WHAT IS CLAIMED IS:

1. A method comprising:

determining, by a contactless access device, an interaction value associated with an interaction;

responsive to determining the interaction value, prompting, by the contactless access device, a user operating a user device for a secret;

receiving, by the contactless access device, the secret from the user;

after receiving the secret from the user, receiving, by the contactless access device from the user device, an initial communication from the user device over a wireless communication medium;

receiving, by the contactless access device from the user device, a user device certificate comprising a public key;

verifying, by the contactless access device, the user device certificate;

concatenating, by the contactless access device, at least the secret and an unpredictable number to form a concatenated value;

encrypting, by the contactless access device, the concatenated value with the public key;

transmitting, by the contactless access device, the encrypted concatenated value over the wireless communication medium to the user device, wherein the user device decrypts the encrypted concatenated value with a private key corresponding to the public key, verifies the unpredictable number, verifies the secret by comparing the secret to another secret stored in the user device, determines whether or not the interaction is approved based at least upon the verification of the secret, produces a user device interaction authorization result, and then provides the user device interaction authorization result to the contactless access device; and

receiving, by the contactless access device from the user device, the user device interaction authorization result.

2. The method of claim 1, wherein the wireless communication medium uses NFC.

3. The method of claim 1, wherein the secret is a PIN, a passcode, a biometric, a one-time password, an access code, or a username-password pair.

4. The method of claim 1, wherein after determining the interaction value, the method further comprises:

determining, by the contactless access device, whether or not to prompt the user operating the user device for the secret based on the interaction value and a predetermined threshold.

5. The method of claim 1, wherein after receiving the secret, the method further comprises:

prompting, by the contactless access device, the user to bring the user device into communication range with the contactless access device;

generating, by the contactless access device, a read record command message that requests at least one or more certificates from the user device; and

when the user device is in the communication range with the contactless access device, providing, by the contactless access device, the read record command message to the user device, wherein the user device obtains the at least one or more certificates, generates a read record response message comprising the at least one or more certificates, and provides the read record response message to the contactless access device, wherein the at least one or more certificates includes the user device certificate.

6. The method of claim 1, wherein the user device is a card.

7. The method of claim 1, wherein the public key is a user device public key, and wherein the method further comprises:

receiving, by the contactless access device, an authorizing entity certificate comprising an authorizing entity public key from the user device.

8. The method of claim 7, wherein the authorizing entity certificate is signed by a certificate authority private key, and wherein prior to verifying the user device certificate the method further comprises:

verifying, by the contactless access device, the authorizing entity certificate using a certificate authority public key available to the contactless access device and corresponding to the certificate authority private key; and

if the authorizing entity certificate is valid, obtaining, by the contactless access device, the authorizing entity public key from the authorizing entity certificate.

9. The method of claim 8, wherein the user device certificate is signed by an authorizing entity private key corresponding to the authorizing entity public key, and wherein verifying the user device certificate further comprises:

verifying, by the contactless access device, the user device certificate using the authorizing entity public key; and

if the user device certificate is valid, obtaining, by the contactless access device, the user device public key from the user device certificate.

10. A contactless access device comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

determining an interaction value associated with an interaction;

responsive to determining the interaction value, prompting a user operating a user device for a secret;

receiving the secret from the user;

after receiving the secret from the user, receiving, from the user device, an initial communication from the user device over a wireless communication medium;

receiving, from the user device, a user device certificate comprising a public key;

verifying the user device certificate;

concatenating at least the secret and an unpredictable number to form a concatenated value;

encrypting the concatenated value with the public key;

transmitting the encrypted concatenated value over the wireless communication medium to the user device, wherein the user device decrypts the encrypted concatenated value with a private key corresponding to the public key, verifies the unpredictable number, verifies the secret by comparing the secret to another secret stored in the user device, determines whether or not the interaction is approved based at least upon the verification of the secret, produces a user device interaction authorization result, and then provides the user device interaction authorization result to the contactless access device; and

receiving, from the user device, the user device interaction authorization result.

