**TLSlite Checklist**

**Tailang Cao u1480633**

1. The name of file created by the CA and certificate setup that is needed for your TLSlite client and server.

CAcertificate.pem,

CAprivateKey.pem,

serverPrivateKey.der,

CASignedServerCertificate.pem,

clientPrivateKey.der,

CASignedClientCertificate.pem

1. Which programs will read each file: client, server, or both. Note that "none" is not an option here; don't mention files that won't be needed at run time.

Client: CAcertificate.pem, clientPrivateKey.der, CASignedClientCertificate.pem

Server: CAcertificate.pem, serverPrivateKey.der, CASignedServerCertificate.pem

Both: CAcertificate.pem

1. A one-line description of the file's content/role.

CAcertificate.pem:

Public key certificate of the Certificate Authority (CA) used for verifying client and server certificates.

CAprivateKey.pem:

Private key of the Certificate Authority (CA) used for signing client and server certificates.

serverPrivateKey.der:

Private key of the server in DER binary format, used for authenticating the server during TLS handshake.

CASignedServerCertificate.pem:

Certificate signed by the CA for the server, containing the server's public key.

clientPrivateKey.der:

Private key of the client in DER binary format, used for authenticating the client during TLS handshake.

CASignedClientCertificate.pem:

Content/Role: Certificate signed by the CA for the client, containing the client's public key.