WHAT IS CLAIMED IS:

1. A method comprising:

establishing, by a communication device, a communication channel with an access device;

receiving, by the communication device, an access device profile of the access device;

emulating, by the communication device, a virtual access device on the communication device based on the access device profile;

issuing, by the virtual access device executing on the communication device, a set of application commands to a transaction applet executing on the communication device;

receiving, by the virtual access device executing on the communication device, a set of application data responses from the transaction applet in response to the set of application commands;

generating, by the communication device, a data packet by concatenating application data contained in the set of application data responses; and

transmitting, by the communication device, the data packet to the access device via the communication channel.

2. The method of claim 1, further comprising:

receiving, by the communication device, an access device digital certificate from the access device; and

verifying, by the communication device, the access device digital certificate prior to emulating the virtual access device.

3. The method of claim 2, wherein the access device digital certificate includes an access device public key, and the data packet is encrypted by the communication device using the access device public key prior to transmitting the data packet to the access device.

4. The method of claim 1, further comprising:

transmitting, by the communication device, a communication device digital certificate to the access device prior to receiving the access device profile,

wherein the communication device digital certificate is verified by the access device prior to transmission of the access device profile to the communication device.

5. The method of claim 1, wherein the access device profile includes a prioritized list of application identifiers supported by the access device.

6. The method of claim 5, wherein the set of application commands includes a select application identifier command that is generated by the virtual access device based on the prioritized list of application identifiers to select an application identifier from a list of available application identifiers associated with the transaction applet.

7. The method of claim 1, wherein the access device profile includes an unpredictable number generated by the access device.

8. The method of claim 7, wherein the set of application data responses includes a transaction cryptogram generated by the transaction applet using the unpredictable number provided to the transaction applet by the virtual access device.

9. The method of claim 1, wherein the application data being concatenated to generate the data packet includes application data in a plurality of read record responses from the transaction applet.

10. The method of claim 1, wherein the communication channel established between the communication device and the access device is a wireless communication channel having a longer communication range than near field communication (NFC).

11. A communication device comprising:

a processor; and

a memory storing code executable by the communication device to implement operations including:

establishing a communication channel with an access device;

receiving an access device profile of the access device;

emulating a virtual access device on the communication device based on the access device profile;

issuing, by the virtual access device executing on the communication device, a set of application commands to a transaction applet executing on the communication device;

receiving, by the virtual access device executing on the communication device, a set of application data responses from the transaction applet in response to the set of application commands;

generating a data packet by concatenating application data contained in the set of application data responses; and

transmitting the data packet to the access device via the communication channel.

12. The communication device of claim 11, wherein the operations further include:

receiving an access device digital certificate from the access device; and

verifying the access device digital certificate prior to emulating the virtual access device.

13. The communication device of claim 12, wherein the access device digital certificate includes an access device public key, and the data packet is encrypted by the communication device using the access device public key prior to transmitting the data packet to the access device.

14. The communication device of claim 11, wherein the operations further include:

Transmitting a communication device digital certificate to the access device prior to receiving the access device profile, wherein the communication device digital certificate is verified by the access device prior to transmission of the access device profile to the communication device.

15. The communication device of claim 11, wherein the access device profile includes a prioritized list of application identifiers supported by the access device.

16. The communication device of claim 15, wherein the set of application commands includes a select application identifier command that is generated by the virtual access device based on the prioritized list of application identifiers to select an application identifier from a list of available application identifiers associated with the transaction applet.

17. The communication device of claim 11, wherein the access device profile includes an unpredictable number generated by the access device.

18. The communication device of claim 17, wherein the set of application data responses includes a transaction cryptogram generated by the transaction applet using the unpredictable number provided to the transaction applet by the virtual access device.

19. The communication device of claim 11, wherein the application data being concatenated to generate the data packet includes application data in a plurality of read record responses from the transaction applet.

20. The communication device of claim 11, wherein the communication channel established between the communication device and the access device is a wireless communication channel having a longer communication range than near field communication (NFC).

WHAT IS CLAIMED IS:

1. A method for secured extended range application data exchange, the method comprising:

establishing, by an access device with a communication device, a communication channel;

providing, by the access device to the communication device, an access device profile of the access device, wherein the communication device emulates a virtual access device based on the access device profile, and wherein the virtual access device issues a set of application commands to a transaction applet executing on the communication device, and receives a set of application data responses from the transaction applet in response to the set of application commands, and wherein the communication device generates a data packet based on the set of application data responses;

receiving, by the access device from the communication device, the data packet via the communication channel;

generating, by the access device, an authorization request message comprising data in the data packet; and

sending the authorization request message to an authorizing entity which authorizes the authorization request message.

2. The method of claim 1, further comprising:

providing, by the access device to the communication device, an access device digital certificate, wherein the communication device verifies the access device digital certificate prior to emulating the virtual access device.

3. The method of claim 2, wherein the access device digital certificate includes an access device public key, and the data packet is encrypted by the communication device using the access device public key the data packet is received by the access device.

4. The method of claim 1, wherein the communication device is a mobile phone.

5. The method of claim 1, wherein the access device profile includes a prioritized list of application identifiers supported by the access device.

6. The method of claim 5, wherein the set of application commands includes a select application identifier command that is generated by the virtual access device based on the prioritized list of application identifiers to select an application identifier from a list of available application identifiers associated with the transaction applet.

7. The method of claim 1, wherein the access device profile includes an unpredictable number generated by the access device.

8. The method of claim 7, wherein the set of application data responses includes a transaction cryptogram generated by the transaction applet using the unpredictable number provided to the transaction applet by the virtual access device.

9. The method of claim 1, wherein the data packet includes application data in a plurality of read record responses from the transaction applet.

10. The method of claim 1, wherein the communication channel is a wireless communication channel having a longer communication range than near field communication (NFC).

11. An access device comprising :

a processor; and

a memory storing code executable by the processor to implement operations including:

establishing, with a communication device, a communication channel;

providing, to the communication device, an access device profile of the access device, wherein the communication device emulates a virtual access device based on the access device profile, and wherein the virtual access device issues a set of application commands to a transaction applet executing on the communication device, and receives a set of application data responses from the transaction applet in response to the set of application commands, and wherein the communication device generates a data packet based on the set of application data responses;

receiving, from the communication device, the data packet via the communication channel;

generating an authorization request message comprising data in the data packet; and

sending the authorization request message to an authorizing entity which authorizes the authorization request message.

12. The access device of claim 11, wherein the operations further include:

providing an access device digital certificate to the communication device, wherein the communication device verifies the access device digital certificate prior to emulating the virtual access device.

13. The access device of claim 12, wherein the access device digital certificate includes an access device public key, and the data packet is encrypted by the communication device using the access device public key.

14. The access device of claim 11, wherein the communication device is a mobile phone.

15. The access device of claim 11, wherein the access device profile includes a prioritized list of application identifiers supported by the access device.

16. The access device of claim 15, wherein the set of application commands includes a select application identifier command that is generated by the virtual access device based on the prioritized list of application identifiers to select an application identifier from a list of available application identifiers associated with the transaction applet.

17. The access device of claim 11, wherein the access device profile includes an unpredictable number generated by the access device.

18. The access device of claim 17, wherein the set of application data responses includes a transaction cryptogram generated by the transaction applet using the unpredictable number provided to the transaction applet by the virtual access device.

19. The access device of claim 11, wherein the data packet includes application data in a plurality of read record responses from the transaction applet.

20. The access device of claim 11, wherein the communication channel established is a wireless communication channel having a longer communication range than near field communication (NFC).