Current SSL vulnerabilities

As of October 2014 there are known vulnerabilities in how the Apache webserver (used by OpenAthens LA) handles SSL.

Until such time as a patch is released for Apache by its developers, the workaround is to disable versions 2 and 3 of the SSL protocol. This can be done either on the users' browsers or on the server.

Clientside

Use any modern browser where the version was released in 2015 or later. Do not use old browsers such as IE6.

Serverside

To apply this on OpenAthens LA runtimes:

1. Open ssl config file in editor

```
sudo nano /etc/httpd/conf.d/ssl.conf
```

2. Find the SSL Virtual Host Context section and add the line '`SSLProtocol All -SSLv2 -SSLv3`' in front of it and save. E.g.

```
SSLProtocol All -SSLv2 -SSLv3
##
## SSL Virtual Host Context
##
```

3. Restart Apache

```
sudo service httpd restart
```

Users may take slightly longer to be authenticated whilst Apache is restarted but will otherwise not be affected unless their browser does not support TLS.

Some older browsers such as Internet Explorer 6 will no longer be able to work with OpenAthens LA after this as they do not support TLS.