MatrixSSL 3.4.2 Open Source Release Notes

1 BUG FIXES AND IMPROVEMENTS

Changes since MatrixSSL 3.4.1

1.1 Improved Run-Time Checks of Certificate Algorithms Against Cipher Suites

Checking the public key and signature algorithms of the certificate material during initialization and cipher suite negotiation is now stricter. Servers now look at the signature algorithm of their certificate when negotiating cipher suites to ensure the authentication mechanism is consistent with the cipher suite. This enables the handshake to fail early in the process if the certificate material does not support a requested cipher suite. This is mainly a protection against user configuration errors because a server should not enable cipher suites it isn't prepared to support. Clients now confirm the server certificate signature algorithm as a pre-emptive measure during the parsing of the CERTIFICATE message. Previous versions would terminate the connection later in the handshake process when the unsupported algorithm was encountered for the public key operation itself.

1.2 SSL Alert Sent on Handshake Message Creation Failure

Previous versions would silently terminate the SSL connection if handshake message creation failed. Now an INTERNAL_ERROR alert is sent before closing the connection.

1.3 Expired Session Resumption Fix

Fixed server support for scenarios in which a session that is already in a resumed handshake state will correctly fall back to a full handshake if the client attempts a resumed re-handshake after the session has expired in the server cache.

1.4 Disable Yarrow by Default and Simplified PRNG Reseeding

The USE_YARROW define is now disabled by default in *cryptoConfig.h* because the two default entropy gathering sources are PRNG sources themselves so it isn't necessary to run that data through Yarrow. This change will result in a minor connection speed improvement. If Yarrow is needed, the logic for reseeding that algorithm has been simplified to update only on the amount of data read rather than including the number of function calls to the PRNG retrieval function.

1.5 Removed the USE_RSA Configuration Define

The open source version of MatrixSSL only supports RSA cipher suites so the removal of that option makes this explicit.

1.6 Example Applications Load Full CA List

To aid in testing, the example client and server applications now load the full list of sample Certificate Authority files so a recompile is not needed if changing the sample certificate material of the peer.