SHRINE 4.2.0 Chapter 12 - Configure Tomcat for TLS-based https

TLS https Tomcat Server

Always use encrypted communication for all http connections in SHRINE networks. SHRINE carries login information in http headers. I2b2 carries similar information in http request bodies.

Standard TLS-based https is sufficient for SHRINE.

Setting up SHRINE's Keystore in versions 3.2 and earlier was much more complex. Now SHRINE uses Tomcat's TLS-based https the way almost all other applications do. Tomcat's own documentation is insufficient but these instructions were clear .

TLS Verified https Client

New in SHRINE 4.2 - SHRINE uses TLS server verification by default for all communication between the hub and downstream nodes. Downstream nodes will be unable to communicate with the hub unless the hub is configured to use a certification that the downstream nodes can validate.

SHRINE nodes can also use TLS server verification when communicating with their local i2b2 server. To take advantage of this security feature in your shrine.conf set

```
shrine.pmEndpoint.tls.trustManager = "VerifyServerCerts"
shrine.adapter.crcEndpoint.tls.trustManager = "VerifyServerCerts"
```