Enabling HTTPS using the NCSA CA

Enabling HTTPS in Tomcat with NCSA CA Certificates

Enabling Tomcat Server Side SSL

- Using Built-in Tomcat SSL Support
- Using Globus Tomcat Extensions for Tomcat SSL Support

Enabling Java Client Side SSL Support

If you try to connect to a Tomcat installation configured as one of the above, you will likely receive the following error:

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to
requested target
```

The exception means that the Java client does not trust the CA of the host to which it is trying to connect.

There are two choices:

1. Import the NCSA CA Certificate into your local trusted certs
2. Use a custom HTTPS handler in your Java client.

Further Reading

- http://security.ncsa.uiuc.edu/research/grid-howtos/