MatrixSSL 3.1.3 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 2.x 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 3.1.3 from a previous version
- Anyone wanting to learn more about MatrixSSL 3.1

MatrixSSL 3.1.3 Release Notes

This section highlights the differences between version 3.1.2 and 3.1.3

Enhancements to Features and Functionality

New server-side configuration option to decrease binary executable size

Servers may now disable a new `USE_CERT_PARSE` define in *crytpoConfig.h* to exclude a relatively large portion of the *x509.c* source code.

Previous versions of MatrixSSL would always pass the server certificate through an X.509 parse phase during initialization. This allowed the library to confirm the format of the certificate and perform algorithm tests based on the chosen cipher suite. However, these tests were in place primarily to prevent user error so if `USE_CERT_PARSE` is disabled, the user must be confident the certificate material is valid for the cipher suites that have been enabled in *matrixsslConfig.h*

New Pseudo-Random Number Generation algorithms

An implementation of Yarrow is now included in the MatrixSSL source code package. Random numbers are now retrieved through Yarrow by default. An entropy source and implementation of `psGetEntropy` is still required for each platform.

Windows project files updated to Microsoft Visual C++ 2010 Express

Previous versions used the 2008 Express Edition of Visual C++

Public API Changes

New members in x509DNattributes_t structure

The Distinguished Name attributes in X.509 certificates such as Common Name, Organization, and Country are now accompanied by the explicit ASN.1 data type and length. Previous versions of MatrixSSL attempted to treat these fields as NULL terminated strings using single byte characters. In order to support a larger variety of certificate formats the Type and Len fields have been added so the user will have all the needed information to interpret certificate information that is passed into the certificate callback routine.

New x509DNattributes_t members.

```
short   countryType;
short   countryLen;
short   stateType;
short   stateLen;
short   localityType;
short   localityLen;
short   organizationType;
short   organizationLen;
short   orgUnitType;
short   orgUnitLen;
short   commonNameType;
short   commonNameLen;
```

Type members will be one of the following:

```
ASN_PRINTABLESTRING
ASN_UTF8STRING
ASN_IA5STRING
ASN_T61STRING
ASN_BMPSTRING
```

Bug Fixes

Error return code fixed for matrixSslReceivedData

One code path through `matrixSslReceivedData` was performing an 'unsigned char' typecast on a potentially negative return code which converted it to a positive value. This resulted in an undocumented and ambiguous return code. The typecast has been removed and all error cases now return negative values as documented.

Support and Bug Reporting

Contacting Support or Reporting Bugs

Email support@peersec.com