

WHAT IS CLAIMED IS:

1. A method comprising:

initiating an authorization process by, receiving, by a resource provider system, a portable device identifier and a cryptogram from a portable device;

verifying, by the resource provider system, the cryptogram, wherein verifying the cryptogram comprises:

generating a second cryptogram based at least in part on the portable device identifier and an intermediate access identifier, the intermediate access identifier comprising a virtual primary account number not operable for being used to directly conduct a transaction; and
comparing the second cryptogram with the cryptogram to determine if they match;

obtaining, by the resource provider system, an authentication response indicator after verification of the cryptogram;

generating, by the resource provider system and based at least in part on the authentication response indicator, an authorization request message comprising an access identifier, the access identifier comprising a primary account number;

transmitting, by the resource provider system, the authorization request message to a processing computer; and

receiving, by the resource provider system from the processing computer, an authorization response message comprising an authorization response indicator, wherein the authorization process is performed in real-time and is completed by receipt of the authorization response message.

2. The method of claim 1, wherein the portable device identifier and the access identifier have different data formats.

~~3. The method of claim 1, wherein verifying the cryptogram comprises:~~

~~generating, by the resource provider system, an authentication request message comprising the portable device identifier and the cryptogram;~~

~~transmitting, by the resource provider system, the authentication request message to the processing computer; and~~

~~receiving, by the resource provider system from the processing computer, an authentication response message comprising the authentication response indicator.~~

34. The method of claim 13, wherein the ~~authentication request message further comprises an intermediate access identifier that is~~ has a different data format from the portable device identifier.

~~45.~~ The method of claim ~~34~~, wherein ~~the intermediate access identifier comprises a virtual primary account number and the access identifier comprises a primary account number, both the intermediate access identifier and the access identifier~~ have being of a same data format.

~~6.~~ ~~The method of claim 5, wherein the virtual primary account number is not operable for being used to directly conduct a transaction.~~

~~57.~~ The method of claim 1, wherein the portable device is a key fob or a mobile phone, and the resource provider system comprises an access device, the access device being an automated fuel dispenser.

~~68.~~ A resource provider system comprising:
a processor; and
a non-transitory computer readable medium coupled to the processor,
the non-transitory computer readable medium comprising code, executable by the processor, for implementing a method comprising:

initiating an authorization process by, receiving a portable device identifier and a cryptogram from a portable device;

verifying the cryptogram, wherein verifying the cryptogram comprises:

generating a second cryptogram based at least in part on the portable device identifier and an intermediate access identifier, the intermediate access identifier comprising a virtual primary account number not operable for being used to directly conduct a transaction; and
comparing the second cryptogram with the cryptogram to determine if they match;

obtaining an authentication response indicator after verification of the cryptogram;

generating, based at least in part on the authentication response indicator, an authorization request message comprising an access identifier, the access identifier comprising a primary account number;

transmitting the authorization request message to a processing computer; and

receiving, from the processing computer, an authorization response message comprising an authorization response indicator, wherein the authorization process is performed in real-time and is completed by receipt of the authorization response message.

~~9. — The resource provider system of claim 8, wherein verifying the cryptogram comprises:~~

~~generating a second cryptogram based at least in part on the portable device identifier; and~~

~~comparing the second cryptogram with the cryptogram to determine if they match; and~~

~~upon determining that the second cryptogram and the cryptogram match, generating the authentication response indicator.~~

710. The resource provider system of claim 69, wherein generating the second cryptogram comprises:

determining a first cryptographic key;

generating, based at least in part on a key derivation parameter and the first cryptographic key, a unique derivation key; and

generating, based at least in part on the portable device identifier and the unique derivation key, the second cryptogram.

811. The resource provider system of claim 710, wherein the key derivation parameter comprises ~~an~~ the intermediate access identifier.

912. The resource provider system of claim 68, wherein the cryptogram corresponds to a digital signature, and wherein verifying the cryptogram comprises:

receiving a public verification key;

determining a hash of the portable device identifier using the public verification key; and

determining if the hash matches the digital signature.

1013. The resource provider system of claim 68, wherein the resource provider system further comprises an access device, and wherein at least one of the access device or the processing computer comprises a hardware security module (HSM), the hardware security module utilizable for generating ~~a~~ the second cryptogram.

1114. The resource provider system of claim 68, the method further comprising:

validating that a user account corresponding to a user of the portable device conforms to one or more rules of the resource provider system.

12~~15~~. The resource provider system of claim 6~~8~~, wherein the access identifier is associated with a user account maintained by an authorization computer, the access identifier operable for being used to directly conduct a transaction.

13~~16~~. The resource provider system of claim 6~~8~~, wherein the authorization request message further comprises a value data field that is set to zero or empty, and wherein the method further comprises:

transmitting a subsequent authorization request message to the processing computer, the subsequent authorization request message comprising the value data field that is set to a non-zero numeral.

14~~17~~. A method comprising:

receiving, by a processing computer from a resource provider system in an authorization process, an authentication request message comprising a cryptogram and a portable device identifier and an intermediate access identifier, the intermediate access identifier comprising a virtual primary account number not operable for being used to directly conduct a transaction;

determining, by the processing computer, that the cryptogram is validated, wherein determining that the cryptogram is validated comprises:

generating a second cryptogram based at least in part on the portable device identifier and the intermediate access identifier;
comparing the second cryptogram with the cryptogram to determine if they match; and
upon determining that the second cryptogram and the cryptogram match, generating an authentication response message;

transmitting, by the processing computer, ~~an~~ the authentication response message to the resource provider system;

receiving, by the processing computer from the resource provider system, a first authorization request message comprising an access identifier;

transmitting, by the processing computer, a second authorization request message comprising the access identifier to an authorization computer;

receiving, by the processing computer from the authorization computer, a first authorization response message containing an authorization response indicator, the access identifier comprising a primary account number; and

transmitting, by the processing computer to the resource provider system, a second authorization response message comprising the authorization response indicator, wherein the authorization process is performed in real-time.

1518. The method of claim 1417, wherein the portable device identifier and the access identifier have different data formats.

~~19. The method of claim 17, wherein determining that the cryptogram is authenticated comprises:~~

~~generating a second cryptogram based at least in part on the portable device identifier;~~

~~comparing the second cryptogram with the cryptogram to determine if they match; and~~

~~upon determining that the second cryptogram and the cryptogram match, generating the authentication response message.~~

1620. The method of claim 1419, wherein the authentication request message further comprises ~~an~~ the intermediate access identifier, and wherein the second cryptogram is generated based at least in part on the intermediate access identifier.