WHAT IS CLAIMED IS:

1. A method for processing a message related to a mobile payment application on a secure element of a mobile communication device through an interconnectivity services hub, the method comprising:

receiving the message from a first entity in a first protocol;

determining, by a server computer, a trusted service manager associated with the secure element from among a plurality of trusted service managers using a routing table comprising routing information corresponding to predetermined secure element management relationships;

determining a second protocol corresponding to the trusted service manager associated with the secure element;

translating the message into the second protocol; and

sending the translated message to the trusted service manager, wherein the trusted service manager communicates with the secure element.

2. The method of claim 1, wherein the first protocol is also the second protocol.

3. The method of claim 1, wherein the message provides value added services for the mobile payment application on the secure element of the mobile communication device.

4. The method of claim 1, wherein the first entity is an issuer.

5. The method of claim 1, wherein the message includes a request, and wherein the request includes adding, deleting, activating, unlocking, locking, reissuing, replacing, or updating the mobile payment application on the secure element.

6. The method of claim 1, wherein the first entity is an issuer, a trusted service manager associated with the issuer, a wallet provider, or a mobile network operator.

7. The method of claim 1, wherein translating the message into the second protocol further comprises:

identifying the first entity;

determining a request by comparing the message to a first entity protocol mapping; and

mapping information in the message according to a secure element trusted service manager protocol mapping for the request.

8. The method of claim 1, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message; and

generating information to be included in the translated message based on a secure element trusted service manager protocol mapping for the request.

9. The method of claim 1, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message;

generating a plurality of translated messages based on a range of available trusted service manager requirements; and

selecting the correct translated message from the plurality of translated messages for the trusted service manager associated with the secure element.

10. The method of claim 1, further comprising:

receiving application personalization information from an application personalization preparation service using a master key;

sending the application personalization information to the trusted service manager in the translated message, wherein the trusted service manager uses the application personalization information to provision a new payment application on the secure element; and

sending the application personalization information to the first entity, wherein the first entity uses the application personalization information to update consumer records..

11. A server computer comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code executable by the processor for implementing a method for processing a message related to a mobile payment

application on a secure element of a mobile communication device through an interconnectivity services hub, the method comprising:

receiving the message from a first entity in a first protocol;

determining a trusted service manager associated with the secure element from among a plurality of trusted service managers using a routing table comprising routing information corresponding to predetermined secure element management relationships;

determining a second protocol for the trusted service manager associated with the secure element;

translating the message into the second protocol; and

sending the translated message to the trusted service manager, wherein the trusted service manager communicates with the secure element.

12. The server computer of claim 11, wherein the first protocol is also the second protocol.

13. The server computer of claim 11, wherein the electronic communication allows the first entity to provide value added services for a stored payment account on a mobile communication device.

14. The server computer of claim 11, wherein the first entity is an issuer.

15. The server computer of claim 11, wherein the electronic communication includes a request, wherein the request includes adding, deleting, activating, unlocking, locking, reissuing, replacing, or updating the mobile payment application on the secure element.

16. The server computer of claim 11, wherein the first entity is an issuer, a trusted service manager associated with an issuer, a wallet provider, or a mobile network operator.

17. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

identifying the first entity;

determining a request by comparing the message to a first entity protocol mapping; and

mapping information in the message according to a second entity protocol mapping for the request.

18. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message; and

generating information to be included in the translated message based on a second entity protocol mapping for the request.

19. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message;

generating a plurality of translated messages based on a range of available trusted service manager requirements; and

selecting the correct translated message from the plurality of translated messages for the trusted service manager.

20. The server computer of claim 11, wherein the method further comprises:

receiving application personalization information from an application personalization preparation service using a master key;

sending the application personalization information to the trusted service manager in the translated message, wherein the trusted service manager uses the application personalization information to provision a new payment application on the secure element; and

sending the application personalization information to the first entity, wherein the first entity uses the application personalization information to update consumer records.

