Tomcat Native 2

Using our own JNI wrapper for OpenSSL in Tomcat and Undertow

Workshop R&D - Red Hat

Supervisors : Jean-Frederic Clere & Rémy Maucherat

Team : Jocelyn Thode & Simon Brulhart

Summary

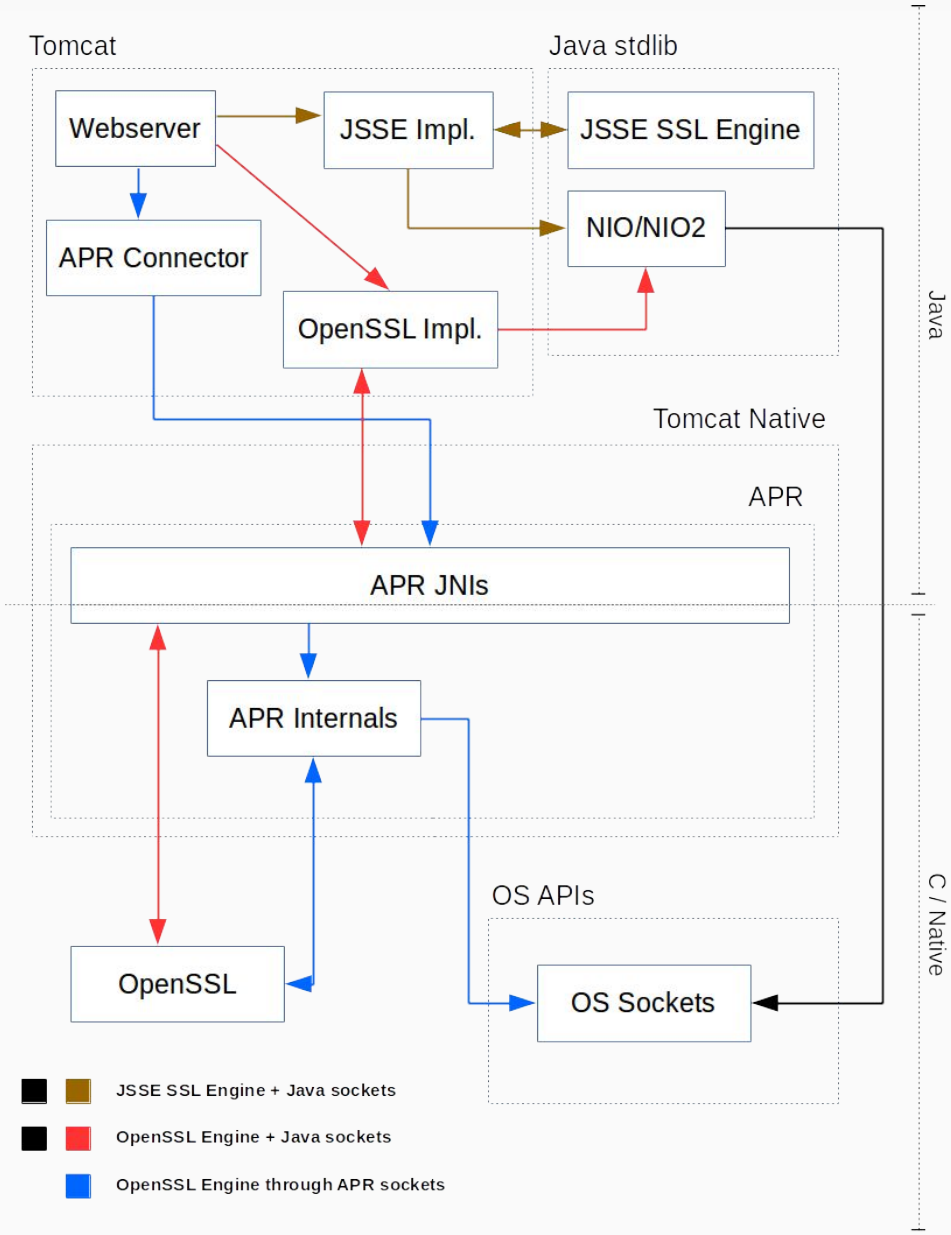
- Overview
- What has been done
- Changes to the Workplan
- What needs to be done
- What may be done

Current State: Tomcat + Tomcat Native

“An optional component for use with Apache Tomcat“

- Better performance and compatibility with OS
- Uses encrypted sockets through Apache Portable Runtime (APR)
- Uses OpenSSL APIs through APR

