WHAT IS CLAIMED IS:

1. A computer-implemented method for performing an authentication procedure when joining a wireless network, comprising:

compressing a certificate chain based on a first mapping to generate a compressed certificate chain, wherein the certificate chain includes a first data entry and the compressed certificate chain includes a first index in place of the first data entry; and

transmitting the compressed certificate chain to a neighboring node to perform the authentication procedure with the neighboring node based on the first data entry.

2. The computer-implemented method of claim 1, wherein first data entry includes a greater number of bits than the size of the first index in bits, and the certificate chain includes a greater number of bits than the compressed certificate chain.

3. The computer-implemented method of claim 1, wherein the certificate chain comprises a chain of X.509 certificates, the first data entry comprises at least one of a field name and a field value included in the chain of X.509 certificates, and wherein the authentication procedure comprises a certificate exchange that, when completed, establishes an authenticated communication channel with the neighboring node.

4. The computer-implemented method of claim 1, wherein compressing the certificate chain comprises:

determining that the first mapping includes the first data entry;

determining that the first data entry corresponds to the first index in the first mapping; and

replacing the first data entry with the first index in the certificate chain.

5. The computer-implemented method of claim 1, wherein compressing the certificate chain comprises:

identifying a second data entry included in the certificate chain;

determining that the first mapping does not include the second data entry; and

incorporating the second data entry into the first mapping at a position that corresponds to a second index.

6. The computer-implemented method of claim 5, further comprising flushing the second data entry and the second index from the first mapping when the authentication procedure has completed.

7. The computer-implemented method of claim 1, wherein the first mapping is pre-populated with a first set of data entries prior to compressing the certificate chain, wherein compressing the certificate chain comprises dynamically populating the first mapping with a second set of data entries, and further comprising removing the second set of data entries from the first mapping when the authentication procedure has completed.

8. The computer-implemented method of claim 1, further comprising decompressing, at the neighboring node, the compressed certificate chain based on a second mapping to generate an uncompressed certificate chain, wherein the uncompressed certificate chain includes the first data entry in place of the first index.

9. The computer-implemented method of claim 1, further comprising:

determining, at the neighboring node, that the second mapping does not include the first data entry; and

incorporating the first data entry into the second mapping at a position that corresponds to the first index.

10. A computer-implemented method for performing an authentication procedure when joining a wireless network, comprising:

receiving a compressed certificate chain from a neighboring node;

decompressing the compressed certificate chain based on a first mapping to generate a decompressed certificate chain, wherein the compressed certificate chain includes a first index and the decompressed certificate chain includes a first data entry in place of the first index; and

performing an authentication procedure with the neighboring node based on the first data entry.

11. The computer-implemented method of claim 10, wherein decompressing the compressed certificate chain comprises:

determining that the first mapping includes the first index;

determining that the first index corresponds to the first data entry in the first mapping; and

replacing the first index with the first data entry in the certificate chain.

12. The computer-implemented method of claim 10, further comprising:

extracting a second data entry from the compressed certificate chain;

determining that the first mapping does not include the second data entry; and

incorporating the second data entry into the first mapping at a position that corresponds to a second index.

13. The computer-implemented method of claim 12, further comprising:

determining that the authentication procedure has completed; and

in response, flushing the second data entry and the second index from the first mapping.

14. The computer-implemented method of claim 10, further comprising:

determining that the compressed certificate chain is compressed; and

in response, preventing the compressed certificate chain from being stored in a cache memory.

15. The computer-implemented method of claim 10, wherein the certificate chain comprises a chain of X.509 certificates, and the first data entry comprises at least one of a field name and a field value included in the chain of X.509 certificates.

16. The computer-implemented method of claim 10, wherein the authentication procedure comprises a certificate exchange that, when completed, establishes an authenticated communication channel with the neighboring node.

