

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a server computer from a communication device, a
3 provisioning request message including a user device identifier and a cryptogram in
4 a first message format, which is received from a user device by the communication
5 device during a message exchange process between the user device and the
6 communication device;
7 generating, by the server computer, an authorization request message
8 in a second message format, the authorization request message comprising the
9 cryptogram;
10 transmitting, by the server computer, the authorization request
11 message to an authorizing computer;
12 receiving, by the server computer, an authorization response message
13 from the authorizing computer; and
14 in response to receiving the authorization response message,
15 providing, by the server computer, access data to the communication device.
- 1 2. The method of claim 1, wherein the communication device is a
2 mobile phone and the user device is a card.
- 1 3. The method of claim 1, wherein the cryptogram is formed using
2 a DES or triple DES encryption process.
- 1 4. The method of claim 1, further comprising:
2 receiving, by the server computer from the communication device, an
3 initialization request message to provision access data; and
4 providing, by the server computer to the communication device, a
5 dynamic data element, wherein the cryptogram is formed using the dynamic data
6 element and the user device identifier.
- 1 5. The method of claim 1, further comprising:

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

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

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

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

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

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

1 11. A server computer comprising:
2 a processor; and
3 a computer readable medium, the computer readable medium
4 comprising code, executable by the processor to implement a method comprising:
5 receiving, from a communication device, a provisioning request
6 message including a user device identifier and a cryptogram in a first message
7 format, which is received from a user device by the communication device during a
8 message exchange process between the user device and the communication
9 device;
10 generating an authorization request message in a second message
11 format, the authorization request message comprising the cryptogram;

12 transmitting the authorization request message to an authorizing
13 computer;
14 receiving an authorization response message from the authorizing
15 computer; and
16 in response to receiving the authorization response message, providing
17 access data to the communication device.

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

1 13. The server computer of claim 11, wherein the authorization
2 response message comprises the user device identifier and an authorization
3 indicator.

1 14. The server computer of claim 11, wherein the access data
2 comprises a token.

1 15. The server computer of claim 11, wherein the method further
2 comprises:
3 providing, by the server computer to the communication device, a
4 dynamic data element comprising a random number, wherein the cryptogram is
5 formed using the dynamic data element and the user device identifier.

1 16. A method comprising:
2 performing, by a communication device, a message exchange process
3 with a user device, wherein a cryptogram is received from the user device by the
4 communication device during the message exchange process;
5 transmitting, by the communication device, a provisioning request
6 message including a user device identifier and the cryptogram to a server computer,
7 which generates an authorization request message comprising the cryptogram,
8 transmits the authorization request message to an authorizing computer, which
9 verifies the cryptogram; and

10 receiving, by the communication device, access data in response to
11 transmitting the provisioning request message.

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

1 18. The method of claim 16, wherein the cryptogram is generated by
2 encrypting, using a key on the user device, and at least a dynamic data element and
3 the user device identifier.

1 19. The method of claim 16, wherein the server computer is in
2 communication with an access data vault, and wherein the server computer retrieves
3 the access data from the access data vault, and transmits the access data to the
4 communication device, after receiving an authorization response message from the
5 authorizing computer, which is responsive to the authorization request message.

1 20. The method of claim 16, wherein the provisioning request
2 message is in an XML data format.

1