TLS Checkpoint
Corinne Jones

File Name	Read By	Description
CASignedClientCertificat.pem	Client	This file contains the client's certification signed by the CA. This is used by the client to authenticate its identity to the server.
CASignedServerCertificate.pem	Server	This file contains the server's certification signed by the CA. This is used by the server to authenticate its identity to the client.
CAcertificate.pem	Client & Server	This file contains the CA's public certificate. This is used by the client and server to verify the identity of one another. Both use this to ensure they are communicated with a CA trusted entity.
clientPrivateKey.der	Client	This file contains the client's private key. It is used for decrypting information received from the server that was encrypted with the client's public key, and for signing messages sent to the server.
serverPrivateKey.der	Server	This file contains the server's private key. It is used for decrypting information received from the client that was encrypted with the server's public key, and for signed messages sent to the client.