WHAT IS CLAIMED IS:

1. A method, comprising:

receiving, by a node of a mesh network, a shared compression dictionary including a static portion and a dynamic portion, the shared compression dictionary storing 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 shared compression dictionary to generate a compressed certificate chain, wherein:

the first certificate chain includes a first data entry and a second data entry,

the compressed certificate chain includes a first index in place of the first data entry, and

the static portion of the shared compression dictionary includes a first mapping between the first index and the first data entry;

storing, by the node and in the dynamic portion of the shared compression dictionary, a second mapping between the second data entry and a second index; 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 the second data entry; and

determining that the static portion of the shared compression dictionary does not include the second data entry.

6. The method of claim 5, further comprising flushing the second data entry and the second index from the dynamic portion of the shared compression dictionary when the authentication procedure has completed.

7. The method of claim 1, wherein the static portion of the shared compression dictionary 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 shared compression dictionary to generate an uncompressed certificate chain, the second shared compression dictionary including a second static portion and a second dynamic portion;

determining, at the neighboring node, that the second shared compression dictionary does not include the second data entry; and

incorporating a second mapping between a second index and the second data entry into the second dynamic portion of the second shared compression dictionary.

9. The method of claim 1, wherein compressing the first certificate chain does not replace a first occurrence of the second data entry in the compressed certificate chain.

10. A method, comprising:

receiving, by a node of a mesh network, a shared compression dictionary including a static portion and a dynamic portion, the shared compression dictionary storing 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 shared compression dictionary, a compressed certificate chain from a neighboring node;

decompressing, by the node, the compressed certificate chain based on the shared 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 static portion of the shared compression dictionary includes a first mapping between the first index and the first data entry;

storing, by the node and in the dynamic portion of the shared compression dictionary, a second mapping between a second index and a second data entry included in the compressed certificate chain; and

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

11. The 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 decompressed certificate chain.

12. The method of claim 10, further comprising:
extracting the second data entry from the compressed certificate chain; and
determining that the static portion of the shared compression dictionary does not include the second data entry.

13. The method of claim 12, further comprising:
determining that the authentication procedure has completed; and
in response, flushing the second data entry from the dynamic portion of the shared compression dictionary.

14. The 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 method of claim 10, 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.

16. The 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:
receiving a shared compression dictionary including a static portion and a dynamic portion, the shared compression dictionary storing 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 shared compression dictionary to generate a compressed certificate chain, wherein (i) the first certificate chain includes a first data entry and a second data entry, (ii) the compressed certificate chain includes a first index in place of the first data entry, and (iii) the static portion of the shared compression dictionary includes a first mapping between the first index and the first data entry,

storing, in the dynamic portion of the shared compression dictionary, a second mapping between the second data entry and a second index, 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 a second shared compression dictionary including a second static portion and a second dynamic portion,

receiving the compressed certificate chain after receiving the second shared compression dictionary,

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

storing, in the second dynamic portion of the second shared compression dictionary, the second mapping between the second data entry and the second index, 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 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.

19. The wireless network of claim 18, 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.

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

determining that the compressed certificate chain includes the first index;

determining that the second shared compression dictionary also includes the first index;

determining that the first index corresponds to the first data entry in the second shared compression dictionary; and

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

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

extracting the second data entry from the compressed certificate chain; and

determining that the second dynamic portion of the second shared compression dictionary.

22. The wireless network of claim 17, 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.

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