Remote Client HTTPS Requirements

Contents of this Page

LexEVS 6.x Installation Links

LexEVS Service Clients to be Able to Consume HTTPS Enabled Services

- All LexEVS 6.4.1 Services will only be available via HTTPS protocols.
  - LexEVS 6.4.1 services will run under SSL protocol level **TLSv1**.
- These services will feature third party approved certificates.
- RMI clients accessing the LexEVS services will need to be updated.

Services Affected:

- LexEVS Remote API
- LexEVS CTS2 Services
- URI Resolver

Impact:

General

All Client references to HTTP URL's should be updated to HTTPS versions

LexEVS Remote API

- LexEVS Remote (Also known as distributed) RMI clients will need to add or replace the following jars to the class path to to support HTTPS updates for 6.4.1
  - lexevs-remote.client.6.4.1.jar
- Combined with updating service URLs to any HTTPS services this should allow processing of valid certificates and failure on self-signed or otherwise invalid certificates by RMI Clients.

CTS2 Service

- Any REST Clients will need to adjust for the HTTPS service as needed.
- Support for REST Clients accessing HTTPS CTS2 services can be had here: https://github.com/cts2/lexevs-service/issues
- REST Clients using the CTS2 Framework client API should already be able to use the SSL services of an HTTPS service.
- Any internal REST Service requests can be forwarded to Bauer, Scott (NIH/NCI) [C] or Unknown User (endlecm)

Other

- The URI Resolver is not considered a public REST API, but it will be switching to HTTPS as well.

Service Related Issues:

LexEVS HTTPS Setup