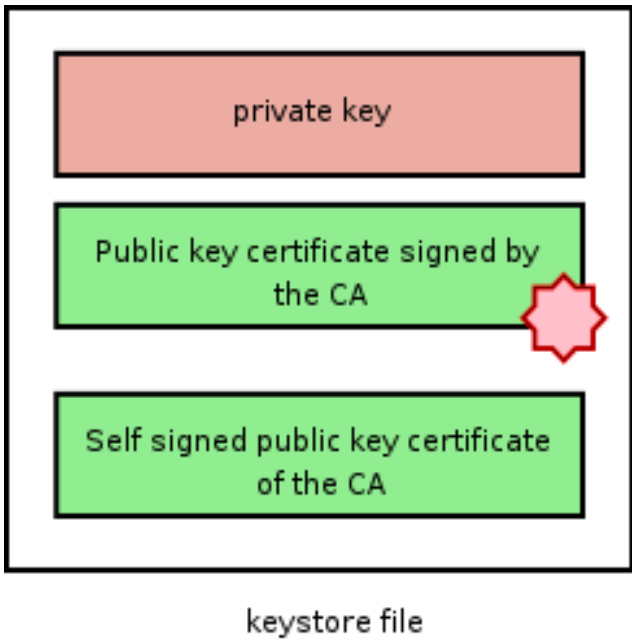
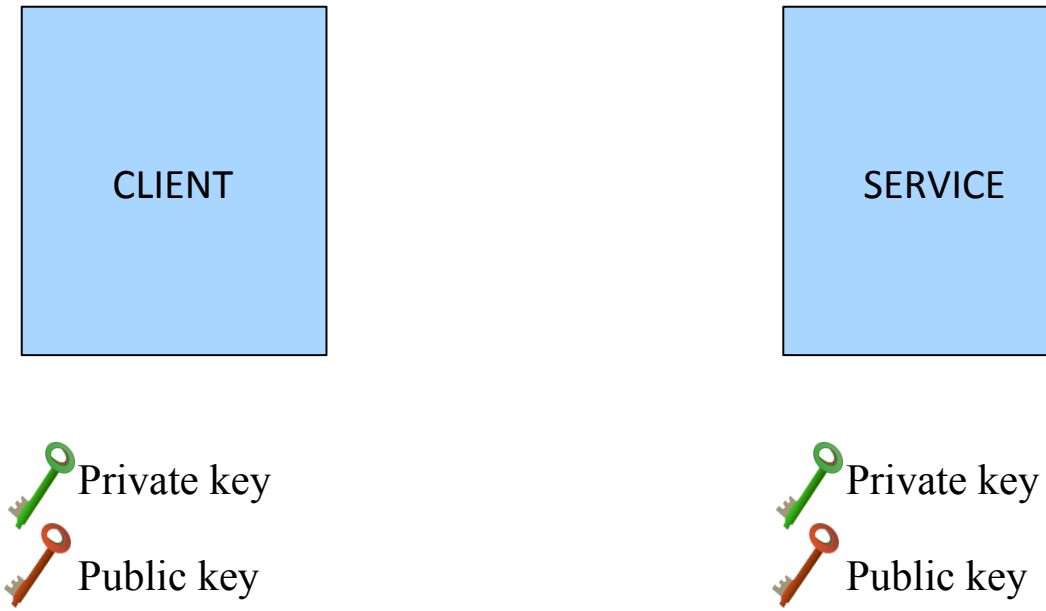
Key Management

Key manipulation

- JDK keytool
- OpenSSL
- A keystore
  - Private Keys
  - Certificates
- Types
  - PKCS12
  - JKS





