[0007] According to an aspect, there is provided a method for enhancing the security of a communication device when conducting a transaction using the communication device that may include receiving, from a remote computer, a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limits usage of the LUK, wherein the LUK is usable for more than one transaction; generating, by the communication device, a transaction cryptogram using the LUK, sending, by the communication device to an access device, a token instead of a real account identifier and the transaction cryptogram to conduct the transaction, wherein the transaction can be authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds, sending, to the remote computer, a replenishment request for a second LUK, the replenishment request including transaction log information derived from a transaction log stored on the communication device, the transaction log storing transaction data for a plurality of transactions conducted using the first LUK, and receiving, from the remote computer, the second LUK when the transaction log information in the replenishment request matches transaction log information at the remote computer.

[0008] Disclosed herein is a communication device that may include a processor; and a memory coupled to the processor and storing a mobile application that performs operations for enhancing security of the communication device when conducting transactions using the communication device. The operations may include receiving a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limits usage of the LUK, generating a transaction cryptogram using the LUK, and sending a token instead of a real account identifier and the transaction cryptogram to conduct the transaction. The transaction may be authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds.

[0009] Disclosed herein is a method for enhancing the security of a communication device when conducting a transaction using the communication device that may include encrypting, by a computer, account information with a first encryption key to generate a second encryption key, and encrypting key index information using the second key to generate a limited-use key (LUK), where the key index information includes a key index having information pertaining to generation of the LUK. The method may also include providing the LUK and the key index to the communication device to facilitate generation of a transaction cryptogram for a transaction conducted using the communication device. The transaction can be authorized based on the LUK and the transaction cryptogram.

Claims:

1. A method for enhancing security of a communication device when conducting a transaction using the communication device, the method comprising:

receiving, from a remote computer, a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limit usage of the LUK, wherein the LUK is usable for more than one transaction;

generating, by the communication device, a transaction cryptogram using the LUK;

sending, to an access device, a token instead of a real account identifier and the transaction cryptogram to conduct the transaction, wherein the transaction is authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds,

sending, to the remote computer, a replenishment request for a second LUK, the replenishment request including transaction log information derived from a transaction log stored on the communication device, the transaction log storing transaction data for a plurality of transactions conducted using the first LUK; and

receiving, from the remote computer, the second LUK when the transaction log information in the replenishment request matches transaction log information at the remote computer.

2. The method of claim 1, wherein the communication device does not store the LUK or the token in a secure element.

3. The method of claim 1, wherein receiving the LUK further includes receiving a key index that includes information pertaining to generation of the LUK.

4. The method of claim 3, wherein the key index is sent with the transaction cryptogram to the access device to conduct the transaction.

5. The method of claim 3, wherein the key index includes time information indicating when the LUK is generated.

6. The method of claim 3, wherein the key index includes a replenishment counter value indicating a number of times the LUK has been replenished.

7. The method of claim 3, wherein the key index includes a pseudo-random number that is used as a seed to generate the LUK.

8. The method of claim 3, wherein the key index includes 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 LUK is generated.

9. 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 LUK is valid for;

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

a cumulative transaction amount indicating a total transaction amount that the LUK is valid for.

10. The method of claim 1, wherein the set of one or more limited-use thresholds includes an international usage threshold and a domestic usage threshold.

11. The method of claim 1, wherein the replenishment request further includes a first key index that includes information pertaining to generation of the LUK, and receiving the second LUK includes receiving a second key index associated with the second LUK.

12. 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;

an application transaction counter value associated with the corresponding transaction; and

a transaction type indicator indicating whether the corresponding transaction is a magnetic stripe based transaction or an integrated chip based transaction.

13. The method of claim 1, wherein the transaction log information sent to the remote computer includes an authentication code computed over at least the transaction log using the LUK.

14. The method of claim 1, wherein the replenishment request is sent in response to determining that a next transaction conducted with the LUK will exhaust the set of one or more limited-use thresholds.

15. The method of claim 1, wherein the replenishment request is sent in response to determining that the set of one or more limited-use thresholds associated with the LUK has been exhausted.

16. The method of claim 1, wherein the replenishment request is sent in response to receiving a push message requesting the communication device to replenish the LUK.

17. The method of claim 3, wherein the LUK is generated by:

encrypting account information using a first encryption key to generate a second encryption key;

encrypting the key index using the second encryption key to generate the LUK.

18. The method of claim 17, wherein encrypting the account information with the first encryption key to generate the second encryption key includes:

encrypting the account information using the first encryption key to generate a first portion of the second encryption key;

inverting the account information; and

encrypting the inverted account information using the first encryption key to generate a second portion of the second encryption key.

19. The method of claim 17, wherein encrypting the key index using the second encryption key to generate the LUK includes:

padding the key index with a first value to generate a first padded key index information;

encrypting the first padded key index information to generate a first portion of the LUK;

padding the key index with a second value to generate a second padded key index information; and

encrypting the second padded key index information to generate a second portion of the LUK.

20. The method of claim 1, wherein the transaction cryptogram is generated by:

enciphering transaction information using a first portion of the LUK;

deciphering the enciphered transaction information using a second portion of the LUK; and

re-enciphering the deciphered transaction information using the first portion of the LUK.

21. The method of claim 1, wherein the transaction cryptogram is generated by:

encrypting a predetermined numeric string using the LUK; and

decimalizing the encrypted predetermined numeric string.

22. The method of claim 21, wherein decimalizing the encrypted predetermined numeric string includes:

extracting numeric digits from the encrypted predetermined numeric string to form a first data block;

extracting hexadecimal digits from the encrypted predetermined numeric string and converting each extracted hexadecimal digit into a numeric digit to form a second data block; and

concatenating the first data block and the second data block.

23. A communication device comprising:

a processor; and

a memory coupled to the processor and storing a mobile application that performs operations for enhancing security of the communication device when conducting transactions using the communication device, the operations implementing the method of any of claims 1 to 22.