NicheStack™ SSL

Management & communication Security

NicheStack SSL is a robust software toolkit supporting networked device developers who have a need to add secure communication and secure web management to their designs. SSL and TLS (Transport Layer Security) the IETF-standardized successor to the SSL protocol reside at the transport layer, effectively being "plugged" between the Web server/browser or other application and the TCP/IP stack. As a result, they also have the potential to protect secure tunnels for other TCP services such as FTP, SMTP, and telnet or be the basis for secure custom applications. The support for secure socket level communications provided by NicheStack SSL gives the device developer the capability to address the three essential issues of network security:

- Data Confidentiality - protection of data against disclosure or use by unauthorized users or processes.
- Content Integrity - protects data from intentional and accidental change by ensuring that changes are detectable.
- Authentication - verifies the identity that is "claimed" by a user or device.

Supporting SSL2.0, SSL3.0, TLS1.0 and both blocking and non-blocking sockets, NicheStack SSL is based on public key asymmetric cryptography, by which the sender uses a public key to encrypt a message, but only the owner of the private key will be able to decrypt it. NicheStack SSL uses RSA key exchange method (RSA public key) with 1024 bit key generation and Triple DES encryption, and offers both Client and Server modes of operation.

The architecture of the NicheStack SSL product supports an industry standard SSL suite, yet provides easy integration with NicheStack™ TCP/IP products on a wide range of hardware and operating systems

NicheStack SSL Highlights

- High-performance implementation supports SSL2.0, SSL3.0, TLS1.0
- Client and Server operations supported
- 1024 bit key and Triple DES encryption
- RSA and Diffie-Hellman key exchange
- RC4 (128 bit) and Triple-DES (168 bit)
- cipher keys
- MD5 (128 bit hash) and SHA-1 (160 bit hash) Message Digests
- Leverages InterNiche CryptoEngine technology

The Specialist Provider of Software and Expertise for Device Networking

InterNiche Technologies, Inc.
51 E Campbell Ave, Suite 160
Campbell, CA 95008
USA
www.iniche.com
Phone: +1 408 540 1160
Fax: +1 408 540 1161
Email: sales@iniche.com
Europe: +31 24 373 7962
sales-europe@iniche.com

interniche
technologies, inc.

The Specialist Provider of Software and Expertise for Device Networking

platforms. As with all InterNiche products, the implementations are specifically optimized for networked devices with constrained resources.
Although the implementation is based on a number of open source technologies, a significant number of improvements have been made to complete a commercial quality embedded offering, including structural optimization, reduction in OS dependencies and communalization of support functions.

InterNiche has architected a common CryptoEngine security subsystem for its security protocol products and the NicheStack SSL product takes full advantage of this optimization. CryptoEngine reduces overall cryptography library memory and run-time overhead, and offers a choice of optimized software implementations of required algorithms with an easy integration approach with available HW encryption engines on specific platforms. Such HW engines significantly lower the overhead of secure communication, especially on lower power CPUs and are especially recommended for applications with higher throughput requirements.

Key Technical Specs

- RFC2246 The TLS Protocol
- RFC 2402 - IP Authentication Header
- RFC 2405 - ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2401 - Security Architecture for the Internet Protocol
- RFC 2406 - Encapsulating Security Payload (ESP)
- RFC 2451 - ESP CBC-Mode Cipher Algorithms
- RFC 2104 - HMAC: Keyed-Hashing for Message Authentication
- RFC 2403 - Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 - Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2410 - NULL Encryption Algorithm

InterNiche Device Networking Products

InterNiche is the premier **specialist provider** of internet protocol software stacks and networking expertise that are specifically targeted at connected device implementations. InterNiche offers a broad range of TCP/IP protocol suites, **optimized** for maximum performance and minimum memory footprint on the highly integrated VLSI at the heart of today's device designs.

All InterNiche device networking products are engineered for **rapid, seamless integration** with best-in-class development environments for the leading VLSI architectures. The combination of rapid integration and low overhead specifically addresses the challenges faced by device development teams by offering **maximum networking performance** and manageability within a low cost system implementation.

InterNiche provides a tasking API that is adaptable to almost any RTOS environment, so that the development team can easily interface to the necessary functions and incur **no additional overhead**. Throughput is maximized through effective usage of zero-copy buffers and availability of assembler optimizations for critical code sections.

A **modular approach** to the entire suite of protocol products maintains a development team's capability to profile stack features to match specific device requirements. With **configuration flexibility** and the tools to identify and eliminate integration problems development teams find that system integration using InterNiche products is **smooth and predictable**.

InterNiche products are supplied as **portable ANSI C** source code packages under **royalty-free** license terms. All products include full technical documentation and a first 12 months of **highly responsive support** service, which includes access to technical experts via email, web, Fax, and telephone.

InterNiche Technologies, Inc.
Phone: +1 408 540 1160
Fax: +1 408 540 1161
Email: sales@iniche.com
Europe: +31 24 373 7962
sales-europe@iniche.com

51 E Campbell Ave, Suite 160
Campbell, CA 95008
USA
www.iniche.com

Apr-05