EMBEDDED
SECURITY SOLUTIONS

Matrix SSL™ Toolkit

Mobile Optimized Highly Configurable FIPS Application Security

→ Key features

- SSL Server
- SSL Client
- TLS 1.2
- Cryptography Suite
- Extensible Cryptography Layer
- Protocol Filter Interface
- In-memory API
- Static memory Management
- FIPS 140-2 Level 1 Validated Cryptography Module
- Suite B Cryptography
- Crypto and PKI
- Memory Management
- OS Abstraction layer

Security for mobile and the internet of things

As the use of mobile devices and the 'internet of things ' (IoT) is exploding with millions of IP-enabled devices ranging from military to medical equipment ; smart grids to home applicances to vending machines new security challenges arise. Protecting the integrity and privacy of data across the open internet is critical to the ongoing expansion of mobile applications, the emerging IoT and is often times a requlatory requirement. Secure Sockets Layer (SSL) and the next generation Transport Layer Security (TLS) are the most widely deployed protocols for creating secure connections between applications on a network. SSL is used to secure proprietary applications as well as common Internet protocols.

Given it's broad applicablity application developers and manufacturers serving a range of industries are looking for ways to embed SSL/TLS in their products to meet the growing demand for security.

Meeting the challenges of embedded applications and devices

Embedding SSL security becomes more complex on non-tradiional compute platform such mobile devices, medical equipment, industrial sensors, smart grid devices, and thermostats, as memory and power are at a premium when it comes to small foot print applications. MatrixSSL is an embedded SSL/TLS library under 50 KB., designed for small footprint applications and devices. MatrixSSL has minimal flash memory and RAM requirements which increases resources avaible for value-add funcitonality. It ensures secure connectivity to web services and supports simulateneous active SSL connections Along with fast download times for applications with integrated security.

Easy to integrate for quicker time to market

MatrixSSL™ is shipped in clean source code which is easily integrated, and supported. Under 500KB of code gives bugs fewer places to hide. With a simple, easy to use API that is fully configurable and easy to compile from 35KB baseline with client or server and a single cipher to full specification support at under 100KB. Pluggable cipher suites allow easy customization to meet specific requirements. No cryptographic expertise is required and INSIDE provides full integration and maintenance support.

Works on any platform

Included C source code is portable to ANY platform to add network security. Inside Technology enables full protocol support without file system, memory allocation or multi-thread support. Even "bare metal" platforms with no Operating System are supported. Open, auditable and compatible with larger implementations and the SSL RFC. All web browsers and servers can communicate securely with MatrixSSL.

FreeRTOS VxWorks

driving trust™ inside SECURE

www.insidesecure.com

Meets the needs of most rigid security requirements –FIPS, Suite B and STIG

MatrixSSL™ SDK uses the FIPS certified SafeZone crypto library is NSA Suite B complaint and offers security in line with the Security Technical Implementation Guides (STIGs) authored by the U.S. Department of Defense's Defense Information Systems Agency. Implementation of this technical guidance provides risk assurance to meet the standards prescribed under the National Institute of Standards and Technology's (NIST) authority and to meet the requirements of the Federal Information Security Management Act (FISMA). Besides being utilized in the U.S. Government, the DISA STIG has been adopted for use in the corporate business sector.

→ Who Needs FIPS 140-2 Crypto?

An increasing number of industries ranging from banking to utilities to transportation are now considered critical infrastructure vital to national security. These industries are prime targets of cyber attacks and many are directed to secure communications inline with government standards

- All U.S. government agencies protecting data designated as "Sensitive but unclassified"
- All Canadian government agencies protecting data designated as "Protected information"
- Civilian companies that contract with U.S., Canadian or U.K. federal government organizations requiring FIPS 140-2 encryption
- The U.K. Communications-Electronics Security Group recommends FIPS 140-2 compliant modules, as do many other organizations across Europe and Asia
- Organizations requiring strong encryption including: Financial services, Healthcare, and Educational institutions have chosen the FIPS-140 standard for their crypto security needs
- Wireless carriers serving the Government and Enterprise markets.

