

# MatrixSSL™

## WORKS ON ANY PLATFORM

Included C source code is portable to ANY platform to add network security. AuthenTec Technology enables full protocol support without filesystem, memory allocation or multi-thread support. Even “bare metal” platforms with no Operating System are supported.

## OPEN AND AUDITABLE

Compatible with larger implementations and the SSL RFC. All web browsers and servers can communicate securely with MatrixSSL.

Core security code is freely downloadable and full source is available for commercial evaluation.

## FULLY CONFIGURABLE

Compile in features 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.

## SUPPORTED CIPHER SUITES

- SSL\_NULL\_WITH\_NULL\_NULL
- SSL\_RSA\_WITH\_NULL\_MD5
- SSL\_RSA\_WITH\_NULL\_SHA
- 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\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_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\_128\_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

## Enterprise Level Security for Devices™

**MatrixSSL™** is an embedded SSL/TLS library under 50KB, designed for small footprint applications and devices. 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 such as HTTP, SIP, H.323 and EAP-TLS.

### MatrixSSL Benefits

- Minimal flash memory and RAM requirements
- Increases resources available for value-add functionality
- Connect securely to Web Services
- More simultaneous active SSL connections on enterprise systems
- Faster failover times for High Availability servers
- Secure payments and financial transactions from devices
- Fast download times for applications with integrated security
- Clean source code, easily integrated, and supported
- Under 50KB of code gives bugs fewer places to hide
- Source code evaluation download
- Full integration and maintenance support
- Simple, easy to use API

## PRODUCT SPECIFICATIONS

<b>Network Protocols</b> SSLv3, TLS 1.0, TLS 1.1, TLS 1.2	<b>Binary Code Footprint</b> 42KB (minimum), 58KB (standard)	<b>Compatible Web Clients</b> All, including Firefox, IE, Chrome, Opera, Safari
<b>Protocol Features</b> Fast session resumption, renegotiation, client authentication, ephemeral keying, pre-shared keys	<b>Dynamic Memory Footprint</b> 4KB per active session 10KB during key negotiation Zero buffer copy API	<b>Compatible Web Servers</b> All, including Apache, IIS, MbedThis AppWeb, GoAhead Webs
<b>Security Algorithms Supported</b> RSA, ECC, DH-Anon, DH-E, AES, 3DES, SEED, ARC4, SHA-1, SHA-256, MD5, MD2, RC2, HMAC, FORTUNA	<b>Platforms</b> 32 bit, 64 bit, 16 bit and 8 bit CPUs Assembly language optimizations for ARM, MIPS, PPC and x86	<b>Operating Systems Supported</b> All, including VxWorks, embedded Linux, eCos, FreeRTOS, WindowsCE, Mac OS X, iPhone, Android, Palm, BREW
<b>Key Formats Supported</b> PKCS#1.5, PKCS#5, PKCS#8, PKCS#12	<b>Authentication Mechanisms</b> X.509 client and server mutual authentication.	<b>Hardware Encryption</b> Asynchronous hardware encryption from multiple vendors
<b>Government certified for worldwide export</b>	Download Source Code Evaluation <a href="http://www.peersec.com">www.peersec.com</a> or <a href="http://www.authentec.com">www.authentec.com</a>	

## MATRIXSSL KEY FEATURES AND BENEFITS

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 STARTTLS protocols.
Cryptography Suite	Full cryptography layer including RSA, ECC, AES-128, AES-256, 3DES, SEED, ARC4, RC2, SHA-1, SHA-256, MD5, 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-tuning of network code is required to secure existing protocols.
Static Memory Management	MatrixSSL one dynamic buffer per connection for deterministic memory usage, no memory fragmentation, zero memory leaks and protection against buffer overruns.

## PRODUCT SPECIFICATIONS

<b>Rapid Development Support</b>			
Full development integration support for your application and platform.			
<b>MatrixSSH</b> Secure Command Line Server and Library	<b>MatrixWiFi</b> WPA Supplicant EAP-TLS support	<b>User Applications</b> Web server, VoIP, VPN, Web services	
		<b>MatrixSSL</b> Transport Layer Security Key and Certificate Generation	<b>MatrixDTLS</b> UDP Datagram Security Library
<b>Crypto and MatrixPKI</b>			
RSA, AES, 3DES, SEED, ARC4, RC2 ciphers. SHA-256, SHA-1, MD5, MD2 hashes. PEM, DER, X.509 parsing.			
<b>Memory Management</b>			
Deterministic memory allocation within a single static buffer. No memory leaks.			
<b>OS Abstraction Layer</b>			
OS not required. Endian Neutral. Filesystem optional. Memory Management optional. Multi-threading optional.			
<b>Operating System</b>			
Ports to VxWorks, embedded Linux, eCos, FreeRTOS, WindowsCE, Mac OS X, iPhone, Android, Palm, BREW			