WHAT IS CLAIMED IS:

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

generating, by the mobile phone, an initialization request message to provision access data;

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

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

performing, by the mobile phone, a message exchange process with a card, 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 the contactless element of a card, wherein a cryptogram is generated at the card by:

encrypting static elements including an account identifier with a first encryption key to generate a second encryption key, and

encrypting the dynamic data element using the second encryption key to create a cryptogram,

wherein the cryptogram is received from the card by the mobile phone during the message exchange process;

transmitting, by the mobile phone, a provisioning request message including a card identifier and the received cryptogram to the server computer; and

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

2. 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.

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

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

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

6. The method of claim 1, wherein the second encryption key is derived from data existing on the card.

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

8. A method according to any preceding claim wherein the cryptogram is formed using a DES or triple DES encryption process.

9. A system comprising a mobile phone and a card, the system being configured to perform any of the methods of claims 3-8.