MatrixSSL 1.8 Open Source Release Notes

This document lists all changes that have been made to the MatrixSSL open source product since the previous 1.7.3 version.

API changes

- Addition of two new server APIs that allow the user to add a custom flag value to client sessions. Servers may now assign custom data to connected sessions that can be later retrieved from a session that was established with a session resumption handshake. See the API documentation for *matrixSslSetResumptionFlag* and *matrixSslGetResumptionFlag* for more details.

Functionality changes

- Ability to put multiple certificates in a single PEM file
- The handshake will now fail on an un-authenticated cert if no user validation callback has been defined with *matrixSslSetCertValidator*. It is still encouraged that a callback be registered.
- Users can now reply to a closure alert with a closure alert of their own using *matrixSslEncodeClosureAlert*. Previously, the SSL_CLOSED flag prevented this. Now only error cases will prevent the closure alert from being created.

Bug fixes

- Numerous compile warnings fixed. Especially in the area of unsigned char / char type mismatches.
- Added explicit ‘void’ types to empty parameter functions.
- Fixed a bad shift operation in cipherSuite.c (no practical functional issue here).
- Fixed possible memory leak of pre-master secret if deleteSession called on some corner failure cases
- Fixed compile and link issues when USE_FILE_SYSTEM was turned off in matrixConfig.h
- Fix for unknown X.509 certificate extension parsing in which the extensions did not provide explicit data lengths in the encoding.
- Fixed parse issue with an empty AuthorityKeyIdentifier certificate extension
- Created new sample certificates with updated dates