CLAIMS

1. A method for processing a message related to a mobile payment application on a secure element of a mobile communication device through an interconnectivity services hub, the method comprising:

receiving, by one or more server computers of the interconnectivity services hub, the message from a first entity in a first protocol;

determining, by the one or more server computers of the interconnectivity services hub, a trusted service manager associated with the secure element from among a plurality of trusted service managers using a routing table comprising routing information corresponding to predetermined secure element management relationships between the secure element of the mobile communication device and the plurality of trusted service managers, the trusted service manager being configured to communicate with the secure element using a secure element key associated with the secure element, wherein the secure element key is stored at the trusted service manager;

determining, by the one or more server computers of the interconnectivity services hub, a second protocol corresponding to the trusted service manager associated with the secure element;

translating, by the one or more server computers of the interconnectivity services hub, the message into the second protocol; and

sending, by the one or more server computers of the interconnectivity services hub, the translated message to the trusted service manager, wherein the trusted service manager communicates with the secure element to perform an action associated with the translated message on the secure element of the mobile communication device.

2. The method of claim 1, wherein the first protocol is also the second protocol.

3. The method of claim 1, wherein the message provides value added services for the mobile payment application on the secure element of the mobile communication device.

4. The method of claim 1, wherein the first entity is an account issuer associated with a user of the mobile communication device.

5. The method of claim 1, wherein the message includes a request, and wherein the request includes adding, deleting, activating, unlocking, locking, reissuing, replacing, or updating the mobile payment application on the secure element.

6. The method of claim 1, wherein the first entity is an issuer, a trusted service manager associated with the issuer, a wallet provider, or a mobile network operator.

7. The method of claim 1, wherein translating the message into the second protocol further comprises:

identifying the first entity;

determining a request by comparing the message to a first entity protocol mapping; and

mapping information in the message according to a secure element trusted service manager protocol mapping for the request.

8. The method of claim 1, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message; and

generating information to be included in the translated message based on a secure element trusted service manager protocol mapping for the request.

9. The method of claim 1, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message;

generating a plurality of translated messages based on a range of available trusted service manager requirements; and

selecting the correct translated message from the plurality of translated messages for the trusted service manager associated with the secure element.

10. The method of claim 1, further comprising:

receiving application personalization information from an application personalization preparation service computer storing a master key, the application

personalization preparation service computer using the master key to generate the application personalization information;

sending the application personalization information to the trusted service manager in the translated message, wherein the trusted service manager uses the application personalization information to provision a new payment application on the secure element; and

sending the application personalization information to the first entity, wherein the first entity uses the application personalization information to update consumer records.

11. A server computer comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code executable by the processor for implementing a method for processing a message related to a mobile payment application on a secure element of a mobile communication device through an interconnectivity services hub, the method comprising:

receiving the message from a first entity in a first protocol;

determining a trusted service manager associated with the secure element from among a plurality of trusted service managers using a routing table comprising routing information corresponding to predetermined secure element management relationships between the first entity and the plurality of trusted service managers, the trusted service manager being configured to access the secure element using a secure element key associated with the secure element, wherein the secure element key is stored at the trusted service manager;

determining a second protocol for the trusted service manager associated with the secure element;

translating the message into the second protocol; and

sending the translated message to the trusted service manager, wherein the trusted service manager communicates with the secure element to perform an action associated with the translated message on the secure element of the mobile communication device.

12. The server computer of claim 11, wherein the first protocol is also the second protocol.

13. The server computer of claim 11, wherein the electronic communication allows the first entity to provide value added services for a stored payment account on a mobile communication device.

14. The server computer of claim 11, wherein the first entity is an account issuer associated with a user of the mobile communication device.

15. The server computer of claim 11, wherein the electronic communication includes a request, wherein the request includes adding, deleting, activating, unlocking, locking, reissuing, replacing, or updating the mobile payment application on the secure element.

16. The server computer of claim 11, wherein the first entity is an issuer, a trusted service manager associated with an issuer, a wallet provider, or a mobile network operator.

17. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

identifying the first entity;

determining a request by comparing the message to a first entity protocol mapping; and

mapping information in the message according to a second entity protocol mapping for the request.

18. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message; and

generating information to be included in the translated message based on a second entity protocol mapping for the request.

19. The server computer of claim 11, wherein translating the electronic communication into the second protocol further comprises:

determining a request based on uniform commands in the message;

generating a plurality of translated messages based on a range of available trusted service manager requirements; and

selecting the correct translated message from the plurality of translated messages for the trusted service manager.

20. The server computer of claim 11, wherein the method further comprises:

receiving application personalization information from an application personalization preparation service computer storing a master key, the application personalization preparation service computer using the master key to generate the application personalization information;

sending the application personalization information to the trusted service manager in the translated message, wherein the trusted service manager uses the application personalization information to provision a new payment application on the secure element; and

sending the application personalization information to the first entity, wherein the first entity uses the application personalization information to update consumer records.