- Client and service should share each other's public keys

Requirement

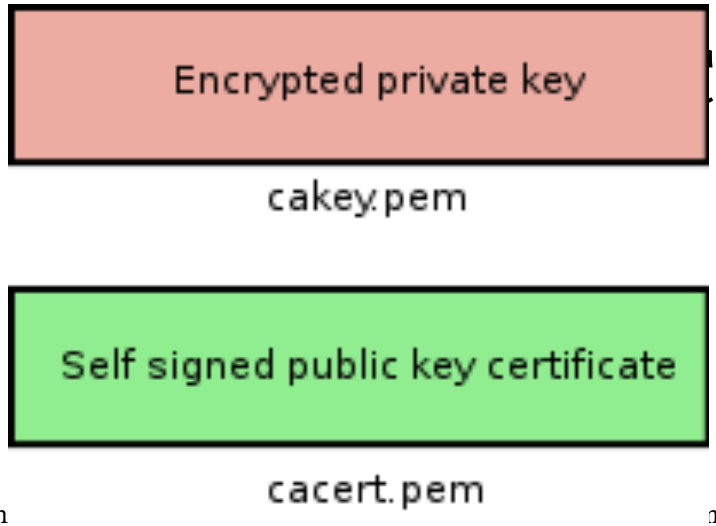
- Two keystores for the service and client
- Signed by a CA

- Make sure you have
  - OpenSSL
  - JDK

Simple Certificate Authority

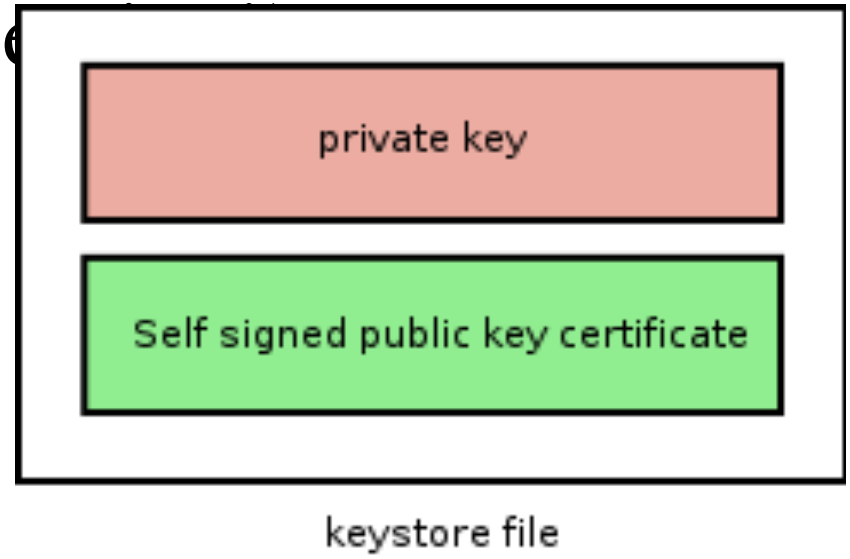
- $ openssl req -x509 -newkey rsa:1024 \
- -keyout cakey.pem -out cacert.pem -config openssl.cnf

- This creates



Client and Service Keys

- $ keytool -genkey -alias client -keyalg RSA -keystore client.jks
- $ keytool -genkey -alias service -keyalg RSA -keystore se



Now we need our CA to sign the public keys

Certificate Signing Request (CSR)

- $ keytool -certreq -keystore client.jks -storepass changeme -alias client -file client.cert.req

- $ keytool -certreq -keystore service.jks -storepass changeme -alias service -file service.cert.req

Sign the CSRs

- $ openssl ca -config openssl.cnf -out client.pem -infiles client.cert.req

- $ openssl ca -config openssl.cnf -out service.pem -infiles service.cert.req

- And convert the signed certificates and CA cert to DER
- $ openssl x509 -outform DER -in client.pem -out client.cert
- $ openssl x509 -outform DER -in service.pem -out service.cert
- $ openssl x509 -outform DER -in cacert.pem -out cacert.cert

Import Certificates

- Import CA certificate
- $ keytool -import -file cacert.cert -keystore service.jks -storepass changeme -alias ca
- $ keytool -import -file cacert.cert -keystore client.jks -storepass changeme -alias ca

- Import signed certificates
- $ keytool -import -file client.cert -keystore client.jks -storepass changeme -alias client
- $ keytool -import -file service.cert -keystore service.jks -storepass changeme -alias service

Importing Peer Certificates

- To be able to directly trust the other

- $ keytool -import -file client.cert -keystore service.jks -storepass changeme -alias client
- $ keytool -import -file service.cert -keystore client.jks -storepass changeme -alias service

Now our service and client keystores are ready!