MatrixSSL 3.1.2 Open Source Release Notes

PeerSec Networks, Inc. 410 Broadway Ave E. #205 Seattle, WA 98102 **T** 425.646.7850 **F** 206.501.4366

support@peersec.com www.peersec.com

Overview

Thank you for choosing MatrixSSL. The 3.1 version is a major revision to the previous releases and enables users to implement strong SSL security into their applications faster than ever. With a design emphasis on further reducing memory usage and providing an easier integration API, MatrixSSL 3.1 is the security solution for virtually any networked application on any platform.

If you are migrating from a previous version of MatrixSSL you will want to read the Migrating To MatrixSSL 3 document to learn more about the specific changes.

Who Is This Document For?

- Software developers that are securing applications with MatrixSSL
- Software developers upgrading to MatrixSSL 3.1.2 from a previous version
- Anyone wanting to learn more about MatrixSSL 3.1

MatrixSSL 3.1.2 Release Notes

This section highlights the differences between version 3.1.1 and 3.1.2

Enhancements to Features and Functionality

Explicit API support for processing multi-record data buffers

The 3.1.1 API set did not include a documented mechanism for processing buffers in which multiple application data records are concatenated in a single 'recv' buffer. This is not an uncommon scenario and users are strongly encouraged to update to this latest MatrixSSL version and implement the new `matrixSslProcessedData` function in their applications. Details can be found in the updated API documentation included in this package.

MatrixSSL version defines added

A *version.h* file has been added that includes defines for the MatrixSSL major, minor, and patch build version. The new header is included by matrixsslApi.h and defines the full version and the individual components. For example:

```
#define MATRIXSSL_VERSION           "3.1.2-OPEN"
#define MATRIXSSL_VERSION_MAJOR     3
#define MATRIXSSL_VERSION_MINOR     1
#define MATRIXSSL_VERSION_PATCH     2
#define MATRIXSSL_VERSION_CODE      "OPEN"
```

The sslTest application includes a timing mode

The sslTest application can now be built to measure the connection speeds for clients and servers for the various cipher suites.

Improvements to HTTP parsing in example application code

The server and client example applications now identify partial and multi-record HTTP records.

Public API Changes

New matrixSslProcessedData prototype and return codes

To support the processing of multi-record data buffers, the `matrixSslProcessedData` function prototype and return codes have changed. The new function has two additional parameters that are used to return the next decoded record in the buffer. The return codes for this function have been expanded to inform the user how that second record should be handled.

Please see the API documentation and code examples for detailed information.

Bug Fixes

Fixed return codes where unsigned data types were assigned negative values

The functions `psRsaDecryptPriv`, `psRsaDecryptPub`, and `matrixSslDecode` are now consistent in their use of unsigned vs. signed data types.

Support and Bug Reporting

Known Issues

None

Contacting Support or Reporting Bugs

Email support@peersec.com