WHAT IS CLAIMED IS:

1. A method for provisioning access data to a communication device, the method comprising:

receiving, by a server computer from the communication device, an initialization request message;

in response to the initialization request message, providing, by the server computer to the communication device, a dynamic data element, wherein the communication device provides the dynamic data element to a user device and the user device generates a cryptogram using the dynamic data element and a user device identifier, and provides the cryptogram and the user device identifier to the communication device;

receiving, by the server computer from the communication device, a provisioning request message including the user device identifier and the cryptogram in a first message format;

generating, by the server computer, an authorization request message in a second message format, the authorization request message comprising the cryptogram;

transmitting, by the server computer, the authorization request message to an authorizing computer;

receiving, by the server computer, an authorization response message from the authorizing computer;

in response to receiving the authorization response message, providing, by the server computer, the access data to the communication device; and

storing, by the 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 formed using a DES or triple DES encryption process.

4. The method of claim 1, further comprising:

verifying that the authorization response message comprises a positive authorization indicator, prior to providing the access data to the communication device.

5. The method of claim 1, wherein the first message format is an HTTP/S message format, and the second message format is an ISO 8583 message format.

6. The method of claim 1, wherein the authorization request message further comprises a nominal value.

7. The method of claim 1, wherein the cryptogram is formed using a first cryptographic key that is on the user device, and is validated using a second cryptographic key that is on the authorizing computer.

8. The method of claim 1, wherein the cryptogram is formed using a first cryptographic key that is on the user device, and is validated using a second cryptographic key that is on the authorizing computer, and wherein the first cryptographic key is derived on the user device.

9. The method of claim 1, wherein the access data comprises data that can allow a user of the communication device to access a secure location.

10. A server computer comprising:

a processor; and

a computer readable medium, the computer readable medium comprising code, executable by the processor to implement a method comprising:

receiving, by the server computer from a communication device, an initialization request message;

in response to the initialization request message, providing, by the server computer to the communication device, a dynamic data element, wherein the communication device provides the dynamic data element to a user device and the user device generates a cryptogram using the dynamic

data element and a user device identifier, and provides the cryptogram and the user device identifier to the communication device;

receiving, from the communication device, a provisioning request message including the user device identifier and the cryptogram in a first message format;

generating an authorization request message in a second message format, the authorization request message comprising the cryptogram;

transmitting the authorization request message to an authorizing computer;

receiving an authorization response message from the authorizing computer;

in response to receiving the authorization response message, providing access data to the communication device; and

storing, by the communication device, the access data.

11. The server computer of claim 10, wherein the authorization request message comprises a zero value amount, the cryptogram, and the user device identifier.

12. The server computer of claim 10, wherein the authorization response message comprises the user device identifier and an authorization indicator.

13. The server computer of claim 10, wherein the access data comprises a token.

14. The server computer of claim 10, wherein the method further comprises:

providing, by the server computer to the communication device, the dynamic data element comprising a random number, wherein the cryptogram is formed using the dynamic data element and the user device identifier.

15. A method comprising:

transmitting, by a communication device to a server computer, an initialization request message to provision access data to the communication device;

receiving, by the communication device from the server computer and in response to the initialization request message, a dynamic data element;

providing, by the communication device to a user device, the dynamic data element;

performing, by the communication device, a message exchange process with the user device, wherein the user device generates a cryptogram using the dynamic data element and a user identifier, and the cryptogram is received from the user device by the communication device during the message exchange process;

transmitting, by the communication device, a provisioning request message including a user device identifier and the cryptogram to the server computer, which generates an authorization request message comprising the cryptogram, transmits the authorization request message to an authorizing computer, which verifies the cryptogram;

receiving, by the communication device, the access data in response to transmitting the provisioning request message; and

storing, by the communication device, the access data.

16. The method of claim 15, wherein the communication device is a mobile phone and the user device is a card.

17. The method of claim 15, wherein the cryptogram is generated by encrypting, using a key on the user device, and at least the dynamic data element and the user device identifier.

18. The method of claim 15, 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, and transmits the access data to the communication device, after receiving an authorization response message from the authorizing computer, which is responsive to the authorization request message.

19. The method of claim 15, wherein the provisioning request message is in an XML data format.