

**PIV**[Introduction](#)**Guides**[Device setup](#)[PIV Walk-Through](#)[SSH with PIV and PKCS11](#)[Securing SSH with OpenPGP or PIV](#)[SSH user certificates](#)[Windows CA issued certificate](#)[Android code signing](#)[Smart card-only authentication on macOS](#)[EJBCA Login with YubiKey](#)**[Generating keys using OpenSSL](#)**[Mac code signing](#)[Tools](#)

## Generating keys using OpenSSL

There are two ways of getting private keys into a YubiKey: You can either generate the keys directly on the YubiKey, or generate them outside of the device, and then importing them into the YubiKey. Reasons for importing keys include wanting to make a backup of a private key (generated keys are non-exportable, for security reasons), or if the private key is provided by an external source. This document will guide you through using the OpenSSL command line tool to generate a key pair which you can then import into a YubiKey. Two different types of keys are supported: RSA and EC (elliptic curve).

When generating a key pair on a PC, you must take care not to expose the private key. Ensure that you only do so on a system you consider to be secure.

### Generating a private RSA key

1. Generate an RSA private key, of size 2048, and output it to a file named `key.pem`:

```
$ openssl genrsa -out key.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
```

```
.....  
e is 65537 (0x10001)
```

2. Extract the public key from the key pair, which can be used in a certificate:

```
$ openssl rsa -in key.pem -outform PEM -pubout -out  
public.pem  
writing RSA key
```

## Generating a private EC key

1. Generate an EC private key, of size 256, and output it to a file named key.pem:

```
$ openssl ecparam -name prime256v1 -genkey -noout -out  
key.pem
```

2. Extract the public key from the key pair, which can be used in a certificate:

```
$ openssl ec -in key.pem -pubout -out public.pem  
read EC key  
writing EC key
```

After running these two commands you end up with two files: key.pem and public.pem. These files are referenced in various other guides on this page when dealing with key import.

---

### DEV.YUBICO

[WebAuthn](#)[OTP](#)[U2F](#)[OATH](#)[PGP](#)[PIV](#)[YubiHSM2](#)[Software Projects](#)

### RESOURCES

[Buy YubiKeys](#)[Blog](#)[Newsletter](#)[Yubico Forum Archive](#)

### YUBICO.COM

[Why Yubico](#)

[About Yubico](#)

[Cookie](#)

[Legal](#)

[Privacy](#)

[Terms of use](#)

[Trust](#)

