RTI TLS Support

Release Notes

Version 5.3.0

Printed in U.S.A. First printing.
June 2017.

Trademarks

Copy and Use Restrictions

Technical Support

Real-Time Innovations, Inc.
232 E. Java Drive
Sunnyvale, CA 94089
Phone: (408) 990-7444
Email: support@rti.com
Website: https://support.rti.com/

Contents

TLS Support Release Notes

1 Supported Platforms

TLS Support is available for the platforms in the following table.

Table 1.1 Supported Platforms

Operating System	Version
Android™	All platforms in the *RTI® Connext® DDS Platform Notes* for the same version number, except not supported on SUSE® 11 or any custom target platform.
iOS®	
Linux®	
OS X®	
QNX®	QNX Neutrino® 6.5 SP1 on ARMv7 (armv7aQNX6.5.0SP1qcc_cpp4.4.2) QNX Neutrino 6.5 on x86 (i86QNX6.5qcc_gpp4.4.2) QNX Neutrino 6.6 on ARMv7 custom target platform (armv7aQNX6.6.0qcc_cpp4.7.3) QNX Neutrino 6.6 on x86 custom target platform (i86QNX6.6qcc_cpp4.7.3)
Windows®	All platforms in the *RTI Connext DDS Platform Notes* for the same version number.

For details on these platforms, see the *RTI Connext DDS Platform Notes*:

2 Compatibility with Current Software

RTI TLS Support is designed for use with the TCP transport that is included with RTI Connext DDS. If you choose to use TLS Support, it must be installed on top of an existing TLS Support installation with the same version number. It can only be used on architectures that support the TCP transport (see the *RTI Core Libraries Platform Notes*).

RTI TLS Support5.3.0 is compatible with OpenSSL 1.02j.

3 Backward Compatibility

If you are upgrading from OpenSSL 1.0.1 to OpenSSL 1.0.2 or above: The number of bits of any Diffie-Hellman (DH) parameters must now be at least 1024 (see https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/). Therefore, if you are using the property **tls.cipher.dh_param_files** and there is a DH parameter file that has fewer than 1024 bits, you must regenerate the file with at least 1024 bits.

4 What's New in 5.3.0

4.1 New Platforms

This release adds support for platforms on the following operating systems:

- OS X 10.12
- Red Hat Enterprise Linux 6.8
- Ubuntu 16.04 LTS
- Windows Server 2016

For details on these platforms, see the *RTI Connext DDS Platform Notes.*

4.2 Platforms on Legacy Operating Systems

The following legacy operating systems have reached end-of-life from their corresponding vendors. Please contact RTI support or your account manager if you require version 5.3 to run on these platforms:

- CentOS 5.x
- Red Hat Enterprise Linux 5.x

4.3 Removed Platforms

Platforms on the following operating systems are no longer supported:

- OS X 10.8
- Red Hat Enterprise Linux 4
- Windows Vista, Windows XP Pro, Windows 2003

5 Third-Party Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).