## CLAIMS

Therefore, the following is claimed:

1. A system, comprising:

a computing device comprising a processor, a memory, and a secure element, the secure element comprising an application; and

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

receive an indication for generating a sub-payment token that is subordinate to a payment token stored on the computing device;

receive a selection of a key restriction for the sub-payment token;

execute the application in the secure element to generate the sub-payment token based on the key restriction;

receive from the application the sub-payment token, the sub-payment token comprising a sub-payment key and an application transaction counter range;

establish a wireless communication session with a client device; and

send the sub-payment token through the wireless communication session to a wallet application of the client device.

2. The system of claim 1, wherein the key restriction comprises at least one of a category restriction parameter, a single transaction limit restriction parameter, or a date restriction parameter.

3. The system of claim 1 or claim 2, wherein the application transaction counter range is based at least in part on a quantity of transactions permitted for the sub-payment token.

4. The system of any of claims 1-3, wherein the wallet application is a second wallet application, and the machine-readable instructions, when executed by the processor, cause the computing device to at least:

display a user interface for a first wallet application on the computing device, the user interface being configured to receive the selection of the key restriction.

5. The system of any of claims 1-4, wherein sending the sub-payment token to the wallet application of the client device further causes the computing device to at least:

secure the sub-payment token using an encryption key stored in the secure element.

6. The system of any of claims 1-5, wherein sending the sub-payment token to the wallet application of the client device comprises using a peer-to-peer messaging protocol.

7. The system of any of claims 1-6, wherein the secure element is a processor component or a restricted application component executed in the computing device.

8. A method, comprising:

establishing, by a first client device, a wireless communication session with a second client device;

receiving, by the first client device, a sub-payment token from the second client device through the wireless communication session, the sub-payment token comprising a sub-payment key and an application transaction counter range, the sub-payment key being linked to a payment key stored on the second client device;

providing, by the first client device, the sub-payment token to a payment application executed on a secure element of the first client device; and

executing, by the first client device, a payment with a point of sale terminal by using the sub-payment token.

9. The method of claim 8, wherein the payment is at least one of a near field communication payment or a quick response code payment.

10. The method of claim 8 or claim 9, wherein the wireless communication session is a peer-to-peer wireless communication session.

11. The method of any of claims 8-10, wherein the sub-payment token is received as an encrypted payload, and further comprising:

validating, by the first client device, the encrypted payload; and

decrypting, by the first client device, the encrypted payload in order to access the sub-payment token.

12. The method of any of claims 8-11, wherein executing the payment further comprising:

providing, by the first client device, the point of sale terminal the application transaction counter range and the sub-payment key.

13. The method of any of claims 8-12, wherein the secure element is a processor component or a restricted application component executed in the first client device.

14. The method of any of claims 8-13, wherein providing the sub-payment token to the payment application executed on the secure element further comprising:

establishing, by the first client device, a secure element session by providing an authentication credential to the secure element.

15. A system comprising:

a computing device;

a secure element comprising a processor and a memory; and

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

receive a request from a wallet application executed on the computing device to generate a sub-payment key, the request comprising a key restriction;

generate the sub-payment key based at least in part on a payment key stored in the secure element and the key restriction; and

return the sub-payment key to the wallet application.

16. The system of claim 15, wherein the secure element comprises an application transaction counter for the payment key and a sub-application transaction counter for the sub-payment key.

17. The system of claim 15 or claim 16, wherein the sub-payment key comprises the key restriction that includes at least one of a category restriction parameter, a single transaction limit restriction parameter, or a date restriction parameter.

18. The system of any of claims 15-17, wherein the key restriction is a quantity of transactions permitted by an account holder.

19. The system of claim 18, wherein generating the sub-payment key further causes the secure element to at least:

generate an application transaction counter (ATC) range based at least in part on the quantity of transactions permitted by the account holder.

20. The system of claim 19, wherein the sub-payment key comprises a starting value for the ATC range and an ending value for the ATC range.