

# Misc Tips & Tricks

## CertificateException: Certificates does not conform to algorithm constraints

Java (JCE) is refusing to process a certificate because it violates configured algorithm constraints. This is most likely a certificate using md5WithRSAEncryption that are still quite common.

The algorithm constraints are defined in `java.security` file located somewhere in your JDK installation (e.g. `/etc/java-8-openjdk/security/java.security` for OpenJDK8 on Ubuntu). Change the following lines

```
jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024  
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768
```

to

```
jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024  
jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768
```