WHAT IS CLAIMED IS:

1. A method comprising performing, by a user device:

storing, in a secure memory of the user device, a credential and a first encryption key for encrypting the credential for sending in a communication to an authorization server, the authorization server providing an authorization response regarding whether to authorize the user device to gain access to a resource;

obtaining, from an access device in communication with an access server and within communication distance of the user device via a short range communication mechanism, a second encryption key via the short range communication mechanism, the access server managing access to the resource and the second encryption key being associated with the access server;

receiving, from the access device that is local to the user device, resource information about the resource;

generating, by the user device, a message including at least:

a first portion of data encrypted using the first encryption key, such that the first portion of data is configured to be decrypted by the authorization server, the first portion of data including the credential; and

a second portion of data encrypted using the second encryption key, such that the second portion of data is configured to be decrypted by the access server, the second portion including at least a portion of the resource information, wherein the first portion of data is different from the second portion of data; and

providing the message over a wide area network to both the authorization server and the access server, the message triggering the authorization server to provide the authorization response to the access server.

2. The method of claim 1, wherein the short range communication mechanism is a scanning device, and the method further comprises scanning a machine readable code using the scanning device to obtain the second encryption key.

3. The method of claim 1, wherein the message is provided to the authorization server and the access server in parallel.

4. The method of claim 1, wherein the message is provided to the access device, which provides at least a portion of the message to the access server, wherein the portion of the message is then forwarded to the authorization server by the access server.

5. The method of claim 1, wherein the access server is only able to decrypt the second portion of data.

6. The method of claim 1, further comprising:

creating multiple secure channels between the user device and multiple computing entities, the multiple computing entities including at least the authorization server and the access server, wherein the first encryption key is generated during creation of a first secure channel between the user device and the authorization server, and wherein the second encryption key is generated during creation of a second secure channel between the user device and the access server.

7. A user device comprising:

one or more processors; and

a memory including instructions that, when executed by the one or more processors, cause the one or more processors to:

receive a first encryption key from a first computer via a network connection;

receive, from an access device in communication with an access server and within communication distance of the user device via a short range communication mechanism, a second encryption key via the short range communication mechanism, the access server managing access to a resource and the second encryption key being associated with the access server;

receive, from the access device, details related to a secure message to be generated using the user device;

generate the secure message that includes at least a first portion of data encrypted using the first encryption key and a second portion of data encrypted using the second encryption key; and

transmit the generated secure message to the access server.

8. The user device of claim 7, wherein the secure message also includes a header indicating a first location of the first portion of data and a second location of the second portion of data.

9. The user device of claim 7, wherein the instructions further cause the one or more processors to:

receive a first encryption protocol from the first computer, wherein the first portion of data in the secure message is encrypted using the first encryption protocol; and

receive a second encryption protocol from the access device via the short range communication mechanism, wherein the second portion of data in the secure message is encrypted using the second encryption protocol.

10. The user device of claim 7, wherein the short range communication mechanism is one of a near-field communications (NFC), Bluetooth, Bluetooth low-energy (BLE), a wireless local area network (e.g., WiFi), or iBeacon.

11. The user device of claim 7, wherein the secure message includes an access credential to be used to complete a transaction.

12. The user device of claim 7, wherein the access device is a point of sale device associated with a resource provider.

13. The user device of claim 7, wherein the access server enables access to a secure area or storage.

14. An authorization computer comprising:

a processor; and

a memory including instructions that, when executed with the processor, cause the authorization computer to, at least:

receive, from a user device, a request for an access credential, the access credential capable of being used to access a resource;

provide, to the user device, in response to receiving the request, the access credential and an encryption key;

receive, from a computing device, an authorization request message, the authorization request message comprising multiple portions of data, each

encrypted using a different encryption key, at least one portion of data of the multiple portions of data being encrypted using the encryption key, wherein at least a second portion of data of the multiple portions of data is encrypted using a second encryption key associated with a provider that manages access to the resource;

decrypt the at least one portion of data to identify transaction data;

determine, based at least in part on the transaction data, whether to approve a transaction to access the resource; and

provide an authorization response message to the provider of the resource, wherein the provider of the resource is caused to complete the transaction based on the authorization response message and the second portion of data of the multiple portions of data.

15. The authorization computer of claim 14, wherein the computing device is a local device within a vicinity of the user device.

16. The authorization computer of claim 14, wherein the authorization computer is only able to decrypt the at least one portion of data.

17. The authorization computer of claim 14, wherein the authorization request message is transmitted to multiple recipient computing entities.

18. The authorization computer of claim 17, wherein each of the multiple portions of data are configured to be decrypted by one of the multiple recipient computing entities.