WHAT IS CLAIMED IS:

1. A method comprising:

transmitting, by an access device to a communication device, a resource provider certificate and an access device certificate;

establishing a secure channel between the access device and the communication device using data from the resource provider certificate and the access device certificate; and

transmitting to or receiving data from the communication device using the secure channel, wherein before the secure channel is established, the communication device:

determines a resource provider public key using data in the resource provider certificate and a certificate authority public key;

determines an access device public key using data in the access device certificate and the resource provider public key; and

derives a first session key using the access device public key and a communication device private key, wherein the first session key is used to form the secure channel.

2. The method of claim 1, further comprising:

receiving, by the access device, a communication device public key; and

determining a second session key corresponding to the first session key using an access device private key and the communication device public key.

3. The method of claim 2, wherein the communication device public key is a blinded public key.

4. The method of claim 3, wherein the first and second session key are also each determined using an unpredictable number and a random number.

5. The method of claim 3, wherein after the secure channel is established, the method further comprises:

receiving, by the access device, the communication device public key and a blinding factor; and

verifying, by the access device, that the blinded public key is equal to the communication device public key blinded with the blinding factor.

6. The method of claim 1, further comprising:

receiving, by the access device from a resource provider computer, the resource provider certificate and the access device certificate.

7. The method of claim 6, wherein the resource provider certificate was received from a certificate authority computer, before the resource provider certificate was received by the access device.

8. The method of claim 1, wherein the access device and the communication device form the secure channel without authenticating each other.

9. The method of claim 1 further comprising:

receiving, by the access device, at least one certificate from the communication device; and

verifying, by the access device, the least one certificate, thereby verifying the authenticity of data received from the communication device.

10. An access device comprising:

a processor;

a memory device; and

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

transmitting, to a communication device, a resource provider certificate and an access device certificate;

establishing a secure channel between the access device and the communication device using data from the resource provider certificate and the access device certificate; and

transmitting to or receiving data from the communication device using the secure channel,

wherein before the secure channel is established, the communication device:

determines a resource provider public key using data in the resource provider certificate and a certificate authority public key;

determines an access device public key using data in the access device certificate and the resource provider public key; and

derives a first session key using the access device public key and a communication device private key, wherein the first session key is used to form the secure channel.

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

receiving a communication device public key; and

determining a second session key corresponding to the first session key using an access device private key and the communication device public key.

12. The access device of claim 11, wherein the communication device public key is a blinded public key.

13. The access device of claim 12, wherein the first and second session key are also each determined using an unpredictable number and a random number.

14. The access device of claim 12, wherein after the secure channel is established, the method further comprises:

receiving the communication device public key and a blinding factor; and

verifying that the blinded public key is equal to the communication device public key blinded with the blinding factor.

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

receiving, from a resource provider computer, the resource provider certificate and the access device certificate.

16. The access device of claim 15, wherein the resource provider certificate was received from a certificate authority computer, before the resource provider certificate was received by the access device.

17. The access device of claim 10, wherein the access device and the communication device form the secure channel without authenticating each other.

18. The method of claim 10, wherein the method further comprises:

receiving at least one certificate from the communication device; and

verifying the least one certificate, thereby verifying the authenticity of data received from the communication device.

19. A method comprising:

receiving, by a communication device from an access device, a resource provider certificate and an access device certificate;

establishing a secure channel between the access device and the communication device using data from the resource provider certificate and the access device certificate; and

transmitting to or receiving data from the access device using the secure channel, wherein before the secure channel is established, wherein the method further comprises:

determining, by the communication device, a resource provider public key using data in the resource provider certificate and a certificate authority public key;

determining, by the communication device, an access device public key using data in the access device certificate and the resource provider public key; and

deriving, by the communication device, a first session key using the access device public key and a communication device private key, wherein the first session key is used to form the secure channel.

20. The method of claim 19, wherein before the secure channel is established, the access device:

receives a communication device public key; and

determines a second session key corresponding to the first session key using an access device private key and the communication device public key.

21. The method of claim 20, wherein the communication device public key is a blinded public key.

22. The method of claim 21, wherein the first and second session key are also each determined using an unpredictable number and a random number.

23. The method of claim 19, wherein the access device:

receives, from a resource provider computer, the resource provider certificate and the access device certificate.

24. The method of claim 19, wherein the access device and the communication device form the secure channel without authenticating each other.

25. The method of claim 19 further comprising:

providing, by the communication device, at least one certificate to the access device, wherein the access device:

verifies the at least one certificate, thereby verifying the authenticity of data received from the communication device.

26. A communication device comprising:

a processor;

a memory device; and

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

receiving, from an access device, a resource provider certificate and an access device certificate;

establishing a secure channel between the access device and the communication device using data from the resource provider certificate and the access device certificate; and

transmitting to or receiving data from the access device using the secure channel,

wherein before the secure channel is established, the method further comprises:

determining a resource provider public key using data in the resource provider certificate and a certificate authority public key;

determining an access device public key using data in the access device certificate and the resource provider public key; and

deriving a first session key using the access device public key and a communication device private key, wherein the first session key is used to form the secure channel.

27. The communication device of claim 26, wherein before the secure channel is established, the access device:

receives a communication device public key; and

determines a second session key corresponding to the first session key using an access device private key and the communication device public key.

28. The communication device of claim 27, wherein the communication device public key is a blinded public key.

29. The communication device of claim 28, wherein the first and second session key are also each determined using an unpredictable number and a random number.

30. The communication device of claim 26, wherein the access device:

receives, from a resource provider computer, the resource provider certificate and the access device certificate.

31. The communication device of claim 26, wherein the access device and the communication device form the secure channel without authenticating each other.

32. The method of claim 26, wherein the method further comprises:

providing at least one certificate to the access device, wherein the access device:

verifies the at least one certificate, thereby verifying the authenticity of data received from the communication device.

33. A method comprising:

transmitting, by a resource provider computer to a certificate authority computer, certificate request values;

receiving, by the resource provider computer from the certificate authority computer, a resource provider certificate;

creating, by the resource provider computer, an access device certificate; and

transmitting, by the resource provider computer to an access device, the access device certificate and the resource provider certificate.

34. The method of claim 33 further comprising:

determining, by the resource provider computer, a resource provider public key and a resource provider private key using at least the resource provider certificate.

35. The method of claim 33, wherein the certificate request values comprise a first elliptic curve cryptography point and a resource provider identifier, wherein the certificate authority computer:

generates the resource provider certificate using at least the certificate request values.

36. The method of claim 33, wherein the resource provider computer creates more than one access device certificate for more than one access device.

37. A resource provider computer comprising:

a processor;

a memory device; and

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

transmitting, to a certificate authority computer, certificate request values;

receiving, from the certificate authority computer, a resource provider certificate;

creating an access device certificate; and

transmitting, to an access device, the access device certificate and the resource provider certificate.

38. The resource provider computer of claim 37, wherein the method further comprises:

determining a resource provider public key and a resource provider private key using at least the resource provider certificate.

39. The resource provider computer of claim 37, wherein the certificate request values comprise a first elliptic curve cryptography point and a resource provider identifier, wherein the certificate authority computer:

generates the resource provider certificate using at least the certificate request values.

40. The resource provider computer of claim 37, wherein the resource provider computer creates more than one access device certificate for more than one access device.