Current State : Ways to Use SSL



Projected State : Tomcat Native 2

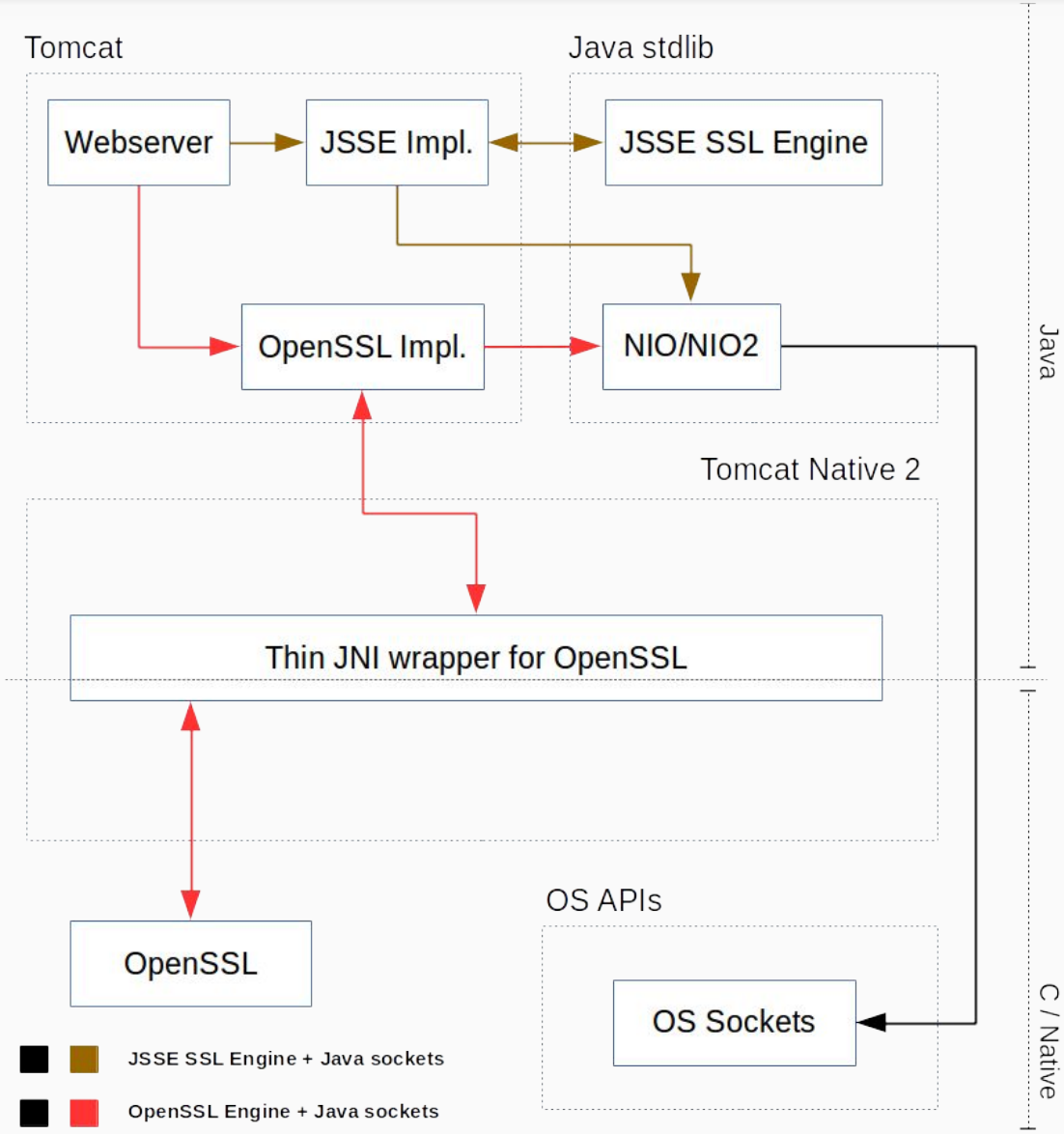
Tomcat + Tomcat Native 2

- Reduces dependencies (no APR)
- Reduces project complexity
- Native/Java bridge with JNI+Homebrewed code

