# What to do when my Private key and Certificate do not match

## Symptoms

During certificate installation, you are presented with a warning that the private key and the certificate do not match.

## Cause

Somewhere during the requesting of the certificate or generating the CSR and the certificate being delivered your CSR got changed. Such often happens if multiple CSRs are created and people lose track of which one was eventually ordered, or if an old CSR is used that does not belong to the certificate.

## Resolution

Verify that an RSA private key matches the RSA public key in a certificate, you need to

1. verify the consistency of the private key and ;
2. compare the modulus of the public key in the certificate against the modulus of the private key ;

Verify the consistency of the RSA private key and to view its modulus:

```
openssl rsa -modulus -noout -in myserver.key | openssl md5
openssl rsa -check -noout -in myserver.key | openssl md5
```

You shall receive the following:

```
RSA Key is ok
```

If it doesn't say "RSA key OK", it isn't OK!"

To view the modulus of the RSA public key in a certificate use the following terminal command:

```
openssl x509 -modulus -noout -in myserver.crt | openssl md5
```

If the first commands show any errors, or if the modulus of the public key in the certificate and the modulus of the private key do not exactly match, then you're not using the correct private key. You can either create a brand new key and CSR, or you can do a search for any other private keys on the system and see if they match.

To search for all private keys on your server use following:

```
find / -name *.key
```

When installing your certificate you are presented with a warning that the private key and the certificate do not match. This means that somewhere during the requesting of the certificate or generating the CSR and the certificate being delivered your CSR got changed. This often happens when multiple CSRs are created and people lose track of which one was eventually ordered, or if an old CSR is used that does not actually belong to the certificate.

To check if your certificate and private key belong to each other you can use this command line to see how values stack up;

```
openssl rsa -noout -modulus -in privateKey.key | openssl md5
openssl req -noout -modulus -in CSR.csr | openssl md5
openssl x509 -noout -modulus -in certificate.crt | openssl md5
```

From this, you will get MD5 values. If they are all the same, then the files belong to each other.

If you get a mismatch, start a reissue for your certificate using a new CSR and Private key pair.

That also can be done using Openprovider API.

---

Revision #5
Created 2026-08-07 14:59:42 UTC by Sarath
Updated 2026-08-24 10:30:06 UTC by Sarath