11. The contactless access device of claim 10, wherein the public key is a user device public key, and wherein the method further comprises:

receiving an authorizing entity certificate comprising an authorizing entity public key from the user device, wherein the authorizing entity certificate is signed by a certificate authority private key;

verifying the authorizing entity certificate using a certificate authority public key available to the contactless access device and corresponds to the certificate authority private key; and

if the authorizing entity certificate is valid, obtaining the authorizing entity public key from the authorizing entity certificate.

12. The contactless access device of claim 11, wherein the user device certificate is signed by an authorizing entity private key corresponding to the authorizing entity public key, and wherein verifying the user device certificate further comprises:

verifying the user device certificate using the authorizing entity public key; and

if the user device certificate is valid, obtaining the user device public key from the user device certificate.

13. The contactless access device of claim 10, wherein the public key is a secret encipherment public key, and wherein the user device certificate includes the secret encipherment public key and a user device public key.

14. The contactless access device of claim 10, wherein concatenating at least the secret and the unpredictable number to form the concatenated value further comprises:

concatenating the secret, the unpredictable number, and a padding value to form the concatenated value, wherein the padding value increases a length of the concatenated value to be equal to an encryption data length specified by the public key.

15. The contactless access device of claim 10, wherein after receiving the user device interaction authorization result the method further comprises:

generating an authorization request message comprising at least the interaction value and interaction data associated with the interaction; and

providing the authorization request message to a resource provider computer, wherein the resource provider computer provides the authorization request message to a transport computer that provides the authorization request message to a network processing computer, wherein the network processing computer provides the authorization request message to an authorizing entity computer for authorization of the interaction.

16. The contactless access device of claim 15, wherein the method further comprises:

receiving an authorization response message from the authorizing entity computer, via the network processing computer, the transport computer, and the resource provider computer, wherein the authorization response message is created by the authorizing entity computer and includes an indication of whether or not the interaction is authorized.

17. The contactless access device of claim 10, wherein the method further comprises:

generating a challenge command message that requests the unpredictable number from the user device;

providing the challenge command message to the user device, wherein the user device obtains the unpredictable number and provides the unpredictable number to the contactless access device; and

receiving the unpredictable number from the user device.

18. A method comprising:

upon entering communication range with a contactless access device during an interaction, providing, by a user device, an initial communication from the user device over a wireless communication medium;

receiving, by the user device, a read record command from the contactless access device, wherein the read record command requests at least one or more certificates from the user device;

obtaining, by the user device, the at least one or more certificates from memory;

generating, by the user device, a read record response message comprising the at least one or more certificates;

providing, by the user device, the read record response message to the contactless access device in response to the read record command, wherein the one or certificates includes a user device certificate comprising a public key, wherein the contactless access device verifies the user device certificate, concatenates at least a secret provided by a user of the user device to the contactless access device and an unpredictable number to form a concatenated value, encrypts the concatenated value with the public key, and transmits the encrypted concatenated value over the wireless communication medium to the user device;

receiving, by the user device, the encrypted concatenated value from the contactless access device;

decrypting, by the user device, the encrypted concatenated value using a private key corresponding to the public key;

verifying, by the user device, the secret included in the concatenated value by comparing the secret to another secret stored in the user device;

producing, by the user device, a user device interaction authorization result based on whether or not the interaction is approved based at least upon the verification of the secret; and

providing, by the user device, the user device interaction authorization result to the contactless access device.

19. The method of claim 18, wherein after providing the user device interaction authorization result to the contactless access device, the contactless access device generates an authorization request message comprising at least an interaction value and interaction data associated with the interaction and provides the authorization request message to a resource provider computer, wherein the resource provider computer provides the authorization request message to a transport computer that provides the authorization request message to a network processing computer, wherein the network processing computer provides the authorization request message to an authorizing entity computer for authorization of the interaction.

20. The method of claim 18 further comprising:

receiving, by the user device, a challenge command message from the contactless access device that requests the unpredictable number;

obtaining, by the user device, the unpredictable number; and

providing, by the user device, the unpredictable number to the contactless access device.