WHAT IS CLAIMED IS:

1. A method comprising:

establishing, a first communication between a user device and a resource provider computer operating a host site in an interaction between the host site and a user of the user device;

establishing, a second communication between the user device and a portable device;

capturing, by the portable device, a biometric sample of the user;

converting, by the portable device, the biometric sample into a first biometric template;

comparing, by the portable device, the first biometric template with a second biometric template stored on the portable device, and determining a match result;

receiving, by the portable device from the resource provider computer, via the user device, interaction data;

generating, by the portable device, a cryptogram by encrypting at least the interaction data and the match result, or a derivative thereof, with an encryption key; and

transmitting, by the portable device, the cryptogram and access data comprising a primary account number or a payment token stored on the portable device, to the resource provider computer via the user device, wherein the resource provider computer generates an authorization request message comprising a transaction amount, the access data and the cryptogram and transmits the authorization request message to a remote server computer, wherein the remote server computer thereafter verifies the cryptogram, analyzes the match result, and allows the interaction to proceed using the access data based upon the verification of the cryptogram and the match result.

2. The method of claim 1, wherein the encryption key is symmetric key.

3. The method of claim 1, wherein the portable device is in the form of a card.

4. The method of claim 1, wherein the derivative is a hash of the interaction data and the match result, and wherein the method further comprises:

hashing the interaction data and the match result.

5. The method of claim 1, wherein the biometric sample is a fingerprint, a retinal scan, a facial scan, or a voice sample.

6. The method of claim 1, wherein the remote server computer is an authorizing entity computer configured to allow or deny access to secure data.

7. The method of claim 1, wherein the remote server computer is a processing computer.

8. The method of claim 1, further comprising:

transmitting, by the portable device to the remote server computer, a request for the interaction data.

9. A portable device capable of being coupled to a user device, the user device capable of establishing, a first communication between the user device and a resource provider computer operating a host site in an interaction between the host site and a user of the user device, comprising:

a processor;

a memory; and

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

establishing, a second communication between the user device and the portable device;

capturing, a biometric sample of the user;

converting, the biometric sample into a first biometric template;

comparing, the first biometric template with a second biometric template stored on the portable device, and determining a match result;

receiving from the resource provider computer, via the user device, interaction data;

generating, a cryptogram by encrypting at least the interaction data and the match result, or a derivative thereof, with an encryption key; and

transmitting, the cryptogram and access data comprising a primary account number or a payment token stored on the portable device, to the resource provider computer via the user device, wherein the resource provider computer generates an authorization request message comprising a transaction amount, the access data and the cryptogram and transmits the authorization request message to a remote server computer, wherein the remote server computer thereafter verifies the cryptogram, analyzes the match result, and allows the interaction to proceed using the access data based upon the verification of the cryptogram and the match result.

10. The portable device of claim 9, wherein the encryption key is a symmetric key.

11. The portable device of claim 9, wherein the portable device is in the form of a card.

12. The portable device of claim 9, wherein the portable device is in the form of a phone.

13. The portable device of claim 9, wherein the biometric sample is a fingerprint, a retinal scan, a facial scan, or a voice sample.

14. The portable device of claim 9, wherein the portable device comprises a reader device configured to read data from the portable device.

15. The portable device of claim 9, wherein the encryption key is stored in the memory and wherein the memory is a secure memory.

16. The portable device of claim 9, wherein the interaction data comprises a time stamp.

17. A method comprising:

establishing, a first communication between a user device and a resource provider computer operating a host site in an interaction between the host site and a user of the user device; and

receiving, by the resource provider computer, a cryptogram and access data comprising a primary account number or a payment token from the user device, wherein the user device received the cryptogram encoding a biometric match result and interaction data, or a derivative thereof, and the access data from a portable device,

generating, by the resource provider computer, an authorization request message comprising a transaction amount, the access data and the cryptogram; and

transmitting by the resource provider computer, the authorization request message to a remote server computer, which verifies the cryptogram and the access data, and allows the interaction to proceed if the cryptogram and the access data are verified.

18. The method of claim 17, wherein the portable device is in the form of a card.

19. The method of claim 17, wherein the interaction data includes a time of the interaction.

20. The method of claim 17, wherein the remote server computer is an authorizing entity computer that provides access to secure data.