WHAT IS CLAIMED IS:

1. A method of securely provisioning access data to a service provider application on a mobile phone comprising:

generating, by ~~a~~ the mobile phone~~communication device~~, an initialization request message to provision access data;

transmitting, by the mobile phone~~communication device~~, the initialization request message to a server computer;

receiving, by the service provider application on the mobile phone~~communication device~~, a dynamic data element from the server computer;

performing, by the mobile phone~~communication device~~, a message exchange process with a card~~user device~~, wherein an operating system of the mobile phone implements a set of access device emulation APIs which allow the service provider application to emulate functions of an access device and to gain access to a contactless element interface of the mobile phone and exchange transaction data communications with a contactless element of the card, wherein a cryptogram is generated by encrypting, using a key on the card, at least the dynamic data element and a card identifier, and the cryptogram is received from the card ~~user device~~ by the ~~communication device~~ mobile phone during the message exchange process;

transmitting, by the mobile phone~~communication device~~, a provisioning request message including ~~a~~ the card ~~user device~~ identifier and the cryptogram to the server computer; and

receiving, by the service provider application of the mobile phone~~communication device~~, the access data.

~~2. The method of claim 1, wherein the communication device is a mobile phone and the user device is a card.~~

~~3. The method of claim 1, wherein the cryptogram is generated by encrypting, using a key on the user device, at least the dynamic data element and the user device identifier.~~

24. The method of claim 1, wherein the server computer is in communication with an access data vault, and wherein the server computer retrieves the access data from the access data vault.

35. The method of claim 1, wherein the message exchange process utilizes get processing option and application identifier request and response messages.

46. The method of claim 1, wherein the mobile phone ~~communication device~~ and the card ~~user device~~ perform the message exchange process while in short-range wireless communication with each other.

57. The method of claim 1, wherein the access data provisioned to the mobile phone ~~communication device~~ is used to conduct a transaction by interfacing with an access device.

68. The method of claim 1, wherein the cryptogram is generated with ~~a~~ the key, and the key is derived from data existing on the card~~user device~~.

79. The method of claim 1, wherein a numerical value of zero is transmitted from the mobile phone ~~communication device~~ to the card ~~user device~~ in the message exchange process.

810. A mobile phone ~~communication device~~ comprising:

a processor; and

a computer readable medium, coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method comprising:

generating an initialization request message to provision access data;

transmitting the initialization request message to a server computer;

receiving, by a service provider application on the mobile phone, a dynamic data element from the server computer;

performing a message exchange process with a card~~user device~~, wherein an operating system of the mobile phone implements a set of access device emulation APIs which allow the service provider application to emulate functions of an access device and to gain access to a contactless element interface of the mobile phone and exchange transaction data communications with a contactless element of the card, wherein a cryptogram is generated by encrypting, using a key on the card, at least the dynamic data element and a card identifier, and the cryptogram is received from the card ~~user device~~ by the mobile phone ~~communication device~~ during the message exchange process;

transmitting a provisioning request message including ~~a~~ the card ~~user device~~ identifier and the cryptogram to the server computer; and

receiving, by the service provider application of the mobile phone~~communication device~~, the access data.

~~9~~11. The mobile phone ~~communication device~~ of claim ~~8~~10, wherein the cryptogram is generated by encrypting, using ~~a~~ the key on the card~~user device~~, the dynamic data element and the ~~user device~~ card identifier.

10~~12~~. The mobile phone ~~communication device~~ of claim 8~~10~~, wherein the server computer is in communication with an access data vault, and wherein the server computer retrieves the access data from the access data vault.

11~~13~~. The mobile phone ~~communication device~~ of claim 8~~10~~, wherein the message exchange process utilizes get processing option and application identifier request and response messages.

12~~14~~. The mobile phone ~~communication device~~ of claim 8~~10~~, wherein the mobile phone ~~communication device~~ and the card ~~user device~~ perform the message exchange process while in short-range wireless communication with each other.

~~15. The communication device of claim 10, wherein the communication device is a mobile phone.~~

13~~16~~. The mobile phone ~~communication device~~ of claim 8~~10~~, wherein the access data provisioned to the mobile phone ~~communication device~~ is used to conduct a transaction by interfacing with an access device.

14~~17~~. The mobile phone ~~communication device~~ of claim 8~~10~~, wherein the cryptogram is generated using ~~a~~ the key that is derived from data on the card~~user device~~.

15~~18~~. A method comprising:

receiving, by a server computer from a mobile phone comprising a service provider application~~communication device~~, an initialization request message to provision access data;

providing, by the server computer to the mobile phone~~communication device~~, a dynamic data element, the mobile phone ~~communication device~~ thereafter performing a message exchange process with a card~~user device~~, wherein an operating system of the mobile phone implements a set of access device emulation APIs which allow the service provider application to emulate functions of an access

device and to gain access to a contactless element interface of the mobile phone and exchange transaction data communications with a contactless element of the card, wherein a cryptogram is generated by encrypting, using a key on the card, at least the dynamic data element and a card identifier, and the cryptogram is received from the card ~~user device~~ by the mobile phone ~~communication device~~ during the message exchange process;

receiving, by the server computer, a provisioning request message including ~~a~~ the card ~~user device~~ identifier and the cryptogram; and

providing, by the server computer, the access data to the service provider application on the mobile phone.

~~19. The method of claim 18, wherein the communication device is a mobile phone and the user device is a card:~~

16~~20~~. The method of claim 15~~18~~, wherein the cryptogram is formed using a DES or triple DES encryption process.

17~~21~~. A server computer comprising:

a processor; and

a computer readable medium, the computer readable medium comprising code, executable by the processor, to perform a method according to any of claims 15-16~~18-20~~.