17. A wireless network, comprising:

a first node that includes:

a first memory storing a first set of instructions, and

a first processor that executes the first set of instructions to perform the steps of:

compressing a certificate chain to generate a compressed certificate chain, and

transmitting the compressed certificate chain across the wireless network; and

a second node that includes:

a second memory storing a second set of instructions, and

a second processor that executes the second set of instructions to perform the steps of:

receiving the compressed certificate chain,

decompressing the compressed certificate chain to generate a decompressed certificate chain, and

performing an authentication procedure with the first node based on the decompressed certificate chain.

18. The wireless network of claim 17, wherein the first processor compresses the certificate chain by:

determining that the certificate chain includes a first data entry;

determining that a first mapping also includes the first data entry;

determining that the first data entry corresponds to a first index in the first mapping; and

replacing the first data entry with the first index in the certificate chain.

19. The wireless network of claim 18, wherein first data entry includes a greater number of bits than the size of the first index in bits, and the certificate chain includes a greater number of bits than the compressed certificate chain.

20. The wireless network of claim 18, wherein the second processor decompresses the compressed certificate chain by:

determining that the compressed certificate chain includes a first index;

determining that a second mapping also includes the first index;

determining that the first index corresponds to the first data entry in the second mapping; and

~~replacing the first index with the first data entry in the certificate chain.~~

~~21. The wireless network of claim 18, wherein the second processor performs the additional steps of:~~

~~extracting a second data entry from the compressed certificate chain;~~

~~determining that a second mapping does not include the second data entry; and~~

~~incorporating the second data entry into the second mapping at a position that corresponds to a second index.~~

~~22. The wireless network of claim 17, wherein the certificate chain comprises a chain of X.509 certificates, and a first data entry included in the chain of X.509 certificates comprises at least one of a field name and a field value.~~

~~23. The wireless network of claim 17, wherein compressing the certificate chain comprises performing an elliptic curve compression operation on a public key portion of the certificate chain.~~

1. A method, comprising:

receiving, by a node of a mesh network, a compression dictionary including associations between one or more data entries in certificate chains and one or more indices in corresponding compressed certificate chains;

compressing, by the node, a first certificate chain based on the compression dictionary to generate a compressed certificate chain, wherein the first certificate chain includes a first data entry and the compressed certificate chain includes a first index in place of the first data entry, and the compression dictionary includes a first mapping between the first index and the first data entry; and

transmitting, by the node, the compressed certificate chain to a neighboring node to perform an authentication procedure with the neighboring node based on the first data entry.

2. The method of claim 1, wherein the first data entry includes a greater number of bits than a size of the first index in bits, and the first certificate chain includes a greater number of bits than the compressed certificate chain.

3. The method of claim 1, wherein the first certificate chain comprises a chain of X.509 certificates, the first data entry comprises at least one of a field name and a field value included in the chain of X.509 certificates, and wherein the authentication procedure comprises a certificate exchange that, when completed, establishes an authenticated communication channel with the neighboring node.

4. The method of claim 1, wherein compressing the first certificate chain comprises:

determining that the first mapping includes the first data entry;

determining that the first data entry corresponds to the first index in the first mapping; and

replacing the first data entry with the first index in the first certificate chain.

5. The method of claim 1, wherein compressing the first certificate chain comprises:

identifying a second data entry included in the first certificate chain;

determining that the first mapping does not include the second data entry; and

incorporating the second data entry into the first mapping at a position that corresponds to a second index.

6. The method of claim 5, further comprising flushing the second data entry and the second index from the first mapping when the authentication procedure has completed.

7. The method of claim 1, wherein the first mapping is received and at least partially pre-populated with a first set of data entries during manufacturing of the node or in response to the node joining the mesh network.

8. The method of claim 1, further comprising:

decompressing, at the neighboring node, the compressed certificate chain based on a second mapping to generate an uncompressed certificate chain;

determining, at the neighboring node, that the second mapping does not include the first data entry; and

incorporating the first data entry into the second mapping at a position that corresponds to the first index.

