push message requesting the communication device to replenish the first transaction cryptogram generation key.

10. The method of claim 1, wherein the second transaction cryptogram generation key has a usage limit that is different than a usage limit of the first transaction cryptogram generation key.

11. A server computer comprising:
a processor; and
a memory coupled to the processor and storing code implementing operations including:
providing a first transaction cryptogram generation key to a communication device;
receiving transaction information for each transaction conducted by the communication device using the first transaction cryptogram generation key;
receiving a replenishment request for a second transaction cryptogram generation key, the replenishment request including transaction log information derived from transaction data stored in a transaction log on the communication device, the transaction data being unique for each transaction conducted by the communication device using the first transaction cryptogram generation key;
verifying that the transaction log information in the replenishment request is consistent with the previously received transaction information; and
providing the second transaction cryptogram generation key to the communication device in response to verifying the transaction log information in the replenishment request.

12. The server computer of claim 11, wherein providing the second transaction cryptogram generation key to the communication device includes providing, to the communication device, a key index that includes information pertaining to generation of the second transaction cryptogram generation key.

13. The server computer of claim 12, wherein the key index includes at least one of:
time information indicating when the second transaction cryptogram generation key is generated; and
a replenishment counter value indicating a number of times that the communication device has been replenished with a transaction cryptogram generation key.

14. The server computer of claim 12, wherein the key index includes:

a pseudo-random number that is used as a seed to generate the second transaction cryptogram generation key; or

a transaction counter value indicating a number of transactions that has been previously conducted by a mobile application of the communication device at the time the second transaction cryptogram generation key is generated.

15. The server computer of claim 11, wherein the first transaction cryptogram generation key is associated with a set of one or more limited-use thresholds that includes at least one of:

a time-to-live indicating a time duration that the first transaction cryptogram generation key is valid for;

a predetermined number of transactions that the first transaction cryptogram generation key is valid for; and

a cumulative transaction amount indicating a total transaction amount that the first transaction cryptogram generation key is valid for.

16. The server computer of claim 15, wherein the set of one or more limited-use thresholds includes an international usage threshold and a domestic usage threshold.

17. The server computer of claim 11, wherein the transaction log stored on the communication device includes:

for each transaction conducted using the first transaction cryptogram generation key:

a transaction timestamp indicating the time of the corresponding transaction; and

an application transaction counter value associated with the corresponding transaction.

18. The server computer of claim 11, wherein the transaction log information in the replenishment request includes an authentication code computed over at least the transaction log using the first transaction cryptogram generation key.

19. The server computer of claim 11, wherein the replenishment request is received in response to:

the communication device determining that a next transaction conducted with the first transaction cryptogram generation key will exhaust one or more limited-use thresholds of the first transaction cryptogram generation key;

the communication device determining that the one or more limited-use thresholds associated with the first transaction cryptogram generation key has been exhausted; or
the communication device receiving a push message requesting the communication device to replenish the first transaction cryptogram generation key.

20. The server computer of claim 11, wherein the second transaction cryptogram generation key has a usage limit that is different than a usage limit of the first transaction cryptogram generation key.