



SSL Certificate

Certificate body

Certificate private key

Certificate chain (optional)





SSL Certificate

Self-signed SSL/TLS certificate - Chain not required

Certificate signed by a certificate authority (CA) - Chain required





Cryptographic algorithms

- 1024-bit RSA (RSA_1024)
- 2048-bit RSA (RSA_2048)
- 3072-bit RSA (RSA_3072)
- 4096-bit RSA (RSA_4096)
- Elliptic Prime Curve 256 bit (EC_prime256v1)
- Elliptic Prime Curve 384 bit (EC_secp384r1)
- Elliptic Prime Curve 521 bit (EC_secp521r1)





Certificate

- The certificate must be an SSL/TLS X.509 version 3 certificate
- It must contain a public key, the fully qualified domain name
- Certificate can be self-signed by your private key or by the private key of an issuing CA
- The private key must be unencrypted
- The certificate, private key, and certificate chain must be PEM-encoded







.crt File





Certificate private key

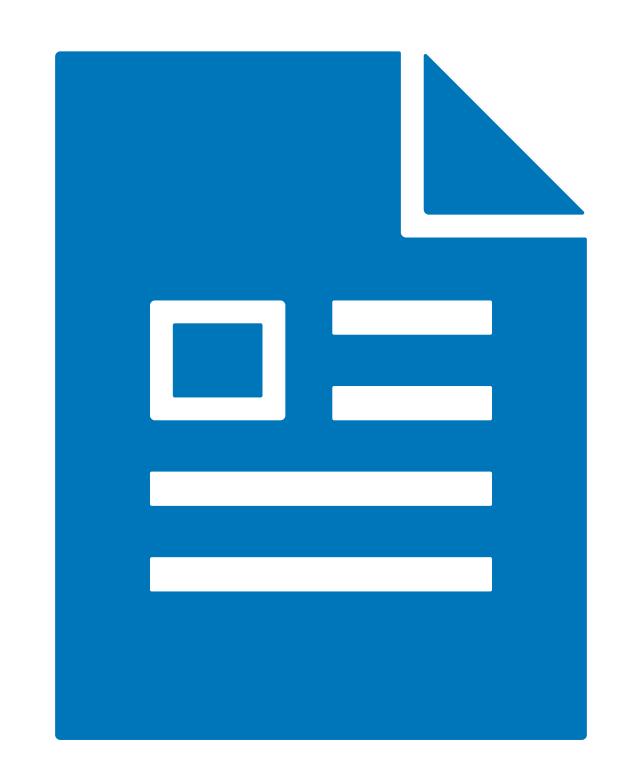


private-key





Certificate chain (optional)



.crt File



