Kubernetes provides the ability for service accounts to authenticate using tokens. It uses a key-pair to provide signatures for those tokens. In this lesson, we will generate a certificate that will be used as that key-pair. After completing this lesson, you will have a certificate ready to be used as a service account key-pair in the form of two files: `service-account-key.pem` and `service-account.pem`.

Here are the commands used in the demo:

```
cd ~/kthw

{

cat > service-account-csr.json << EOF
{
  "CN": "service-accounts",
  "key": {
    "algo": "rsa",
    "size": 2048
  },
  "names": [
    {
      "C": "US",
      "L": "Portland",
      "O": "Kubernetes",
      "OU": "Kubernetes The Hard Way",
      "ST": "Oregon"
    }
  ]
}
EOF

cfssl gencert \
  -ca=ca.pem \
  -ca-key=ca-key.pem \
  -config=ca-config.json \
  -profile=kubernetes \
  service-account-csr.json | cfssljson -bare service-account

}
```