WHAT IS CLAIMED IS:

1. A method comprising:

providing, by a remote computer, a first limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limit the usage of the LUK to a communication device, wherein the communication device generates a transaction cryptogram using the LUK, the communication device uses the transaction cryptogram to conduct a transaction, the transaction is authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds, and the LUK is usable for more than one transaction;

receiving, by the remote computer, a replenishment request for a new LUK, the replenishment request including transaction log information derived from a transaction log on the communication device, wherein the transaction log stores transaction data for a plurality of transactions conducted using the LUK;

verifying, by the remote computer, that the transaction log information in the replenishment request matches transaction log information at the remote computer; and

providing, by the remote computer, the new LUK 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 new LUK to the communication device includes providing, to the communication device, a key index that includes information pertaining to generation of the new LUK.

3. The method of claim 2, wherein the key index includes at least one of:

time information indicating when the new LUK is generated; and

a replenishment counter value indicating a number of times that the communication device has been replenished with an LUK.

4. The method of claim 2, wherein the key index includes:

a pseudo-random number that is used as a seed to generate the new LUK; 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 new LUK is generated.

5. The method of claim 1, wherein the set of one or more limited-use thresholds includes at least one of:

a time-to-live indicating a time duration that the first LUK is valid for;

a predetermined number of transactions that the first LUK is valid for; and

a cumulative transaction amount indicating a total transaction amount that the first LUK 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 LUK:

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 LUK.

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 LUK will exhaust one or more of the set of one or more limited-use thresholds of the first LUK;

the communication device determining that the one or more of the set of one or more limited-use thresholds associated with the first LUK has been exhausted; or

the communication device receiving a push message requesting the communication device to replenish the first LUK.

10. The method of claim 1, wherein the new LUK has a usage limit that is different than a usage limit of the first LUK.

11. A server computer comprising:

a processor; and

a memory coupled to the processor and storing code implementing operations including:

providing a first limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limit the usage of the LUK to a communication device, wherein the communication device generates a transaction cryptogram using the LUK, the communication device uses the transaction cryptogram to conduct a transaction, the transaction is authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds, and the LUK is usable for more than one transaction;

receiving a replenishment request for a new LUK, the replenishment request including transaction log information derived from a transaction log on the communication device, wherein the transaction log stores transaction data for a plurality of transactions conducted using the LUK;

verifying that the transaction log information in the replenishment request matches transaction log information at the server computer; and

providing the new LUK 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 new LUK to the communication device includes providing, to the communication device, a key index that includes information pertaining to generation of the new LUK.

13. The server computer of claim 12, wherein the key index includes at least one of:

time information indicating when the new LUK is generated; and

a replenishment counter value indicating a number of times that the communication device has been replenished with an LUK.

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 new LUK; 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 new LUK is generated.

15. The server computer of claim 11, wherein the set of one or more limited-use thresholds includes at least one of:

a time-to-live indicating a time duration that the first LUK is valid for;

a predetermined number of transactions that the first LUK is valid for; and

a cumulative transaction amount indicating a total transaction amount that the first LUK 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 method of claim 1, wherein the communication device also provides a token to conduct the transaction, the token representing a real account identifier.

18. The method of claim 17, wherein the communication device does not store the LUK or the token in a secure element.

19. The method of claim 1, wherein the new LUK is associated with a second set of one or more limited-use thresholds that limit the usage of the new LUK, and wherein the communication device generates a second transaction cryptogram using the LUK, the communication device uses the second transaction cryptogram to conduct a second transaction, the second transaction is authorized based on at least whether usage of the LUK has exceeded the second set of one or more limited-use thresholds.

20. The method of claim 1, wherein second set of one or more limited-use thresholds is different than the first set of one or more limited-use thresholds.