Smart Software Solutions
for Embedded Success

SSL

Secure Sockets Layer

Features

- Developed for embedded systems
- SSLv2, SSLv3 support
- Transport Layer Security (TLS) v1, v1.1 and v1.2 support
- Anonymous Diffie Hillman support
- Processor independent
- RTOS independent
- Highly configurable
- Includes verification tools
- Comprehensive documentation

Applications

- Point of Sale terminals
- Merchant terminals
- Transaction processing
- File transfer
- Data collection

EBSnet's SSL offers 'industrial strength' authentication and encryption for embedded communication and application devices. EBSnet's SSL adds security to any TCP based communication protocol by authenticating users and encrypting sensitive data.

FUNCTIONALITY HIGHLIGHTS:

EBSnet's SSL package provides a set of tools to test client/server communications and test encryption/decryption speed. We have included a sample CLISRV/SSL application allowing device developers to verify all of these operations on their embedded system.

Highly Configurable:

- Flexible Cipher Support
- Variable Digests
- Developer Defined Certificates
- Hashing Algorithm

Add security to any TCP based protocol:

- FTP
- Telnet
- Web Server
- Web Browser

Digests supported :

MD2, MD4, MD5, SHA-1, SHA-2 (SHA-256, SHA-512), RIPEMD-160

Ciphers supported:

AES(CBC, CTR, GCM), DES, 3DES, ARC4, RABBIT, HC-128,
RSA, DSS, Diffie-Hellman, EDH, NTRU
HMAC, PBKDF2, PKCS#5

ECC cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

Static ECDH cipher suites:

- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_RC4_128_SHA
- TLS_ECDH_ECDSA_WITH_RC4_128_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA

ECC AES-GCM cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384