Undertow + Tomcat Native 2

- Brings OpenSSL
- Small dependencies (no APR)
- Native/Java bridge with JNI+SPI

What has been done : APR Removal



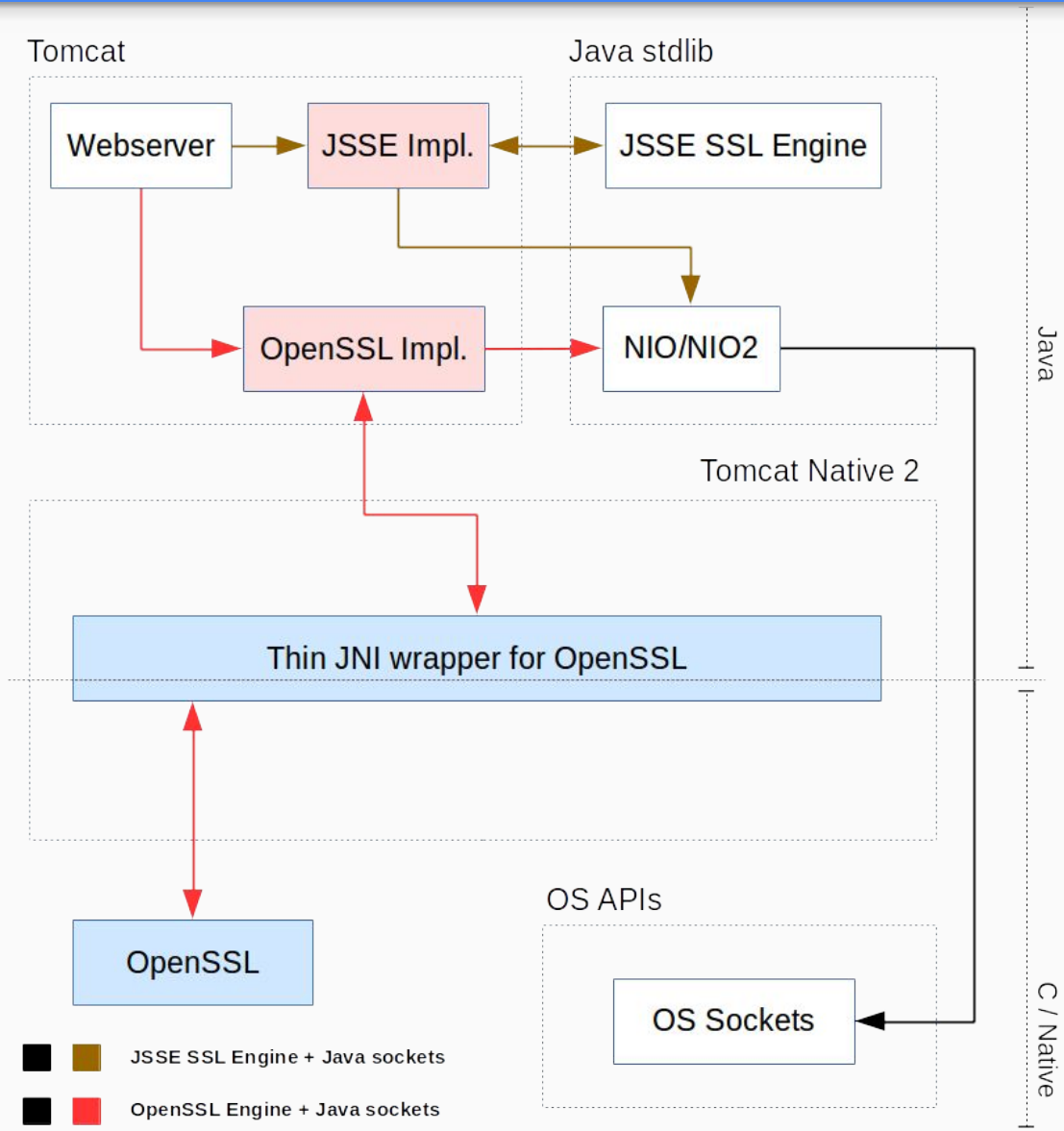
What has been done (2)

- Prototype tested (informally) by Rémy Maucherat
  - No performance regression!
- Experiment with dynamic linking
  - Prior work in Undertow was doing it
  - Not planned beforehand
- Evaluation of the changes needed to port Tomcat Native 2 to Undertow

Changes to the Workplan

- Tomcat-Native now compatible with OpenSSL 1.1
  - Merge upstream changes in Tomcat Native 2 down the road
- Prior work on Undertow used dynamic loading
  - Experiment with dynamic loading in Tomcat Native 2
- OpenSSL classes from Tomcat and Undertow could not be reconciled
  - Different philosophies

What needs to be done (1)



Common code

Forked code

What needs to be done (2)

- Integrate Tomcat Native 2 in Undertow
- Fix ALPN in Tomcat with Tomcat Native 2
  - Required for HTTP/2
  - Re-use code from Stuart's OpenSSL experiment
- Merge changes related to OpenSSL 1.1
- Run benchmarks

What may be done

- Finish prototype using dynamic linking
  - Need to support both OpenSSL 1.0.2 and 1.1.0
  - Could be complicated
- Support for OpenSSL handshake callback
  - Currently using a hack
- Support for large frames
- More support for security options

Questions