Obtaining an SSL certificate for Chariot

Chariot uses certificates and TLS/SSL to secure Chariot HTTP and MQTT traffic. The process for obtaining SSL certificates to be used to secure HTTP and MQTT traffic to Chariot is the same whether using an external/commercial Certificate Authority (CA) or your company's internal Certificate Authority (CA). Cirrus Link doesn't recommend any specific Certificate Authority (CA), but we do recommend using non-self-signed certificates from a trusted Certificate Authority for securing your Production assets.

1. Create your CSR (Certificate Signing Request)
    a. Generate/select the keypair to use to generate the CSR
        i. The private part of this public/private keypair is one of the artifacts that you will need to upload to Chariot to enable HTTPS /MQTTS. Please be sure to keep this keypair in a known, secure location.
    b. Complete all required CSR fields
2. Submit your CSR to your Certificate Authority (CA) of choice
    a. Proof of control
    b. Certificates you should expect to receive from the Certificate Authority (CA)
        i. Signed SSL server certificate signed by the CA
        ii. CA chain (chain-of-trust): typically contains the Root CA certificate and any intermediate CA certificates in a single file