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 a restricted 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, the payment token having a first application transaction counter range;

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

execute the restricted application in the secure element to generate the sub-payment token based at least in part on the key restriction, the sub-payment token comprising a sub-payment key and a second application transaction counter range, wherein the second application transaction counter range is restricted by the first application transaction counter range;

receive from the restricted application the sub-payment token;

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 any of claims 1-2, 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.

4. The system of any of claims 1-3, 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.

5. The system of any of claims 1-4, wherein sending the sub-payment token to the wallet application of the client device comprises using a peer-to-peer messaging protocol.

6. The system of any of claims 1-5, wherein the secure element is a processor component.

7. A method, comprising:

receiving, via a first mobile device that comprises a secure hardware element, an indication for generating a sub-payment token that is subordinate to a payment token stored on the first mobile device, the payment token having a first application transaction counter range;

receiving, via the first mobile device, a selection of a key restriction for the sub-payment token;

executing, via the first mobile device, a restricted application in the secure hardware element to generate the sub-payment token based on the key restriction, the sub-payment token comprising a sub-payment key and a second application transaction counter range, wherein the second application transaction counter range is restricted by the first application transaction counter range;

receiving, via the first mobile device, from the restricted application the sub-payment token;

establishing, via the first mobile device, a wireless communication session with a second mobile device; and

sending, via the first mobile device, the sub-payment token through the wireless communication session to a wallet application of the second mobile device.

8. The method of claim 7, wherein the key restriction comprises at least one of a category restriction parameter, a single transaction limit restriction parameter, or a date restriction parameter.

9. The method of claim 7, wherein the second application transaction counter range is based at least in part on a quantity of transactions permitted for the sub-payment token.

10. The method of claim 7, wherein the wallet application is a second wallet application, and the method further comprising:

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

11. The method of claim 7, wherein sending the sub-payment token to the wallet application of the second mobile device further comprising: securing, via the first mobile device, the sub-payment token using an encryption key stored in the secure hardware element.

12. The method of claim 7, wherein sending the sub-payment token to the wallet application of the second mobile device comprises using a peer-to-peer messaging protocol.

13. The method of claim 7, wherein the secure hardware element is tamper-resistant and the secure hardware element comprises a processor and a memory, wherein the memory stores the restricted application.

14. A non-transitory computer-readable medium embodying machine-executable instructions stored thereon that, when executed by a processor of a computing device, 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, wherein the computing device comprises a secure hardware element, the payment token having a first application transaction counter range;

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

execute a restricted application in the secure hardware element to generate the sub-payment token based on the key restriction, the sub-payment token comprising a sub-payment key and a second application transaction counter range, wherein the second application transaction counter range is restricted by the first application transaction counter range;

receive from the restricted application the sub-payment token;

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.

15. The non-transitory computer-readable medium of claim 14, wherein the key restriction comprises at least one of a category restriction parameter, a single transaction limit restriction parameter, or a date restriction parameter.

16. The non-transitory computer-readable medium of claim 14, wherein the second application transaction counter range is based at least in part on a quantity of transactions permitted for the sub-payment token.

17. The non-transitory computer-readable medium of claim 14, wherein the machine-executable 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.

18. The non-transitory computer-readable medium of claim 14, 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 hardware element.

19. The non-transitory computer-readable medium of claim 14, wherein the secure hardware element comprises a processor and a memory, wherein the restricted application is stored in the memory.

20. The system of claim 1, wherein the sub-payment key is an account specific secret key.