wolfSSL vs. OpenSSL

Why choose us?

Description

Many people are curious how wolfSSL compares to OpenSSL and what benefits there are to using an SSL library that has been optimized to run on embedded platforms. We believe that wolfSSL will provide you with more flexibility, an easier integration of SSL/TLS into your existing platform, current standards support, and much more – all provided under a very easy-to-use license model.

The points below outline several of the main differences between wolfSSL and OpenSSL.

Size

With a 20-100kB build size and runtime memory usage between 1-36kB, wolfSSL is up to 20 times smaller than OpenSSL. In an embedded environment where footprint size is critical or a large cloud environment where memory usage per connection makes a big impact on the performance and success of a project, wolfSSL is an optimal TLS and cryptography solution.

Standards Support

wolfSSL is up-to-date with the most recent standards: TLS 1.2 and DTLS 1.2. With the vulnerabilities in SSL 3.0 and TLS 1.0, or the recent timing attack in block cipher mode TLS, your project should use TLS 1.2 with ephemeral keys and AEAD ciphers for maximum security. wolfSSL fully supports modern security on the client and server. As we have with previous TLS standards, we will continue to lead the way with TLS 1.3. wolfSSL supports all relevant IoT specifiations including Apple™ HomeKit™.

Progressive Ciphers & Hardware Crypto

wolfSSL is progressive with support for new secure and high-performance ciphers. wolfSSL includes some of the most current ciphers like ChaCha20, Poly1305, Blake2b, curve25519, and ed25519. We have hardware acceleration support for a vast list of platforms. Contact us for more detail.

Company

wolfSSL is backed by an outstanding group of security professionals who care about users, security, and quality. The wolfSSL team is based in Bozeman, Portland, and Seattle.

Ease of Use

OpenSSL is burdened with legacy code that must be maintained and kept up to date. wolfSSL was designed from the beginning with developers in mind. Written from scratch, wolfSSL has a simple and well documented API, easy-to-use abstraction layers, IDE integration, and clear usage examples.

Portable

wolfSSL is the leading TLS library by virtue of its breadth of platform support and successful implementations. With our long list of supported platforms, your time to market is dramatically decreased, out of the box. OpenSSL requires porting to many platforms, which will cost your team time and money.

License

wolfSSL is dual licensed under the GPLv2 or commercial terms, where OpenSSL is available only under their unique license from multiple intellectual property sources. All wolfSSL code is devloped by our staff under strict source code and intellectual property control.

Support

The original authors of OpenSSL are no longer involved in the project. wolfSSL was written from the ground up and is actively developed by our original authors. We are available by phone, email, or the support forums to answer your questions quickly and accurately. Making quick progress on adding security to your product is easier than ever.

Learn More

For more information about wolfSSL, how it compares to OpenSSL, or joining our community please contact us at info@wolfssl.com, or visit our website wolfssl.com.