

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 transmitting, by an access device to a communication device, a resource
3 provider certificate and an access device certificate;
4 establishing a secure channel between the access device and the
5 communication device using data from the resource provider certificate and the access
6 device certificate; and
7 transmitting to or receiving data from the communication device using the
8 secure channel, wherein before the secure channel is established, the communication
9 device:
10 determines a resource provider public key using data in the resource
11 provider certificate and a certificate authority public key;
12 determines an access device public key using data in the access device
13 certificate and the resource provider public key; and
14 derives a first session key using the access device public key and a
15 communication device private key, wherein the first session key is used to form the
16 secure channel.
- 1 2. The method of claim 1, further comprising:
2 receiving, by the access device, a communication device public key; and
3 determining a second session key corresponding to the first session key
4 using an access device private key and the communication device public key.
- 1 3. The method of claim 2, wherein the communication device public
2 key is a blinded public key.
- 1 4. The method of claim 3, wherein the first and second session key
2 are also each determined using an unpredictable number and a random number.
- 1 5. The method of claim 3, wherein after the secure channel is
2 established, the method further comprises:

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

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

1 6. The method of claim 1, further comprising:
2 receiving, by the access device from a resource provider computer, the
3 resource provider certificate and the access device certificate.

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

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

1 9. The method of claim 1 further comprising:
2 receiving, by the access device, at least one certificate from the
3 communication device; and
4 verifying, by the access device, the at least one certificate, thereby
5 verifying the authenticity of data received from the communication device.

1 10. An access device comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for implementing a
6 method comprising:
7 transmitting, to a communication device, a resource provider certificate
8 and an access device certificate;
9 establishing a secure channel between the access device and the
10 communication device using data from the resource provider certificate and the access
11 device certificate; and

12 transmitting to or receiving data from the communication device using the
13 secure channel,
14 wherein before the secure channel is established, the communication
15 device:
16 determines a resource provider public key using data in the resource
17 provider certificate and a certificate authority public key;
18 determines an access device public key using data in the access device
19 certificate and the resource provider public key; and
20 derives a first session key using the access device public key and a
21 communication device private key, wherein the first session key is used to form the
22 secure channel.

1 11. The access device of claim 10, wherein the method further
2 comprises:
3 receiving a communication device public key; and
4 determining a second session key corresponding to the first session key
5 using an access device private key and the communication device public key.

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

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

1 14. The access device of claim 12, wherein after the secure channel is
2 established, the method further comprises:
3 receiving the communication device public key and a blinding factor; and
4 verifying that the blinded public key is equal to the communication device
5 public key blinded with the blinding factor.

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

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

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

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

1 18. The method of claim 10, wherein the method further comprises:
2 receiving at least one certificate from the communication device; and
3 verifying the at least one certificate, thereby verifying the authenticity of
4 data received from the communication device.

1 19. A method comprising:
2 receiving, by a communication device from an access device, a resource
3 provider certificate and an access device certificate;
4 establishing a secure channel between the access device and the
5 communication device using data from the resource provider certificate and the access
6 device certificate; and
7 transmitting to or receiving data from the access device using the secure
8 channel, wherein before the secure channel is established, wherein the method further
9 comprises:
10 determining, by the communication device, a resource provider public key
11 using data in the resource provider certificate and a certificate authority public key;
12 determining, by the communication device, an access device public key
13 using data in the access device certificate and the resource provider public key; and
14 deriving, by the communication device, a first session key using the
15 access device public key and a communication device private key, wherein the first
16 session key is used to form the secure channel.

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

3 receives a communication device public key; and
4 determines a second session key corresponding to the first session key
5 using an access device private key and the communication device public key.

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

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

1 23. The method of claim 19, wherein the access device:
2 receives, from a resource provider computer, the resource provider
3 certificate and the access device certificate.

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

1 25. The method of claim 19 further comprising:
2 providing, by the communication device, at least one certificate to the
3 access device, wherein the access device:
4 verifies the at least one certificate, thereby verifying the authenticity of
5 data received from the communication device.

1 26. A communication device comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for implementing a
6 method comprising:
7 receiving, from an access device, a resource provider certificate and an
8 access device certificate;

9 establishing a secure channel between the access device and the
10 communication device using data from the resource provider certificate and the access
11 device certificate; and
12 transmitting to or receiving data from the access device using the secure
13 channel,
14 wherein before the secure channel is established, the method further
15 comprises:
16 determining a resource provider public key using data in the resource
17 provider certificate and a certificate authority public key;
18 determining an access device public key using data in the access device
19 certificate and the resource provider public key; and
20 deriving a first session key using the access device public key and a
21 communication device private key, wherein the first session key is used to form the
22 secure channel.

1 27. The communication device of claim 26, wherein before the secure
2 channel is established, the access device:
3 receives a communication device public key; and
4 determines a second session key corresponding to the first session key
5 using an access device private key and the communication device public key.

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

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

1 30. The communication device of claim 26, wherein the access device:
2 receives, from a resource provider computer, the resource provider
3 certificate and the access device certificate.

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

1 32. The method of claim 26, wherein the method further comprises:
2 providing at least one certificate to the access device, wherein the access
3 device:
4 verifies the at least one certificate, thereby verifying the authenticity of
5 data received from the communication device.

1 33. — A method comprising:
2 transmitting, by a resource provider computer to a certificate authority
3 computer, certificate request values;
4 receiving, by the resource provider computer from the certificate authority
5 computer, a resource provider certificate;
6 creating, by the resource provider computer, an access device certificate;
7 and
8 transmitting, by the resource provider computer to an access device, the
9 access device certificate and the resource provider certificate.

1 34. — The method of claim 33 further comprising:
2 determining, by the resource provider computer, a resource provider
3 public key and a resource provider private key using at least the resource provider
4 certificate.

1 35. — The method of claim 33, wherein the certificate request values
2 comprise a first elliptic curve cryptography point and a resource provider identifier,
3 wherein the certificate authority computer:
4 generates the resource provider certificate using at least the certificate
5 request values.

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

1 37. ~~A resource provider computer comprising:~~
2 ~~a processor;~~
3 ~~a memory device; and~~
4 ~~a computer readable medium coupled to the processor, the computer-~~
5 ~~readable medium comprising code executable by the processor for implementing a~~
6 ~~method comprising:~~
7 ~~transmitting, to a certificate authority computer, certificate request values;~~
8 ~~receiving, from the certificate authority computer, a resource provider~~
9 ~~certificate;~~
10 ~~creating an access device certificate; and~~
11 ~~transmitting, to an access device, the access device certificate and the~~
12 ~~resource provider certificate.~~

1 38. ~~The resource provider computer of claim 37, wherein the method~~
2 ~~further comprises:~~
3 ~~determining a resource provider public key and a resource provider private~~
4 ~~key using at least the resource provider certificate.~~

1 39. ~~The resource provider computer of claim 37, wherein the certificate~~
2 ~~request values comprise a first elliptic curve cryptography point and a resource provider~~
3 ~~identifier, wherein the certificate authority computer:~~
4 ~~generates the resource provider certificate using at least the certificate~~
5 ~~request values.~~

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