

MatrixSSL 1.8.6 Release Notes

This document highlights the changes from the 1.8.5 open source version of MatrixSSL.

New Features

- The matrixRsaParsePubKey routine has added support for X.509 SubjectPublicKeyInfo formatted keys
- Full parsing support of the subjectAltName extension in certificates

Functional Changes

- Allowing clients to send multiple compression parameters in the CLIENT_HELLO message
- The matrixX509ReadCert routine supports additional PEM file header and footer formats

Minor Fixes

- Corrected filename misspelling in httpsReflector.c for loading the example CAcertCln.der certificate