INSIDE SECURE TLS TOOLKIT 4.0

A complete and compact TLS implementation supporting TLS 1.3

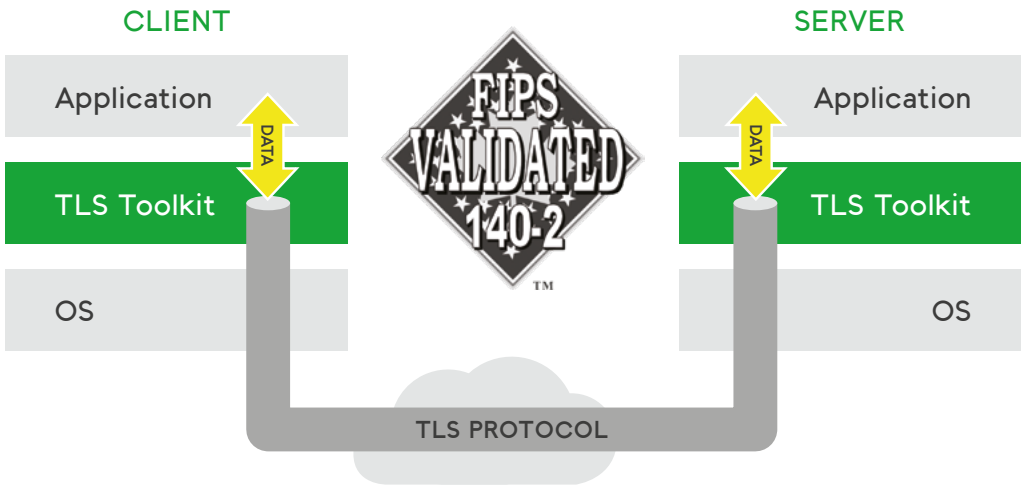
Key features

- Full support of the latest TLS specifications and features
- Available with FIPS 140-2 validated Inside Secure Crypto Module
- Standards compliant proven interoperability
- Portable on any platform
- Better alternative to OpenSSL and RSA BSAFE
- Small footprint and optimized performance for IoT devices
- Delivered in clear, readable, cross-platform and well documented C source code

TLS is everywhere

The use of the TLS protocol has increased dramatically over the last few years. More than **80%** of all web traffic is TLS protected. For APIs exposed from the Cloud the percentage is even higher. TLS protocol is used everywhere, not only in the web and cloud but also in IoT devices and even between different components of a single device.

To enable TLS in your product Inside Secure provides a **complete toolkit** that contains a compact implementation of the TLS protocol for both clients and servers.



Inside Secure TLS Toolkit

Inside Secure TLS Toolkit (formerly known as MatrixSSL) is a **TLS protocol implementation in C language with minimalistic system dependencies** making it easily portable on any platform. Inside's TLS Toolkit powers millions of products ranging from embedded devices with very limited capabilities to high-end network equipment.

Thanks to a clear and well documented source code integration is faster and smoother than alternatives. To further simplify and accelerate the integration, Inside Secure offers developer level support.

Inside's TLS Toolkit has always been quick to adopt the latest TLS specifications. For example, support for the TLS 1.3 protocol was released in August 2018, within days of IETF publishing the RFC 8446 specification.

Inside's standard offering **can be configured to a minimal code footprint of 66 kB (PSK)**. Manual optimization can further reduce the code footprint to meet the needs of memory constrained devices.

For applications that require FIPS validation, Inside'sTLS Toolkit is also offered with a state-of-the-art **FIPS 140-2** validated crypto module*, successfully used in hundreds of millions devices.

For applications switching from OpenSSL a compatibility layer is provided to smoothen and accelerate migration to Inside's TLS Toolkit.

* FIPS certificate #2389

FULL SUPPORT OF TLS SPECIFICATIONS

TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3

DTLS 1.0, DTLS 1.2

TLS 1.3 KEY FEATURES

0-RTT (zero round-trip time mode)

OCSP stapling

Ciphersuites

- AES 128/256 GCM with SHA256/384
- CHACHA20 POLY1305 with SHA256

Key exchange modes

- DHE (ffdhe2048, ffdhe3072, ffdhe4096 groups)
- ECDHE (P-256, P-384, P-521, Curve 25519)
- PSK and PSK with DHE and ECDHE

Signature algorithms

- ECDSA (P-256, P-384, P-521 groups)
- Ed25519
- RSASSA-PSS, RSA PKCS#1.5 (certificates only)

For further details on all of Inside's security solutions, visit www.insidesecure.com

inside secure