9. A method, comprising:

receiving, by a node of a mesh network, a compression dictionary including associations between one or more data entries in certificate chains and one or more indices in corresponding compressed certificate chains;

receiving, by the node after receiving the compression dictionary, a compressed certificate chain from a neighboring node;

decompressing, by the node, the compressed certificate chain based on the compression dictionary to generate a decompressed certificate chain, wherein the compressed certificate chain includes a first index and the decompressed certificate chain includes a first data entry in place of the first index and the compression dictionary includes a first mapping between the first index and the first data entry; and

performing, by the node, an authentication procedure with the neighboring node based on the first data entry.

10. The method of claim 9, wherein decompressing the compressed certificate chain comprises:

determining that the first mapping includes the first index;

determining that the first index corresponds to the first data entry in the first mapping; and

replacing the first index with the first data entry in the decompressed certificate chain.

11. The method of claim 9, further comprising:

extracting a second data entry from the compressed certificate chain;

determining that the first mapping does not include the second data entry; and

incorporating the second data entry into the first mapping at a position that corresponds to a second index.

12. The method of claim 11, further comprising:
determining that the authentication procedure has completed; and
in response, flushing the second data entry and the second index from the first mapping.

13. The method of claim 9, further comprising:
determining that the compressed certificate chain is compressed; and
in response, preventing the compressed certificate chain from being stored in a cache memory.

14. The method of claim 9, wherein the decompressed certificate chain comprises a chain of X.509 certificates, and the first data entry comprises at least one of a field name and a field value included in the chain of X.509 certificates.

15. The method of claim 9, wherein the authentication procedure comprises a certificate exchange that, when completed, establishes an authenticated communication channel with the neighboring node.

16. A wireless network, comprising:
a first node that includes:
a first memory storing a first set of instructions, and
a first processor that executes the first set of instructions to perform the steps of:
receiving a compression dictionary including associations between one or more data entries in certificate chains and one or more indices in corresponding compressed certificate chains,
compressing a first certificate chain based on the compression dictionary to generate a compressed certificate chain, wherein the first certificate chain includes a first data entry and the compressed certificate chain includes a first index

in place of the first data entry and the compression dictionary includes a first mapping between the first index and the first data entry, and

transmitting the compressed certificate chain across the wireless network; and

a second node that includes:

a second memory storing a second set of instructions, and

a second processor that executes the second set of instructions to perform the steps of:

receiving the compression dictionary,

receiving the compressed certificate chain after receiving the compression dictionary,

decompressing the compressed certificate chain based on the compression dictionary to generate a decompressed certificate chain, and

performing an authentication procedure with the first node based on the decompressed certificate chain.

17. The wireless network of claim 16, wherein the first processor compresses the first certificate chain by:

determining that the first certificate chain includes the first data entry;

determining that the first mapping also includes the first data entry;

determining that the first data entry corresponds to the first index in the first mapping; and

replacing the first data entry with the first index in the first certificate chain.

18. The wireless network of claim 17, wherein the first data entry includes a greater number of bits than a size of the first index in bits, and the first certificate chain includes a greater number of bits than the compressed certificate chain.

19. The wireless network of claim 17, wherein the second processor decompresses the compressed certificate chain by:

determining that the compressed certificate chain includes the first index;

determining that a second mapping also includes the first index;

determining that the first index corresponds to the first data entry in the second mapping; and

replacing the first index with the first data entry in the decompressed certificate chain.

20. The wireless network of claim 17, wherein the second processor performs the additional steps of:

extracting a second data entry from the compressed certificate chain;

determining that a second mapping does not include the second data entry; and

incorporating the second data entry into the second mapping at a position that corresponds to a second index.

21. The wireless network of claim 16, wherein the first certificate chain comprises a chain of X.509 certificates, and the first data entry included in the chain of X.509 certificates comprises at least one of a field name and a field value.

22. The wireless network of claim 16, wherein compressing the first certificate chain comprises performing an elliptic curve compression operation on a public key portion of the first certificate chain.

23. The method of claim 1, wherein:

the first certificate chain further includes a second data entry; and

the method further comprises storing, by the node and in a dynamic portion of the compression dictionary, a second mapping between a second index and the second data entry.