

MatrixSSH™

WORKS ON ANY PLATFORM

Included C source code is portable to ANY platform, even platforms without a Command Line Interpreter (CLI). Server code does not use fork(), memory allocation or a filesystem. Even “bare metal” platforms with no Operating System are supported.

COMPATIBLE AND AUDITABLE

With larger implementations and standard SSH 2.0 terminal clients. Private key and password authentication fully supported. Core security code is freely downloadable and full source is available for commercial evaluation.

FULLY CONFIGURABLE

SSH server support adds only 70KB to binary size when using AuthenTec Core Technology and MatrixPKI, or in conjunction with MatrixSSL. Pluggable cipher suites allow easy customization to meet specific requirements.

SUPPORTED CIPHER SUITES

- AES128-CTR, • AES256-CTR, • AES128-CBC, • AES256-CBC, • 3DES-CBC

Enterprise Level Security for Devices™

MatrixSSH™ is an embedded SSH server and library under 70KB, designed for embedded device management. Secure Shell (SSH) is ideal for providing a secure command line for configuring and administering remote devices.

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

Network Protocols SSH 2.0	Binary Code Footprint 70KB	Compatible SSH Clients All, including OpenSSH, PuTTY
Protocol Features Fast session resumption, renegotiation, client authentication, ephemeral keying, pre-shared keys	Dynamic Memory Footprint 5KB per active session 12KB during key negotiation Zero buffer copy API	Platforms 32 bit, 64 bit and 16 bit CPUs Assembly language optimizations for ARM, MIPS, PPC and x86
Security Algorithms Supported RSA, Diffie-Hellman, AES, 3DES, SHA-1, MD5	Government certified for worldwide export	Operating Systems Supported All, including VxWorks, embedded Linux, eCos, FreeRTOS, ThreadX, Mac OS X, iPhone, Android
Authentication Mechanisms Authorized RSA keys and/or passwords.	Download Source Code Evaluation www.peersec.com or www.authentec.com	

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	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	MatrixSSH shares the same underlying cryptography engine used by MatrixSSL, resulting in code size savings.
Extensible Cryptography Layer	Additional hardware and software cryptography engines can be plugged in to MatrixSSH 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 MatrixSSH interface and continue processing as usual.
In-Memory API	Transport-layer agnostic implementation allows use of network security protocols on POSIX sockets, kernel level sockets, and serial connections. 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

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