WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a server node from a client node, a client compression dictionary that includes one or more first mappings between one or more first index values and one or more first data entries, the one or more first data entries identifying one or more first certificates that are included in a certificate cache of the client node; and

in response to the server node receiving the client compression dictionary:

processing, by the server node, the one or more first data entries to identify the one or more first certificates that are included in the certificate cache of the client node;

identifying, by the server node, one or more second certificates that are not included in the one or more first certificates and should be transmitted to the client node; and

transmitting, from the server node to the client node, the one or more second certificates.

2. The method of claim 1, further comprising:

storing, at the server node, a server compression dictionary that includes one or more second mappings between one or more second index values and one or more second data entries included in a certificate cache of the server node;

wherein identifying the one or more second certificates is further based on the server compression dictionary.

3. The method of claim 2, wherein identifying the one or more second certificates comprises:

identifying, from the one or more second data entries, a subset of data entries included in the server compression dictionary that are not included in the client compression dictionary;

wherein the one or more second certificates correspond to the subset of data entries.

4. The method of claim 2, wherein transmitting the one or more second certificates comprises compressing the one or more second certificates based on at least one of the client compression dictionary or the server compression dictionary.

5. The method of claim 1, wherein the one or more second certificates includes only a client certificate of the server node.

6. The method of claim 1, further comprising transmitting, from the server node to the client node, a server compression dictionary that includes one or more second mappings between one or more second index values and one or more second data entries, the one or more second data entries identifying the one or more second certificates that are in a certificate cache of the server node.

7. The method of claim 6, further comprising:

receiving, at the server node from the client node, one or more third certificates; and

updating, at the server node, the server compression dictionary based on the one or more third certificates.

8. The method of claim 7, wherein:

the one or more third certificates comprise one or more compressed certificates, and

the method further comprises decompressing, at the server node, the one or more compressed certificates.

9. The method of claim 1, further comprising:

validating, at the server node, the client compression dictionary based on the one

or more first data entries; and

in response to successfully validating the client compression dictionary:

identifying, by the server node, the one or more second certificates, and

transmitting, from the server node to the client node, the one or more second certificates in response to successfully validating the client compression dictionary.

10. The method of claim 9, further comprising:

receiving, at the server node from a second client node, a second client compression dictionary that includes one or more third mappings between one or more third index values and one or more third data entries included in a certificate cache of the second client node;

validating, by the server node, the second client compression dictionary based on the one or more third data entries included in a certificate cache of the second client node; and

in response to failing to validate the second client compression dictionary,

terminating, by the server node, a connection with the second client node.

11. One or more non-transitory computer-readable media storing instructions which, when executed by one or more processors, cause the one or more processors of a server node to perform operations comprising:

receiving, from a client node, a client compression dictionary that includes one or more first mappings between one or more first index values and one or more first data entries, the one or more first data entries identifying one or more first certificates that are included in a certificate cache of the client node; and

in response to receiving the client compression dictionary:

determining, using the one or more first data entries the one or more first certificates that are included in the certificate cache of the client node,

determining whether to transmit one or more second certificates to the

client node; wherein the one or more second certificates are not included in the one or more first certificates, and

in response to determining that the one or more second certificates should be transmitted to the client node, transmitting the one or more second certificates to the client node.

12. The one or more non-transitory computer-readable media of claim 11, wherein the operations further include:

storing a server compression dictionary that includes one or more second mappings between one or more second index values and one or more second data entries, the one or more second data entries identifying the one or more second certificates included in a certificate cache of the server node;

wherein determining whether to transmit the one or more second certificates to the client node is further based on the server compression dictionary.

13. The one or more non-transitory computer-readable media of claim 12, wherein determining whether to transmit the one or more second certificates to the client node comprises:

identifying, from the one or more second data entries, a subset of data entries included in the server compression dictionary that are not included in the client compression dictionary;

wherein the one or more second certificates correspond to the subset of data entries.

14. A network device comprising:

a transceiver;

a processor; and

a memory storing executable instructions that, when executed by the processor, cause the network device to:

receive, via a transceiver and from a second network device, a

compression dictionary that includes one or more first mappings between one or more first index values and one or more first data entries, the one or more first data entries identifying one or more first certificates that are included in a certificate cache of the second network device;

in response to receiving the compression dictionary:

processing the one or more first data entries to identify the one or more first certificates that are included in the certificate cache of the second network device,

identifying one or more second certificates as not included in the certificate cache of the second network device; and

transmit the one or more second certificates to the second network device.

15. The network device of claim 14, wherein the received compression dictionary corresponds to a dynamically-updated portion of a compression dictionary of the second network device.

16. The network device of claim 14, wherein the one or more second certificates that are not included in the certificate cache of the second network device include a client certificate associated with the network device.

17. The network device of claim 14, wherein the executable instructions further cause the network device to:

store, at the network device, a local compression dictionary that includes one or more second mappings between one or more second index values and one or more second data entries that are included in a certificate cache of the network device;

wherein identifying the one or more second certificates is further based on the local compression dictionary.