Product specifications

Network Protocols SSLv3, TLS 1.0, TLS 1.1, TLS 1.2	**Binary Code Footprint** 42 KB (minimum), 58 KB (standard)	**Compatible Web Clients** All, including Firefox, IE, Chrome, Opera, Safari
Protocol Features Fast session resumption, renegotiation, client authentication, ephemeral keying, pre-shared keys	**Dynamic memory Footprint** 4KB per active session 10KB during key negotiation Zero buffer copy API	**Compatible Web Servers** All, including Apache, IIS, MbedThis AppWeb, GoAhead Webs
Security Algorithms Supported RSA, ECC, DH-Anon, DH-E, AES, 3DES, SEED, ARC4, SHA-1, SHA-256, MDS, MD2, RC2, HMAC, FORTUNA	**Platforms** 32 bit, 64 bit, 16 bit and 8 bit CPUs Assembly language optimizations for ARM, MIPS, PPC and x86	**Operating Systems Supported** All, including VxWorks, embedded Linux, eCos, FreeRTOS, WindowsCE, Mac OSX, iPhone, Android, Palm, BREW
Key Formats Supported PKCS#1.5, PKCS#5, PKCS#8, PKCS#12, PCKS#11	**Authentication Mechanisms** X.509 client and server mutual authentication	**Hardware Encryption** Asynchronous hardware encryption from multiple vendors
Government certified for worldwide export	**Download Source Code Evaluation www.peersec.com**	**FIPS 140-2 Level 1 cryptography library available**

MatrixSSL key features

SSL Server	Accept connections from standard SSL clients for secure web management through HTTPS. Secure existing server protocols through SSL filter interface.
SSL Client	Connect to and authenticate standard SSL servers, including all secure sites on the net. Secure existing client protocols such as software update and Web services clients.
TLS 1.2	Transport layer Security support for client and server provides the most up-to-date network security standards for HTTPS, EAP-TLS and START TLS protocols.
Cryptography Suite	Full cryptography layer including RSA, ECC, AES-128, AES-256, 3DES, SEED, ARC4, RC2, SHA-1, SHA-256, MDS, Fortuna and HMAC, Anonymous, PSK, RSA, Diffie-Hellman and ephemeral key exchange. Key and certificate generation.
Extensible Cryptography Layer	Additional hardware and software cryptography engines are available for MatrixSSL to leverage hardware and platform specific optimizations.
Protocol Filter Interface	Easily integrated into existing applications and protocols via the protocol filter interface. Simply pass incoming or outgoing data through the MatrixSSL interface and continue processing as usual. Support for zero-buffer-copy.
In-memory API	Transport-layer agnostic implementation allows use of network security protocols on POSIX sockets, kernel level sockets, and packet networks such as Wi-Fi. No rewrite or re-turning of network code is required to secure existing protocols.
Static memory Management	MatrixSSL one dynamic buffer for connection for deterministic memory usage, no memory fragmentation, zero memory leaks and protection against buffer overruns.
FIPS 140-2 Level 1 Validated Cryptography Module	Available FIPS 140-2 Level 1 validate cryptography module. FIPS 140-2 Level 1 is the highest certification available for a software module.
Suite B Cryptography	MatrixSSL supports the Suite B set of cryptographic techniques standardized by the National Security Agency as part of its Cryptographic Modernization Program.

MatrixSSL key features

<table>
<tr><th colspan="3">Full development integration support for your application and platform</th></tr>
<tr><td rowspan="2">MatrixSSH
secure command Line
server and Library</td><td colspan="2">User Applications
Web server, VoIP, VPN, Web services</td></tr>
<tr><td>MatrixSSL
Transport layer Security
Key and certificate generation</td><td>MatrixDTLS
UDP Datagram Security
library</td></tr>
<tr><td colspan="3">Crypto and PKI
RSA, AES, 3DES, ARC4, RC2 ciphers. SHA-256, SHA-1, MD5, MD2 hashes. PEM, DER, X.509 parsing</td></tr>
<tr><td colspan="3">Memory Management
Deterministic memory allocation within a single static buffer. No memory leaks</td></tr>
<tr><td colspan="3">OS Abstraction layer
OS no required. Endian Neutral, File system optional. Memory Management optional. Multi-threading optional</td></tr>
<tr><td colspan="3">Operating System
Ports to VxWorks, embedded Linux, eCos, FreeRTOS, Windows CE, Mac OS X, iPhone, Android, palm, BREW</td></tr>
</table>

Supported Cipher Suites

- SSL_NULL_WITH_NULL_NULL
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TSL_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- TLS_DH_anon_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_SEED_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_DHE_ PSK_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256TLS1.2
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA384
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384TLS1.2
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256TLS1.2
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384TLS1.2
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384TLS1.2
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384TLS1.2
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256TLS1.2
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384TLS1.2
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256TLS1.2
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384TLS1.2
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384TLS1.2
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384TLS1.2
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256TLS1.2
- TLS_RSA_WITH_AES_128_CBC_SHA256TLS1.2
- TLS_RSA_WITH_AES_256_CBC_SHA256TLS1.2
- TLS_RSA_WITH_AES_128_GCM_SHA256TLS1.2
- TLS_RSA_WITH_AES_256_GCM_SHA384TLS1.2
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_RSA_WITH_NULL_SHA

0613 - Document non contractuel - zaostratecrea.com